False Targets vs. Protection in defending Parallel Systems against Unintentional and Intentional Impacts

G. LEVITIN¹, R. PENG², M. XIE², S-H. NG², and H. BEN HAIM¹

¹The Israel Electric Corporation Ltd. P.O. Box 10, Haifa 31000, Israel
²Department of Industrial and Systems Engineering, National University of Singapore, Singapore, Singapore 119260

(Received on October 06, 2011 and revised on July 09, 2012)

Abstract: This article considers a parallel system exposed to external intentional impacts caused by malicious attacks, and unintentional impacts caused by natural disasters or technological accidents. The defender distributes its resource between the deployment of false targets and the protection of genuine system elements. The deployment of false targets is intended to misinform the attacker so that it is not able to distinguish between the false targets and the genuine system elements, which leads to dissipating the attack resources. Different combinations of unintentional and intentional impacts sequences are considered. The vulnerability of each system element is determined by an attacker-defender and unintentional impact-defender contest success functions. A framework of solving the optimal defense resource distribution which minimizes the overall system vulnerability is suggested. Illustrative examples are presented.

Keywords: Reliability, contest success function, defense, false targets, protection

1. Introduction

Basic Definitions and Notation

- **genuine element (GE)**: lowest-level part of the system separated from other parts;
- **false target (FT)**: imitation of GE used as a decoy;
- **target**: either GE or FT (the attacker cannot distinguish GEs and FTs by observation);
- **target vulnerability**: conditional probability of target destruction given it is attacked;
- **protection**: technical or organizational measure aimed at reduction of GE vulnerability;
- **effort**: amount of intentional force aimed at destruction or protection of a GE (in this paper it is measured as the amount of attacker's or defender's resource allocated to each element);
- **intentional impact (II)**: an impact caused by strategically planned malicious human actions;
- **unintentional impact (UI)**: an impact caused by natural or technological accidents or human errors

The literature on the system defense against external impacts grows steadily [1,2]. Protecting against intentional impacts (II) is fundamentally different from protecting against unintentional impacts (UI), such as naturally occurring events or technological accidents. For a system under intentional attacks, the attacker can take advantage of his knowledge about the system to optimize his attacking strategy so as to incur maximum damage to the system [3-6]. Thus it is important for the defender to take into account the attacker's strategy when he decides how to allocate his resource among several defensive measures [7-10].
In practice, systems can be exposed to both UI and II. The UI can be any type of natural or technological harmful event. The examples of natural UI are events caused by avalanches, earthquakes, tsunamis, fire, and disease. Examples of technological UI are industrial hazards, power outage, hazardous materials, aviation, and space incidents. The II can include any means available in warfare and terrorism that render a system nonfunctional. The II is different from the UI in two ways. First, the intentional attack is strategic, which means that the attacker can choose the time and place of the attack that maximize the expected damage; whereas the UI is random, and the magnitude, time, and place of its occurrence do not depend on human actions. Second, if the attacker attacks several elements, it has to distribute its resource among the elements. In contrast, we assume that the reach of a UI is greater than the distribution of the genuine elements (GEs) so that any element can be affected by the UI, whereas the reach of a single II cannot affect more than one element. This assumption implies that the magnitude of a UI which impacts a given element does not depend on the number of elements exposed to the UI.

There are three measures of passively defending objects against II and UI: 1) providing redundancy (and separating redundant elements, which makes impossible destruction of several elements by a single impact); 2) protecting the system elements (where protection presumes actions aimed at reducing the destruction probability of an element in the case of any external impact); 3) deploying false targets (which dissipates the attacker resources among greater number of targets and reduces its per-target effort). Measure 1 makes the system parallel (though each redundant object may have complex structure, it can be considered as a single target that can be destroyed/incapacitated by an impact from the defender's and attacker's points of view). The effect of measure 2 against UI and II has been studied extensively [11-16]. While measure 1 and measure 2 are effective in the case of both UI and II, measure 3 is effective only against II.

