Limiting Adversarial Budget in Quantitative Security Assessment

Aleksandr Lenin[1,2] and Ahto Buldas[1,2,3,⋆]

[1] Cybernetica AS, Mäealuse 2/1, Tallinn, Estonia
[2] Guardtime AS, Tammsaare tee 60, Tallinn, Estonia
[3] Tallinn University of Technology, Ehitajate tee 5, Tallinn, Estonia

Abstract. We present the results of research of limiting adversarial budget in attack games, and, in particular, in the failure-free attack tree models presented by Buldas-Stepanenko in 2012 and improved in 2013 by Buldas and Lenin. In the previously presented models attacker's budget was assumed to be unlimited. It is natural to assume that the adversarial budget is limited and such an assumption would allow us to model the adversarial decision making more close to the one that might happen in real life. We analyze three atomic cases – the single atomic case, the atomic AND, and the atomic OR. Even these elementary cases become quite complex, at the same time, limiting adversarial budget does not seem to provide any better or more precise results compared to the failure-free models. For the limited model analysis results to be reliable, it is required that the adversarial reward is estimated with high precision, probably not achievable by providing expert estimations for the quantitative annotations on the attack steps, such as the cost or the success probability. It is doubtful that it is reasonable to face this complexity, as the failure-free model provides reliable upper bounds, being at the same time computationally less complex.

1 Introduction

The failure-free models [2,3] provide reliable utility upper bounds, however this results in systems that might be over-secured. It has not been studied how much extra cost the upper-bound oriented methods cause. We present the intermediate results of researching the model assuming that the adversarial budget is limited and compare the results of analysis using adaptive strategies with limited budget to the analysis results of the failure-free model, in which the adversary is not limited in any way. The adversarial limitation is the only limitation applied to

⋆ The research leading to these results has received funding from the European Regional Development Fund through Centre of Excellence in Computer Science (EXCS), the Estonian Research Council under Institutional Research Grant IUT27-1, and the the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement ICT-318003 (TREsPASS). This publication reflects only the authors' views and the Union is not liable for any use that may be made of the information contained herein.

R. Poovendran and W. Saad (Eds.): GameSec 2014, LNCS 8840, pp. 155–174, 2014.

the adversary, all other assumptions and concepts are identical to the failure-free model.

The assumption that the adversarial budget is limited is natural, as this is what happens in reality. Limited budget models the adversarial strategic decision making in a better way, which is more close to the one likely to be observed in real life and the research on the adaptive strategies with limited budget is an important research area in quantitative security analysis based on attack trees.

We analyze three cases: the atomic attack case, the atomic AND, and the atomic OR analyzing the effect of limiting adversarial budget in fully-adaptive strategies [2,3]. We show that the atomic attack case and the atomic AND case do not provide whatsoever better or more reliable results, compared to the existing failure-free models. The atomic AND case might provide more precise result, but in this case analysts must estimate the adversarial reward with the required precision, which in real-life scenarios might be less than €1. If they fail to do that, the results of such an analysis are unreliable. In practice, it is doubtful that analysts would be able to come up with such precise estimations. Even if such precise estimations existed, the model would not provide reliable results, as there is still margin for human mistake and in case analysts might overlook the estimations provided to such parameters as cost of the attack step, or the adversarial reward, the results of the analysis would not be reliable. On the contrary, the existing failure-free models with unlimited adversarial budget provide reliable utility upper bounds, despite the fact that this may result in over-secured systems.

It seems that limited budget makes the model much more complex compared to the unlimited budget approach. For example, optimal strategies that were shown to be non-adaptive in the failure-free models [2,3] can be adaptive and more complex to analyze in the limited budget model. The best move to undertake in certain states of the game changes bouncing between the attack steps.

Even the elementary cases studied in this paper become quite complex considering limited budget assumption compared to the corresponding cases in the failure-free models [2,3]. It is doubtful that the more general case will have a graceful easy solution to derive optimal strategies. Considering the requirement to be able to estimate the adversarial reward very precisely it is doubtful that it is reasonable to face the complexity of the calculations on the limited adaptive strategies.

