A stochastic vulnerability analysis method for armored vehicles with active protection systems (APS)

B Feng*, X Liang, W G Du, C L Qiu and R S Hou

China Huayin Ordnance Test Center, #450, Yuemiao Street, Huayin, Shaanxi, China

Email: fengbin.plaust@foxmail.com

Abstract. A stochastic vulnerability analysis method for armored vehicles with APS was proposed. A two-processes threat-target interaction, including an interception process and a damage process, replaced the one-process of threat-target interaction in the traditional vulnerability method. Depending on the vulnerability results of the incoming threat, various residues-after-interception because of detection or interception failure, deflection, explosion and/or decomposition of the threat and collateral damage was generated and treated as input in the damage process. After randomization of the interception point, the residual penetrator deflection, warhead performance, behind armor debris, and component vulnerability characterization, a stochastic vulnerability analysis was performed. The stochastic model could provide damage states of all the critical components of interest, more practical and informative compared to the expected model.

1. Introduction

Active Protection Systems, or APS, are an upgrade that can be installed on armored vehicles or motorcrafts [1]. These systems are designed to protect the vehicle from incoming missiles and/or projectiles by either diverting them away (soft kill systems) or destroying them completely (hard kill systems). Since 1960s, the development of APS has witnessed a booming stage. The major military forces in the world, America, Russia, Germany, Israel, etc., have already deployed APS on their main battle tanks and other armored vehicles.

Vulnerability analysis is used to characterize the ability of a combat system to withstand enemy threats [2], which often involving four stages: 1) Determining the relevant threat-engagement parameters and values; 2) Analyzing the elementary ballistic processes; 3) Evaluating the response of major subsystems to damage; 4) Estimating the implications of these subsystems responses for tactical utility and mission success. Multiple vulnerability analysis software packs (e.g. MUVES, COVART, AJEM) with associated live-fire test database are released and maintained by related organizations.

Limited by the computing ability at early stages of vulnerability development, most vulnerability analysis models established then are expected-value models. That is, they calculate the probability that a given outcome (e.g., an K-Kill) occurs for a given encounter, but they give no information on the variability of that outcome. However, it has long been known that the threat-target ballistic interactions involve many random processes, such as the location of the impact point about the aimpoint and the orientation of the munition at the instant of impact [3, 4]. With advancements in computing technology and computing hardware, a stochastic vulnerability analysis could model the events probabilistically. As the model was exercised, various discrete damage states were predicted,
together with a likelihood of occurrence and the attendant effects on battlefield functions. A stochastic vulnerability analysis method could estimate the expected change in system-level results due to changes in error distribution parameters of various random phenomenon, therefore overcomes the deterministic nature of expected-value models.

Although the vulnerability analysis for armored vehicles has been widely researched and implemented, the vulnerability analysis for armored vehicles with APS was rarely reported. However, armored vehicles with APS could intercept an incoming threat from 360° at 85%–95% possibility, more recent APS could even intercept successive threats, which greatly enhance the survivability of the armored vehicle [5]. Therefore, present vulnerability analysis methods must be modified and updated to accommodate this new challenge.

In this paper, a stochastic vulnerability analysis method for armored vehicles with APS was proposed. It would be shown that when the APS was considered, the method and results of vulnerability analysis for armored vehicles would be drastically different.

2. Theoretical Framework

2.1. Define the Interception Scenario

In this section, the scenario of an RPG (rocket-propelled grenades) attacking an armored vehicle with a hard kill system (figure 1) was used to demonstrate the theoretical framework of the stochastic vulnerability analysis method. It is assumed that the APS uses a radar to detect the incoming threat. When a threat is detected, the APS would fire an intercept munition, and the time-fused munition would explode at the approximation of the incoming threat and generate multiple fragments to disable it.

![Interception Scenario](image)

Figure 1. Interception Scenario.

2.2. Factor Decomposition

In traditional vulnerability analysis for armored vehicles, only one process of threat-target interaction is analyzed, i.e. the interaction of incoming missiles and/or projectiles with armored vehicles. Therefore the most general form of the probability of the target damaged by the weapon \(P_{\text{damage}}\) could be written as:

\[
P_{\text{damage}} = P_{\text{hit}} \times P_{\text{damage|hit}}
\]

Where \(P_{\text{hit}}\) addresses the accuracy with which the weapon may be delivered, whereas \(P_{\text{damage|hit}}\) is a
measure of the effectiveness of the weapon against the target if it is hit.