The objective of a FT is to give the appearance that the element is something else than it actually is. A FT conceals or distracts something else, i.e., the genuine object, which the attacker actually searches for. FTs are effective if the attacker cannot confidently distinguish them from the genuine elements. False elements are usually cheaper than the system elements to produce and deploy, but are not costless, and hence the defender must make a deployment assessment. Deploying many FTs leaves less resource for protecting genuine elements.

Blanks [17] provides historical examples for the use of decoys in WWII and the 1990-1991 Operation Desert Storm, and writes that the U.S. Army (at one point prior to 1994) invested $7.5M into fielding multispectral tactical decoys. NATO commander Wesley Clark publicly admits that during the 1998-1999 Kosovo war the Serbs "did skillfully deploy lots of decoys."

The optimal strategy of deploying FTs has first been studied in [18] and [19]. It has later been extended in different aspects, such as considering imperfect false targets, and systems with more complex configurations [20-24]. All these works studied the effectiveness of the FTs only under II scenario and did not take into account the possible effect of combination of UI and II. In this paper we study the defense resource distribution between measure 2 and measure 3 in defending a parallel system against both unintentional and intentional impacts. Considering the simple parallel systems is essential to understanding the basic outcomes of the interaction between UI and II when false targets are involved. In the case of more complex system structures and non-identical elements, the results may be strongly affected by the system configuration, which prevents eliciting general conclusions. The analysis of specific systems with complex structures is beyond the scope of the paper. However, the insights presented could help in the analysis of complex systems because they usually consist
of subsystems containing parallel (redundant) elements. Moreover the framework can be suitable to many real world systems that have a parallel structure, such as power generators, water supply systems, and telecommunication systems.

We consider different scenarios of II and UI, and assume that the attacker can adapt its strategy in a way that maximizes its chance of destroying the system. More specifically we assume that the system can be damaged in four scenarios: UI only, II only, II before UI, and UI before II. The defender distributes its resource into deployment of FTs and protections against the impacts. The UI is an unintentional event with a specified magnitude that occurs with a certain probability. In the cases that the II is involved, the attacker distributes its resource among a chosen subset of targets which maximizes the expected damage. For the fourth scenario, we assume that the attacker has full information about the elements destroyed by the UI. This means that we confine attention to UI where the impact is observable. The vulnerability of each element is determined by contest success function between the defender and the attacker, and between the defender and the unintentional impact.

Section 2 presents the general model of contests over element destruction in the case of II and UI. Section 3 contains derivation of the system vulnerability for different combinations of UI and II. Section 4 presents a methodology of the model analysis.

2. The Model

Nomenclature

<table>
<thead>
<tr>
<th>Symbol</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>N</td>
<td>number of parallel genuine elements (GEs)</td>
</tr>
<tr>
<td>F</td>
<td>number of FTs deployed</td>
</tr>
<tr>
<td>M</td>
<td>number of protected GEs</td>
</tr>
<tr>
<td>T</td>
<td>per target attack effort (attack resource allocated on a target)</td>
</tr>
<tr>
<td>t</td>
<td>per element protection effort (protection resource allocated on a GE)</td>
</tr>
<tr>
<td>s</td>
<td>cost of a single FT</td>
</tr>
<tr>
<td>r</td>
<td>defender’s total resource</td>
</tr>
<tr>
<td>R</td>
<td>attacker’s total resource</td>
</tr>
<tr>
<td>D</td>
<td>magnitude of the UI</td>
</tr>
<tr>
<td>z</td>
<td>probability of FT destruction by the UI</td>
</tr>
<tr>
<td>q</td>
<td>number of attacked targets</td>
</tr>
<tr>
<td>q_j</td>
<td>optimal value of q for scenario j</td>
</tr>
<tr>
<td>M</td>
<td>optimal value of M</td>
</tr>
<tr>
<td>F</td>
<td>optimal value of F</td>
</tr>
<tr>
<td>m</td>
<td>II-protection contest intensity</td>
</tr>
<tr>
<td>f</td>
<td>UI-protection contest intensity</td>
</tr>
</tbody>
</table>