The outline of the paper is the following: Section 1 provides a high-level overview of the problem and briefly outlines the results obtained so far. Section 2 describes the work related to the presented approach, Section 3 provides definitions of terms used throughout the paper. Section 4 describes the effect of limited budget assumption on the fully-adaptive strategies and the strategic decision making undertaken by the adversary. Finally, Section 5 summarizes the obtained results, outlines questions still left open, and describes interesting problems for future research.

2 Related Work

In this section, we outline the work that has lead to and influenced the development of the presented model.

2.1 Schneier Attack Trees' Concept

The idea of analyzing security using the so-called attack trees was popularized by Schneier in [7]. The author suggested to use attack trees as a convenient hierarchical representation of an attack scenario. The analysis implied that the analysts had to estimate one single parameter they would like to reason about, for each of the leaves in the attack tree. Then the bottom-up parameter propagation approach was applied to propagate the results of calculations towards the root node of the tree, the result of the root node was considered the result of such an analysis. The suggested bottom-up parameter propagation method allowed to reason about such parameters like minimal/average/maximal cost of the attack scenario, likelihood of its success, etc. The analysis relied on an assumption that the analyzed parameters are mutually independent, which allowed to analyze them independently of each other and to derive some meaningful conclusions about the security of the systems based on the obtained results.

2.2 Buldas-Priisalu Model

The model of Buldas *et al.* [1] is remarkable for introducing the multi-parameter approach to the quantitative security risk analysis. The model is based on the assumption of a rational adversary who is always trying to maximize his average outcome. The authors state that in order to assess security it is sufficient to assess adversarial utility. If the utility is negative or zero, the system is reasonably secure, as attacking it is not profitable. If the utility is positive, the adversary has an incentive to attack and attacking is profitable for him. The adversary undertakes strategic decision-making in accordance with the rationality assumption – the adversary will start attacking iff it is profitable. Additionally, authors state that malicious actions are, as a rule, related to criminal behavior and for this reason they applied economic reasoning in their model which considers the risk of detection and potential penalties of the adversary. Their model introduced a novel way to think about security and gave start to multi-parameter quantitative security analysis. Jürgenson *et al.* have shown that Buldas *et al.* model is inconsistent with Mauw-Oostijk foundations [6] and introduced the so-called parallel model [4] and the serial model [5] which provided more reliable results, however in both models the adversary did not behave in a fully adaptive way.

2.3 Buldas-Stepanenko Fully Adaptive Model

In the Buldas-Stepanenko fully adaptive model [3] the adversaries behave in a fully adaptive way launching atomic attack steps in an arbitrary order, depending on the results of the previous trials. However, the model had force-failure states,

when the adversary could not continue playing and thus adversarial fully adaptive behavior was limited. In their model optimal strategies are non-adaptive and in some cases, like atomic OR or atomic AND, may be easily derived by calculating certain invariants. In their failure-free model the adversary was expected to launch attack steps until success, thus the failure-free model is similar to the fully adaptive model with the difference that in the failure-free model success probabilities of the attack steps are equal to 1. The most significant contribution of the paper [3] is the upper bounds ideology by which the models should estimate adversarial utility from above, trying to avoid false-positive security results.

2.4 Improved Failure-Free Model

The improved failure-free model [2] improves the Buldas-Stepanenko failure-free model [3] by eliminating the force-failure states. In the improved model the adversarial behavior more fully conforms to the upper bounds ideology introduced in [3] – the adversary may repeat failed attack steps and play on when caught. It turned out that the elimination of the force failure states has made the model computationally easier. The authors show that in the new model optimal strategies always exist. Optimal strategies are single-branched BDD-s where the order of attack steps is irrelevant. Additionally, authors show that finding an optimal strategy in the new model is NP-complete. Two computational methods were introduced – the one allowing to compute the precise adversarial utility value, and the one which allowed to derive the approximated estimation of adversarial utility upper bound.