When the APS is added into the analysis, the threat-target interaction becomes much more complicated, which could be divided into two processes. The first is called the interception process, in which the interaction of interception ammunition and incoming threat is dealt with. The second is called the damage process, in which the traditional vulnerability analysis for armored vehicles was performed except the incoming threat was replaced by residues-after-interception. Multiple events could happen in the two processes (Figure. 2), according to which the residues-after-interception could be weapons because of unsuccessful interception, deflected weapons and/or fragments generated by the intercept ammunition or destroyed weapons. Therefore, the general form of the $P_{damage}$ becomes to:

$$P_{damage} = (1 - P_{interception}) \times P_{hit} \times P_{damage|hit}$$

Where $P_{interception}$ represents the probability of interception of APS against the weapon. In the new equation, the $P_{interception}$ could be expanded into:

$$P_{interception} = P_{detect} \times P_{precision} \times P_{intercept|hit}$$

Where $P_{detect}$ is the probability of detection of the incoming threat by the radar of the APS, $P_{precision}$ represents the probability of the intercept ammunition delivered precisely onto the incoming threat, and $P_{intercept|hit}$ addresses the effectiveness of the intercept ammunition against the incoming threat if it is hit. $P_{intercept|hit}$ could be further expanded according to the survivor rule:

$$P_{intercept|hit} = 1 - (1 - P_{destroy|hit})(1 - P_{deflect|hit})$$

In which $P_{destroy|hit}$ is the probability of destruction of the incoming threat if it is hit by the intercept ammunition, and $P_{deflect|hit}$ is the probability of the weapon deflected away from the target if it is hit. Although it seems that only one factor was added into the equation, the meaning of all remained factors is changed. The $P_{hit}$ should include not only the weapon accuracy but also the probability of hitting by residues-after-interception. The $P_{damage|hit}$ should also be represented according to the type of the residues-after-interception, which could be written as:

$$P_{damage|hit} = 1 - (1 - P_{penetration})(1 - P_{fragment})(1 - P_{collateral})$$

$P_{penetration}$ is the damage probability of the threat because of unsuccessful interception or deflection, and the damage mechanism is usually penetration caused by armor-piercing or shaped charge weapons. $P_{fragment}$ is the damage probability of residue fragments generated by the explosion or decomposition of the intercepted threat. $P_{collateral}$ represents the collateral damage caused by intercept munition.

Figure 2. Threat-target interaction events.

Finally, the full expression of damage probability of armored vehicles with APS could be written
as:

\[ P_{\text{damage}} = \{1 - P_{\text{detect}} \times P_{\text{precision}} \times [1 - (1 - P_{\text{destroy|hit}})(1 - P_{\text{deflect|hit}})]\} \]

\[ \times P_{\text{hit}} \times [1 - (1 - P_{\text{penetration}})(1 - P_{\text{fragment}})(1 - P_{\text{collateral}})] \]  \hspace{1cm} (6)

The advantage of the full expression is that every factor in the equation could be analyzed and experimented separately, therefore the whole vulnerability analysis could be decomposed into independent and executable subsets.

3. Stochastic Vulnerability Analysis

A stochastic vulnerability analysis could give the user the ability to observe the effects of penetration errors and threat input on system-level vulnerability results. As for the vulnerability analysis of armored vehicles with APS, many random events occur in this scenario, and these events could always be described with a distribution function or empirical function. Therefore a stochastic method is appropriate for the situation.

3.1. Events randomization

The first thing to develop a stochastic model is identifying the events and variables that need to be stochastically varied. The following events should be firstly considered:

(1) Radar detection rate

The prerequisite condition for the interception is for the radar to detect the incoming threat. Usually a radar has a possibility to miss the threat, so the threat has a chance to hit the target without being detected [6]. Therefore the radar detection rate should be tested and input into the model as a stochastical event. In the early stages of the development, contractor specification values could also be used as radar detection rate input.

(2) Interception point

Here the interception point is defined as the explosion point of the intercept munition, this definition is convenient for the following vulnerability computation. The variability of the interception point comes from many sources. It could come form random variation in radar detection precision (\( \sigma_{\text{detect}} \)), the velocity and trajectory of the incoming threat (\( \sigma_{\text{threat-precision}} \)) and the intercept ammunition (\( \sigma_{\text{intercept-precision}} \)), and the fuse time of the intercept ammunition (\( \sigma_{\text{fuse-time}} \)). Part of these sources of variation could be analytically calculated, and since most of these factors are independently distributed, these variations could be separately tested and added into the whole variation. For example, if all the above variations are tested and expressed as their effects on the position of the interception point, since all these factors could be assumed as independent of each other, the overall variation of the interception point could be written as:

\[ \sigma_{\text{interception}}^2 = \sigma_{\text{detect}}^2 + \sigma_{\text{threat-precision}}^2 + \sigma_{\text{intercept-precision}}^2 + \sigma_{\text{fuse-time}}^2 \]  \hspace{1cm} (7)

The position of the interception point could be distributed as an intercept band (Figure 1) with the overall variation. The overall variation could also be obtained from live-fire tests, therefore systematic errors and missed out factors could be included into the overall variation.