The UI and II can be dependent events. For example, the attacker that had no intention to attack the undamaged system can decide to attack it if the UI has occurred, and the system has been partly destroyed. Therefore, like model considered in [13], our model is based on four scenarios in which the system can be damaged, and a fifth “no event occurs”, which constitute a complete set of mutually exclusive events:

1) only UI happens during the system lifecycle;
2) only II happens during the system lifecycle
3) both UI and II happen during the system lifecycle, and the II happens first
4) both UI and II happen during the system lifecycle; the UI happens first; and
5) no event occurs.
Each of the scenarios can happen with a certain probability \( P_j (1 \leq j \leq 5) \), that can be estimated based on historical data, and experts’ judgment. We don’t analyze the fifth scenario which leaves the system intact, and assume that the probabilities of scenarios 1-4 are exogenously given. Thus the scenarios do not depend on the agents’ strategies. In particular, this means that the attacker’s decision to attack is not influenced by the number of FTs deployed, and by the protection efforts allocated on the GEs.

As in [13], we determine the vulnerability of any GE using the impact-protection contest success function modeled with the common ratio form \([25, 26]\) as

\[
v(T, t) = \frac{T^m}{T^m + t^m} = \frac{1}{1 + [t/T]^m}
\]

where \( T \) is the effort of the attacker (or the magnitude of the UI, whichever applies), \( t \) is the defender’s protective effort allocated to each element, and \( m \) is a parameter that describes the intensity of the contest. Especially if an attacked element is without protection \((T>0, t=0)\), the element will be destroyed with probability 1. When \( m=0 \), no matter what are the sizes of \( T \) and \( t \) the vulnerability of the element is 50%. When \( 0<m<1 \), there is a disproportional advantage of investing less than one’s opponent. When \( m=1 \), the investments have proportional impact on the vulnerability. When \( m>1 \), there is a disproportional advantage of investing more than one’s opponent. When \( m=\infty \), \( v \) is a step function where “winner-takes-all”.

A system consists of \( N \) identical GEs connected in parallel. The system is destroyed if and only if all its \( N \) GEs are destroyed. The defender and the attacker’s resources, \( r \) and \( R \), are fixed. The defender distributes his resource among deploying \( F \) false targets and protecting the GEs. The cost for deploying one FT is \( s \). We assume that the FTs are perfect, that is, the attacker cannot distinguish between genuine GEs and FTs. In the case that all the \( N \) GEs are equally protected, the protection resource allocated on each element is \( t = (r-Fs)/N \).

If the defender protects \( M \) out of the \( N \) GEs, the protection resource per protected GE is \( t = (r-Fs)/M \). It is assumed that the attacker knows the number of \( M \), but does not know which \( M \) GEs are protected.

The UI has magnitude \( D \), and strikes any element with the same magnitude irrespective of the number of elements in the system. The conditional probability of protected GE destruction by the UI given it occurs is determined by the contest success function (1), replacing \( T \) with \( D \), and \( m \) with \( f \):

\[
w(D, t_M) = D^f \left( D^f + t_M^f \right)^{-1} = [1 + ((r - Fs) / DM)^f ]^{-1}
\]

where \( f \) is the UI-defender contest intensity. The conditional probability of destruction of a false target in the case of UI is assumed to be constant, and is denoted as \( \epsilon \).

The attacker allocates its resource \( R \) among the attacked targets. Assuming that the attacker attacks \( q \) targets, its resource per target is \( T_q = R/q \), and the conditional probability of protected GE destruction is

\[
v(T_q, t_N) = T_q^m \left( T_q^m + t_N^m \right)^{-1} = [1 + (q(r - Fs) / MR)^m ]^{-1}
\]

The unprotected GEs are destroyed by any impact with probability 1.