3 Definitions

Definition 1 (Derived function). *If* $\mathcal{F}(x_1, \ldots, x_m)$ *is a Boolean function and* $v \in \{0, 1\}$*, then by the derived Boolean function* $\mathcal{F}|_{x_j=v}$ *we mean the function* $\mathcal{F}(x_1, \ldots, x_{j-1}, v, x_{j+1}, \ldots, x_m)$ *derived from* $\mathcal{F}$ *by the assignment* $x_j := v$*.*

Definition 2 (Constant functions). *By* **1** *we mean a Boolean function that is identically true and by* **0** *we mean a Boolean function that is identically false.*

Definition 3 (Satisfiability game). *By a satisfiability game we mean a single-player game in which the player's goal is to satisfy a monotone Boolean function* $\mathcal{F}(x_1, x_2, \ldots, x_k)$ *by picking variables* x_i *one at a time and assigning* $x_i = 1$*. Each time the player picks the variable* x_i *he pays some amount of expenses* $\mathcal{E}_i \in \mathcal{R}$*, sometimes also modelled as a random variable. With a certain probability* p_i *the move* x_i *succeeds. Function* $\mathcal{F}$ *representing the current game instance is transformed to its derived form* $\mathcal{F}|_{x_i=1}$ *and the next game iteration starts. The game ends when the condition* $\mathcal{F} \equiv 1$ *is satisfied and the player wins the prize* $\mathcal{P} \in \mathcal{R}$*, or when the player stops playing. With probability* $1 - p_i$ *the move* x_i *fails. The player may end up in a different game instance represented by the derived Boolean function* $\mathcal{F}|_{x_i \equiv 0}$ *in the case of a game without move repetitions,*

and may end up in the very same instance of the game $\mathcal{F}$ in the case of a game with repetitions. Under certain conditions with a certain probability the game may end up in a forced failure state, i.e. if the player is caught and this implies that he cannot continue playing, i.e. according to the Buldas-Stepanenko model [3]. The rules of the game are model-specific and may vary from model to model. Thus we can define three common types of games:

1. *SAT Game Without Repetitions - the type of a game where an adversary can perform a move only once.*
2. *SAT Game With Repetitions - the type of a game where an adversary can re-run failed moves again an arbitrary number of times.*
3. *Failure-Free SAT Game - the type of a game in which all success probabilities are equal to 1. It is shown in [2] that any game with repetitions is equivalent to a failure-free game (Thm. 5).*

Definition 4 (Satisfiability game with limited budget). *By a satisfiability game with limited budget we mean the SAT game with move repetitions in which the current state of the game is described by the Boolean function $\mathcal{F}(x_1, \ldots, x_k)$ and the budget λ – $\langle \mathcal{F}, \lambda \rangle$. Every move x_i made by the player changes the state of the game. If x_i succeeded, the game moves into the state $\langle \mathcal{F}|_{x_i=1}, \lambda - \mathcal{C}_i \rangle$ and if x_i has failed, the new state of the game is $\langle \mathcal{F}|_{x_i=0}, \lambda - \mathcal{C}_i \rangle$, where $\mathcal{C}_i$ is the cost of x_i. The game ends if the player has satisfied the Boolean function $\mathcal{F} \equiv 1$ and reached the state $\langle \mathbf{1}, \lambda \rangle$ thus winning the game, or when the player has reached the state $\langle \mathcal{F}, \lambda \rangle$ in the case of which the expenses of every possible move $\mathcal{E}_i > \lambda$ and $\mathcal{F}$ has not been satisfied, meaning the loss of the game.*

Definition 5 (Line of a game). *By a line of a satisfiability game we mean a sequence of assignments $\gamma = \langle x_{j_1} = v_1, \ldots, x_{j_k} = v_k \rangle$ (where $v_j \in \{0, 1\}$) that represent the player's moves, and possibly some auxiliary information. We say that γ is a **winning line** if the Boolean formula $x_{i_1} \wedge \ldots \wedge x_{i_k} \Rightarrow \mathcal{F}(x_1, \ldots, x_n)$ is a tautology, where $\mathcal{F}$ is a Boolean function of the satisfiability game.*

Definition 6 (Strategy). *By a strategy $\mathcal{S}$ for a game $\mathcal{G}$ we mean a rule that for any line γ of $\mathcal{G}$ either suggests the next move $x_{j_{k+1}}$ or decides to give up.*

Strategies can be represented graphically as binary decision diagrams (BDDs).