(3) Residual penetrator deflection

If the intercept ammunition did not destroy but only deflected the incoming threat. The deflection angle is randomly distributed. And when the incoming threat hit the armor of the target vehicle, the penetrator’s residual portion can deflect upon existing armor. The deflection is greatest near the limit velocity. Therefore, a distribution function should be used to select trajectories near the expected deflection.

(4) Warhead performance

Warhead performance parameters, e.g., depth of penetration and hole size, are usually randomly distributed [7]. The distribution parameters could be obtained by repeated warhead/armor experiments. Then, in the course of warhead/armor calculations, random draws could be made from these
distribution functions.

(5) Behind armor debris (BAD)

When a munition perforates armor, a spray of potentially lethal fragments is formed behind the armor. These fragments consist of broken pieces of penetrator and armor material ejected by the penetration process and/or shock wave release. Many of the fragments are large enough and are moving fast enough to be extremely dangerous to personnel and highly damaging to vehicle components [8]. A spall model based on BAD described in terms of fragment mass, velocity, and shape factor should be established. Then the program could randomly draw from distributions of BAD fragment characteristics and treat each fragment as a separate penetrator to compute damage to each component it encounters along its path.

(6) Component vulnerability characterization

The randomization of component vulnerability is somewhat straightforward. Usually a fragility curve for any critical component in the system should be available for the vulnerability analysis [9]. Therefore the kill or degraded state of that any component could be randomly drawn from the fragility curve in one Monte Carlo iteration. Each critical component is separately characterized against main penetrators and single lethal spall fragments, then multiple hits are assessed using the survivor rule.

3.2. Stochastic Vulnerability Analysis Process

The following is a simple outline of the stochastic vulnerability analysis process:

(1) Identify the incoming threat based on the radar detection rate. If the radar failed to detect the threat, go to step (5).

(2) Randomly draws an interception point from the intercept band.

(3) Generate point-burst fragments from the interception munition, interact fragments with the incoming threat through shotlines.

(4) Execute vulnerability analysis for the incoming threat.

(5) According to the state of critical components (figure 3) of the threat after the impact by the fragments, generate the residues-after-interception. The residues-after-interception could have the following states: 1) The warhead or fuse of the RPG threat was hit and detonated, generate multiple fragment debris; 2) The hitting of the fragments causes structural failure of the RPG threat, generate several large debris; 3) The hitting on motor and/or tail sections causes the deflection of the RPG; 4) No critical components were damaged, the threat keeps flying unaffected. In addition, if the threat was not identified by the radar in step (1), it automatically becomes the residues-after-interception.

(6) Generate collateral damage fragments from intercept munition and adds them into the residues-after-interception.

(7) Interact residues-after-interception with the armored vehicle through shotlines.

(8) Execute vulnerability analysis for the armored vehicle, including: 1) Check for suspension and other exterior damage; 2) Check for perforation of armor; 3) If perforation, randomly deflect residual penetrator, randomly generate BAD; 4) Assess components killed because of residual penetrator and BAD, randomly draw from the fragility curve.

(9) Record vehicle damage state.

(10) Repeat the above damage assessment processes for pre-defined times, 999 in this case.
4. Model Output

In this section, an example of the model output was presented to demonstrate how the results of the stochastic vulnerability analysis differ from an expected model. Please note that all quantitative results are notional and are for illustrative purposes only.

Table 1 shows the vulnerability results of the incoming RPG threat after 1000 iterations. Instead of a definative kill probability (Pₖ) of the expected model, the stochastic model could provide damage states of all the critical components of interest. The “0” in table 1 indicates no damage for the given component, and the “1” indicates the component has been damaged. For each damage state, the residues-after-interception the state generated was presented, along with the relative occurrence probability of that damage state. The damage states were sorted and ranked from the most to the least likely in occurrence. It shows that the most likely incoming threat component damage state is for only the fuse or warhead was damaged, and the residues-after-interception generated was fragment debris caused by the explosion of the warhead. This outcome occurred 354 times in the 1000 iterations. Note that the final cumulative sum occurrence probability is not 1.000 but 0.972, because for 28 times the radar of the APS had not detected the incoming RPG and the vulnerability analysis was not executed.

| Fuse/| Mortor/tail section | Strucutral failure | Residues-after-interception | Occurrence probability |
|---|---|---|---|---|
| Component damage states | | | Fragment debris | 0.354 | 0.354 |
| 1 | 0 | 0 | 0 | 0.328 | 0.682 |
| 1 | 1 | 1 | Fragment debris | 0.125 | 0.807 |
| 0 | 1 | 0 | Deflected threat | 0.114 | 0.921 |
| 0 | 0 | 0 | Unaffected threat | 0.051 | 0.972 |
| 0 | 1 | 1 | Large debris | |