3. System Vulnerability Evaluation

Scenario 1: The UI hits the system consisting of \( N \) parallel GEs. The GEs without protection are destroyed with probability 1. Thus the system is destroyed if and only if the \( M \) protected
False Targets vs. Protection in defending Parallel Systems against Unintentional and Intentional Impacts

GEs are destroyed, the conditional probability of which is \( w(D, t_M)^M \). The unconditional system destruction probability by the UI under scenario 1 is

\[
P_1 w(D, t_M)^M
\]

**Scenario 2:** The attacker cannot distinguish the F FTs from the N GEs. The attacker distributes its resource among \( q \) out of the \( N+F \) targets to attack which maximizes the system destruction probability. Since the system is destroyed only if all the N GEs are destroyed, the optimal number of attacked targets \( q^*_2 \) must satisfy \( N \leq q^*_2 \leq N+F \). The probability that all the N GEs are attacked is

\[
\left( \frac{F}{q-N} \right) \left( \frac{N+F}{q} \right)^{-1}
\]

Since the attacked unprotected GEs are destroyed with probability 1, the conditional system destruction probability given that the N GEs are attacked is

\[
v(T_{q^*_2}, t_M)^M
\]

The conditional system destruction probability given \( q \) is

\[
\left( \frac{F}{q-N} \right) \left( \frac{N+F}{q} \right)^{-1} v(T_{q}, t_M)^M
\]

The attacker chooses the most harmful \( q \) which maximizes the system destruction probability, hence we have

\[
q^*_2 = \arg \max_{N \leq q \leq N+F} \left( \frac{F}{q-N} \right) \left( \frac{N+F}{q} \right)^{-1} v(T_{q^*_2}, t_M)^M
\]

The unconditional system destruction probability is

\[
P_2 \left( \frac{F}{q^*_2 - N} \right) \left( \frac{N+F}{q^*_2} \right)^{-1} v(T_{q^*_2}, t_M)^M
\]

Figure 1 presents the optimal number of attacked targets as a function of the number of protected GEs \( M \) for different values of \( m \) when \( r/R=1, s/R=0.1, N=8, \) and \( F=3 \). It can be seen that when the contest is not intensive (low \( m \)), the attacker always attacks all the \( N+F \) targets to ensure that all the GEs are attacked. For intensive contests (high \( m \)) the function \( q^*_2(M) \) is U-shaped. Indeed, when \( M \) increases remaining small enough, the number of protected GEs increases, whereas their protection remains strong enough. In order to destroy all these protected GEs, the attacker needs to concentrate his attack effort distributing it among less attacked targets in the risk of leaving some GEs not attacked. When \( M \) continues to increase, the defender’s per element protection effort decreases, thus the attacker again chooses to attack more targets to ensure that all the GEs are attacked. It can also be seen that \( q^*_2 \) decreases with the increase of \( m \). This is because with the increase of intensity, it becomes more important to achieve resource superiority on attacked GEs. The attacker concentrates on fewer targets in the risk of leaving some GEs not attacked.
Figure 1: The optimal number of attacked targets $q^*_{m}$ of a function of $M$ for different values of $m$ when $r/R=1$, $s/R=0.1$, $N=8$, and $F=3$.

Figure 2 presents the optimal number of attacked targets as a function of the number of deployed FTs $F$ for different values of $m$ when $r/R=1$, $s/R=0.1$, $N=8$, and $M=5$. It can be seen that $q^*_{m}(F)$ is an increasing function of $F$. This is because when there are more FTs the attacker needs to attack more targets to ensure that all the GEs are attacked. It can also be seen that $q^*_{m}$ decreases with the increase of $m$. The behavior of $q^*_{m}$ with the change of $m$ can be explained similarly to Fig. 1.

Scenario 3: First the attacker chooses the number of attacked targets $q$ which maximizes the system destruction probability and attacks these targets. Then the UI with magnitude $D$ hits each element. The attacker cannot know whether UI will happen or not after the II (thus, he cannot distinguish scenarios 2 and 3). However, acting at random, it can choose $q = q^*_{m}$ that maximizes the system destruction probability. The defender anticipates the worst case.

The probability that $k$ ($0 \leq k \leq M$) protected GEs are attacked in II given $q$ targets are attacked is

$$
P_3 = \sum_{k=0}^{M} \binom{M}{k} \binom{N + F - M}{q - k} \binom{N + F}{q}^{-1}
$$

(10)

All the unprotected GEs are destroyed by either II or UI. The conditional probability that $i$ protected GEs out of $k$ attacked protected GEs are destroyed by II is

$$
P_3 \sum_{k=0}^{M} \binom{M}{k} \binom{N + F - M}{q - k} \binom{N + F}{q}^{-1} \sum_{i=0}^{k} \binom{k}{i} v(T_q \cdot t_M)^i \left(1 - v(T_q \cdot t_M)ight)^{k-i} w(D, t_M)^{M-i}
$$

(11)

The conditional system destruction probability by UI given that $i$ protected GEs are destroyed by II is $w(D, t_M)^{M-i}$. Thus the unconditional system destruction probability is

$$
P_3 \sum_{k=0}^{M} \binom{M}{k} \binom{N + F - M}{q - k} \binom{N + F}{q}^{-1} \sum_{i=0}^{k} \binom{k}{i} v(T_q \cdot t_M)^i \left(1 - v(T_q \cdot t_M)ight)^{k-i} w(D, t_M)^{M-i}
$$

(12)
The optimal number of attacked targets \( q_3^* \) can be expressed as
\[
q_3^* = \arg \max_{k \leq q \leq M} \sum_{k=0}^{M} \binom{N + F - M}{k} \binom{N + F}{q - k} \sum_{i=0}^{k} \binom{k}{i} r(T_q \cdot t_M)^i [1 - v(T_q \cdot t_M)]^{k-i} w(D, t_M)^{M-i}
\]
(13)

Figure 3 presents the optimal number of attacked targets as a function of the number of protected GEs \( M \) for different values of \( m \) when \( r/R=1, s/R=0.1, N=8, D=1, f=4 \) and \( F=3 \). It can be seen that \( q_3^* \) increases with \( M \). Actually in this scenario the attacker only needs to destroy the protected GEs, as all the unprotected GEs are destroyed by the UI. As \( M \) increases, the attacker attacks more targets to ensure that all the protected GEs are attacked. The behavior of \( q_3^* \) with the change of \( m \) can be explained similarly to Fig. 1.

![Figure 3: The optimal number of attacked targets \( q_3^* \) of a function of \( M \) for different values of \( m \) when \( r/R=1, s/R=0.1, N=8, D=1, f=4 \) and \( F=3 \).](image)

Figure 4 presents the optimal number of attacked targets as a function of the number of deployed FTs \( F \) for different values of \( m \) when \( r/R=1, s/R=0.1, N=8, D=1, f=4 \) and \( F=3 \).

![Figure 4: The optimal number of attacked targets \( q_3^* \) of a function of \( F \) for different values of \( m \) when \( r/R=1, s/R=0.1, N=8, D=1, f=4 \) and \( M=5 \).](image)

Similar to Fig. 2, \( q_3^* \) is an increasing function of \( F \). When there are more FTs the attacker needs to attack more targets to ensure that more genuine GEs are attacked. The behavior of \( q_3^* \) with the change of \( m \) can be explained similarly to Fig. 1.

Scenario 4: First the UI with magnitude \( D \) hits the system. Then the attacker attacks a subset of survived targets choosing such number of attacked targets \( q \) that maximizes the system destruction probability.