Table 2 shows the vulnerability results of the crew in the armored vehicle. It indicates that the most likely crew damage state is no one get killed, the occurrence probability is 0.808, which means that in this scenario the APS indeed enhanced the survivability of the armored vehicle effectively. Other damage states were also sorted and ranked from the most to the least likely in occurrence.

| Component damage states | Occurrence probability |
|---|---|
| Commander | Gunner | Loader | State | Cumulative sum |
| 0 | 0 | 0 | 0.808 | 0.808 |
| 0 | 1 | 0 | 0.053 | 0.861 |
| 1 | 0 | 0 | 0.054 | 0.915 |
| 1 | 1 | 0 | 0.085 | 1.000 |

Table 3 shows all the critical components of the armored vehicle got killed in 1000 iterations and corresponding damage sources. In this threat-target scenario, the most vulnerable component is fuel tank 1, and the most lethal threat source is incoming RPG threats that unafected by the APS intercept munition. Deflected threat and undetected threat also contributed to the overall damage. On the other hand, fragment debris and large debris that induced by the explosion and decomposition of the RPG caused no damage to the vehicle, which is reasonable since metal jet rather than explosive fragments are the main damage mechanism of RPGs. Obviously the safety of the intercept munition still needs some improvement since collateral damage killed the fuel tank 1 and right track 3 times.
Table 3. Vulnerability results of critical components of the armored vehicle.

| Component     | Total | Fragment debris | Deflected threat | Unaffected threat | Undetected threat | Large debris | Collateral damage |
|---------------|-------|-----------------|------------------|-------------------|-------------------|--------------|-------------------|
| Fuel tank 1   | 0.152 | 0.000           | 0.017            | 0.104             | 0.028             | 0.000        | 0.003             |
| Commander     | 0.139 | 0.000           | 0.010            | 0.102             | 0.027             | 0.000        | 0.000             |
| Gunner        | 0.138 | 0.000           | 0.011            | 0.098             | 0.029             | 0.000        | 0.000             |
| Right track   | 0.112 | 0.000           | 0.005            | 0.085             | 0.019             | 0.000        | 0.003             |

Finally, the probability of the armored vehicle falls into one of the three kill categories, i.e. Mobility kill (M-Kill), Firepower kill (F-Kill) and Catastrophic Kill (K-kill), could be calculated by aggregating above vulnerability results of critical components (table 4).

Table 4. Kill categories of the armored vehicle.

| Target       | M-Kill | F-Kill | K-Kill |
|--------------|--------|--------|--------|
| Armored Vehicle #1 | 0.152  | 0.085  | 0.057  |

5. Conclusions
In this paper, a stochastic vulnerability analysis method for armored vehicles with APS was proposed. When the APS was considered, a two-processes threat-target interaction, including an interception process and a damage process, replaced the one-process of threat-target interaction in the traditional vulnerability method. Depending on the vulnerability results of the incoming threat, various residues-after-interception because of detection or interception failure, deflection, explosion and/or decomposition of the threat and collateral damage was generated and treated as input in the damage process. After randomization of the interception point, residual penetrator deflection, warhead performance, behind armor debris, and component vulnerability characterization, a stochastic vulnerability analysis was performed. The stochastic model could provide damage states of all the critical components of interest, more practical and informative compared to the expected model.

References
[1] Hazell P J 2007 Active Protection Systems Come of Age Military Technology
[2] Pearce J R 2016 Weaponeering: Conventional Weapon System Effectiveness – Second edition 117 864-5
[3] Rosenberg Z. and E Dekel 2012 Terminal Ballistics (Berlin: Springer) p 117-25
[4] Grinfeld Michael 2014 Novel Methods in Terminal Ballistics and Mechanochemistry of Damage (US Army Research Laboratory) p2001-7
[5] Wey P, V Fleck and P Y Chanteret 2001 Proceedings of the 19th International Symposium on Ballistics
[6] Pappert, Gunnar WR, Klaus Schlüeter and Volker Koch 2002 Anti-tank munitions detectability and interceptability Targets and Backgrounds VIII: Characterization and Representation 4718 (International Society for Optics and Photonics)
[7] Huang and Xue Feng 2014 Simulation on Influence of Two-Stage Warhead Penetration at Different Obliquity Angles Applied Mechanics and Materials 556 (Trans Tech Publications)
[8] Yossifon G and A L Yarin 2002 Behind-the-armor debris analysis International journal of impact engineering 27 807-35
[9] Chircop Paul A and Bernard J Kachoyan 2018 Damage accumulation and probability of kill for gun and target engagements Naval Research Logistics (NRL) 65 160-75