The GEs without protection are destroyed by the UI with probability 1. The probability that \( k \ (0 \leq k \leq M) \) protected GEs are destroyed by the UI is...
\[
\binom{M}{k} w(D,t_M)^k [1 - w(D,t_M)]^{M-k} .
\]
In this case there are \(M-k\) surviving GEs and all these elements are protected.

Since the destruction probability of a single FT is \(z\), the probability that \(F-i\) FTs survive the UI can be calculated as \(\binom{F}{i} z^i (1 - z)^{F-i}\). If the attacker attacks \(q\) targets out of \(M+F-k-i\) targets that survive the UI, the probability that he attacks all \(M-k\) protected GEs is
\[
\binom{F - i}{q - M + k} \left(\frac{M + F - k - i}{q}\right)^{M-k} v(T_q,t_M)^{M-k}
\]
(14)

The system is destroyed if all \(M-k\) GEs that survived the UI are destroyed by the II. Therefore the probability of the system destruction is
\[
\binom{F - i}{q - M + k} \left(\frac{M + F - k - i}{q}\right)^{M-k} v(T_q,t_M)^{M-k}
\]
(15)

After the UI the attacker attacks \(q\) out of \(M+F-k-i\) remaining targets. The best attacker's strategy for any given \(k\) and \(i\) is to attack \(q^*_4(k,i)\) targets, where
\[
q^*_4(k,i) = \arg \max_{M-k \leq q \leq M+F-k-i} \left(\frac{F - i}{q - M + k} \left(\frac{M + F - k - i}{q}\right)^{M-k} v(T_q,t_M)^{M-k}\right)
\]
(16)

The unconditional system destruction probability under scenario 4 is
\[
P_4 \sum_{k=0}^{M} \sum_{i=0}^{\min(F-k,i)} \binom{F}{i} w(D,t_M)^k [1 - w(D,t_M)]^{M-k} z^i (1 - z)^{F-i} \binom{q^*_4(k,i) - M + k}{q^*_4(k,i)} v(T_q^*,t_M)^{M-k}
\]
(17)

Figure 5 presents the optimal number of attacked targets as a function of \(k\) for different values of \(m\) when \(r/R=2\), \(s/R=0.1\), \(N=8\), \(M=5\), \(F=5\), and \(i=2\). With the increase of \(k\) the number of targets which survive the UI decreases, thus the attacker attacks fewer targets. When \(k=5\) all the protected GEs are destroyed by UI, the attacker does not need to attack any target at all. The behavior of \(q^*_4\) with the change of \(m\) can be explained similarly to Fig. 1.

![Figure 5](image-url)

**Figure 5:** The optimal number of attacked targets \(q^*_4\) of a function of \(k\) for different values of \(m\) when \(r/R=2\), \(s/R=0.1\), \(N=8\), \(M=5\), \(F=5\) and \(i=2\).
Figure 6 presents the optimal number of attacked targets as a function of the number of FTs destroyed by UI $i$ for different values of $m$ when $r/R=2$, $s/R=0.1$, $N=8$, $M=5$, $F=5$, and $k=3$.

With the increase of $i$ fewer FTs survive the UI, thus the attacker can concentrate on fewer targets. The behavior of $q_4^*$ with the change of $m$ can be explained similarly to Fig. 1.

The overall system vulnerability (probability of total destruction under any one of four mutually exclusive scenarios) is

$$V = P_1 w(D,t_M)^M + P_2 \left( \frac{F}{q_2^* - N} \right)^{-1} v(T_{q_2^*}, t_M)^M + \sum_{k=0}^{M} P_3 \left( \frac{N + F - M}{q_3^*} \right)^k \sum_{i=0}^{t_M} \left[ (1 - v(T_{q_3^*}, t_M)) w(D,t_M)^M - i \right] v(T_{q_3^*}, t_M)^k \cdot$$

$$\sum_{k=0}^{M} \sum_{i=0}^{t_M} \left( \frac{F}{M + F - k - i} \right)^{k-i} v(T_{q_4^*(k,i)}, t_M)^{M-k}$$

(18)

4. Analysis of the Defender's Strategy

The defender’s optimal strategy is to choose the $M^*$ and $F^*$ that minimize the system vulnerability $V(M,F)$ given that the attacker chooses the values $q_2$, $q_1$, maximizing $V$ for any combination of $M$ and $F$ and the value $q_3$ which maximizes $V$ for any combination of $M$, $F$, $k$ and $i$: $M^*, F^* = \arg\min_{M,F} (V(M,F,q_2^*(M,F),q_3^*(M,F),q_4^*(k,i,M,F)))$.

Consider an example with scenario probabilities $P_1=0.1$, $P_2=0.2$, $P_3=0.1$, and $P_4=0.3$; and with $s/R=0.1$, $N=8$, and $z=0.5$. Fig. 7 presents the optimal number of protected GEs $M^*$, the optimal number of deployed FTs $F^*$, and the corresponding optimal system vulnerability $V^*$ as functions of the normalized UI magnitude $D/R$ for various combinations of the contest intensities $f$ and $m$ when $r/R=2$. 
Figure 7: Optimal values of $M$, $F$ and the corresponding system vulnerability $V$ as functions of $D/R$ for various combinations of $f$ and $m$ when $r/R=2$.

It can be seen that $M^*$ decreases with the increase of $D/R$. This is because the defender needs to concentrate its protection resource on fewer GEs increasing their chances to survive the UI. The change of $F^*$ with the increase of $D/R$ is complex, since the contest involves four different scenarios. When $D/R$ is high enough and the contest intensity $f$ is also high, $F^*$ approaches 0. This is because deploying FTs is not useful against UI, which is dominant in three scenarios that involve the UI. When $D/R$ is high, $V^*$ increases with the increase of $f$ as the high intensity makes the GEs more vulnerable in the case of UI. When $D/R$ is low, $V^*$ decreases with the increase of $f$ as the defender having the per element resource superiority benefits from the high contest intensity.

Figure 8 presents the optimal number of protected GEs $M^*$, the optimal number of deployed FTs $F^*$, and the corresponding optimal system vulnerability $V^*$ as functions of the normalized defender’s resource $r/R$ for various combinations of the contest intensities $f$ and $m$ when $D/R=1$. The general tendency is to increase the number of the FTs when the defense resource increases. The number of protected GEs first decreases with $r$ and then increases. Indeed, when the attacker’s resource is superior, the defender concentrates its resource on protecting fewer GEs.
False Targets vs. Protection in defending Parallel Systems against Unintentional and Intentional Impacts

However, when $r$ increases the defender has enough resources to deploy FTs and provide good protection for greater number of GEs. The behavior of $M^*$, $F^*$ and $V^*$ with the change of $f$ and $m$ are very complicated. Actually in different scenarios the optimal $M$, $F$ and $V$ are different. The final optimal $M$, $F$ and $V$ depend on the scenario probabilities. This makes the intuitive analysis of the optimal defense strategy impossible and justifies the use of the suggested model.

Figure 8: Optimal values of $M$, $F$ and the corresponding system vulnerability $V$ as functions of $r/R$ for various combinations of $f$ and $m$ when $D/R=1$.

Figure 9: Optimal values of $M$, $F$ and the corresponding system vulnerability $V$ as functions of $s/R$ for various values of $s/R$ when $D/R=1$, $r/R=2$, $f=1$ and $m=1$.

Figure 9 presents the optimal number of protected GEs $M^*$, the optimal number of deployed FTs $F^*$, and the corresponding optimal system vulnerability $V^*$ as functions of $z$ for...
various values of \( s/R \) when \( D/R=1, \ r/R=2, \ f=1 \) and \( m=1 \). \( F^* \) generally decreases with the increase of \( z \). Indeed, when \( z \) is high FTs can be easily destroyed by the UI in scenario 4 and thus they are less effective. Similarly \( V^* \) increases with the increase of \( z \). \( M^* \) decreases with the increase of \( z \). This is because in scenario 4 the attacker can concentrate more on the GEs when \( z \) is high (with more FTs destroyed by UI), which makes the concentration of protection effort more important. With the increase of \( s \), \( F^* \) decreases since deploying the same number of FTs requires more resources.

5. Conclusions

The paper considers a parallel system, which is subject to intentional impacts (malicious human actions), and unintentional impacts (natural or technological accidents). A defender develops optimal defense strategy against both the intentional impact (II), and the unintentional impact (UI). To defend the system the defender can deploy FTs aimed at dissipating the attacker's efforts and protect some GEs reducing probability of their destruction in the case of the impacts. The defender has a limited resource, and distributes it between deploying FTs and protecting GEs. We confine attention to UI where the impact is observable. If the UI occurs first, the strategic attacker has full information about the elements destroyed, and concentrates all its effort on attacking only the survived elements. The entire system is destroyed if all its GEs are destroyed.

The vulnerability of each GE is determined by one contest success function between the defender and the II, and one contest success function between the defender and the UI, presented in section 2. For scenarios 2 and 3, the attacker distributes its resource equally across all GEs. For scenario 4, the attacker distributes its resource across all survived targets. The UI has a parametrically determined magnitude, and occurs with a certain probability.

The complex interrelation among the strategic variables (number of protected GEs and number of FTs) can produce unexpected results, which makes an intuitive analysis (not based on the suggested model) impossible.

The paper presents the model and the methodology for analysis and optimization of the defense strategy, which can be implemented for getting proper insight of the effect of defense resource distribution in the case when both the intentional and unintentional impacts threaten the system functionality.

Further research can be devoted to considering \( k \)-out-of-\( n \) systems and systems with damage proportional to the amount of unsupplied demand caused by the destruction of some of the GEs. The model can also be extended to consider the case when the attacker's decision to attack (expressed by the probability of II before and after UI) depends on the defender's strategy, and on the information available to the attacker.

References


False Targets vs. Protection in defending Parallel Systems against Unintentional and Intentional Impacts


**Gregory Levitin** is presently a senior expert at the Reliability Department of the Israel Electric Corporation and Distinguished Visiting Professor at University of Electronic Science and Technology of China. His current interests are in risk analysis, defense and
reliability. In this field he has published more than 180 papers and four books. He is a senior member of IEEE, and an associate editor of IEEE Transactions on Reliability.

**Rui Peng** is currently an assistant professor in Dongling School of Economics & Management, University of Science & Technology Beijing. He obtained B.Sc. degree from Special Class for Gifted Young, University of Science & Technology of China in 2007. He obtained Ph.D. degree from Industrial & Systems Engineering Department, National University of Singapore in 2011. His research interests include software reliability, networked system reliability, and defense strategies.

**Min Xie** received his Ph.D. from Linkoping University in 1987. He joined the National University of Singapore in 1991 as one of the first recipients of the prestigious Lee Kuan Yew Fellowship. In May 2011, Prof. Xie moved to City University of Hong Kong as Chair Professor of Industrial Engineering. Prof. Xie has published over 200 journal papers and 8 books. Prof. Xie is a fellow of IEEE.

**Szu-Hui Ng** received the Ph.D. degree from the University of Michigan, Ann Arbor. Currently, she is an Associate Professor with the Department of Industrial and Systems Engineering, National University of Singapore. Her research interests include quality and reliability engineering, design of experiments, and simulation.

**Ben Haim** is presently Head of the Reliability Department of the Israel Electric Corporation. He has got his M.Sc. and D.Sc. from the Department of Biomedical Engineering, at the Technion, the Israel Institute of Technology. His current research interests are in risk and RAMS analysis and management in which he has published some 50 papers. He is a member of CIGRE.