Definition 7 (Line of a strategy). *A line of a strategy $\mathcal{S}$ for a game $\mathcal{G}$ is the smallest set $\mathcal{L}$ of lines of $\mathcal{G}$ such that (1) $\langle\rangle \in \mathcal{L}$ and (2) if $\gamma \in \mathcal{L}$, and $\mathcal{S}$ suggests x_j as the next move to try, then $\langle \gamma, x_j = 0 \rangle \in \mathcal{L}$ and $\langle \gamma, x_j = 1 \rangle \in \mathcal{L}$.*

Definition 8 (Branch). *A branch β of a strategy $\mathcal{S}$ for a game $\mathcal{G}$ is a line γ of $\mathcal{S}$ for which $\mathcal{S}$ does not suggest the next move. By $\mathcal{B}_{\mathcal{S}}$ we denote the set of all branches of $\mathcal{S}$.*

For example, all winning lines of $\mathcal{S}$ are branches.

Definition 9 (Expenses of a branch). *If $\beta = \langle x_{i_1=v_1}, \ldots, x_{i_k=v_k} \rangle$ is a branch of a strategy $\mathcal{S}$ for $\mathcal{G}$, then by expenses $\epsilon_{\mathcal{G}}(\mathcal{S}, \beta)$ of β we mean the sum $\overline{\mathcal{E}}_{i_1} + \ldots + \overline{\mathcal{E}}_{i_k}$ where by $\overline{\mathcal{E}}_{i_j}$ we mean the mathematical expectation of $\mathcal{E}_{i_j}$.*

Definition 10 (Prize of a branch). *The prize* $\mathcal{P}_{\mathcal{G}}(\mathcal{S}, \beta)$ *of a branch* β *of a strategy* $\mathcal{S}$ *is* $\mathcal{P}$ *if* β *is a winning branch, and* 0 *otherwise.*

Definition 11 (Utility of a strategy). *By the utility of a strategy* $\mathcal{S}$ *in a game* $\mathcal{G}$ *we mean the sum:* $\mathcal{U}(\mathcal{G}, \mathcal{S}) = \sum_{\beta \in \mathcal{B}_{\mathcal{S}}} Pr(\beta) \cdot [\mathcal{P}_{\mathcal{G}}(\mathcal{S}, \beta) - \epsilon_{\mathcal{G}}(\mathcal{S}, \beta)]$. *For the empty strategy* $\mathcal{U}(\mathcal{G}, \emptyset) = 0$.

Definition 12 (Prize and Expenses of a strategy). *By the expenses* $\mathcal{E}(\mathcal{G}, \mathcal{S})$ *of a strategy* $\mathcal{S}$ *we mean the sum* $\sum_{\beta \in \mathcal{B}_{\mathcal{S}}} Pr(\beta) \cdot \epsilon_{\mathcal{G}}(\mathcal{S}, \beta)$. *The prize* $\mathcal{P}(\mathcal{G}, \mathcal{S})$ *of* $\mathcal{S}$ *is* $\sum_{\beta \in \mathcal{B}_{\mathcal{S}}} Pr(\beta) \cdot \mathcal{P}_{\mathcal{G}}(\mathcal{S}, \beta)$.

It is easy to see that $\mathcal{U}(\mathcal{G}, \mathcal{S}) = \mathcal{P}(\mathcal{G}, \mathcal{S}) - \mathcal{E}(\mathcal{G}, \mathcal{S})$.

Definition 13 (Utility of a satisfiability game). *The utility of a SAT game* $\mathcal{G}$ *is the limit* $\mathcal{U}(\mathcal{G}) = \sup_{\mathcal{S}} \mathcal{U}(\mathcal{G}, \mathcal{S})$ *that exists due to the bound* $\mathcal{U}(\mathcal{G}, \mathcal{S}) \leqslant \mathcal{P}$.

Definition 14 (Optimal strategy). *By an optimal strategy for a game* $\mathcal{G}$ *we mean a strategy* $\mathcal{S}$ *for which* $\mathcal{U}(\mathcal{G}) = \mathcal{U}(\mathcal{G}, \mathcal{S})$.

It has been shown that for satisfiability games optimal strategies always exist [2].

4 Limiting Adversarial Budget in the Improved Failure-Free Model

In this paper we focus on the fully adaptive adversarial strategies assuming that the adversarial budget is limited. Budget limitation is the only limitation used, compared to the improved failure-free model [2]. Adversaries still behave in a fully adaptive way and are allowed to launch failed attack steps again in any order, until the budget gets so small that no attack steps can be launched. When the budget decreases by a considerable amount, monetary limitation starts effecting possible strategic choices of the attacker – possible set of choices reduces (the adversary may launch only some subset of the attack steps) and eventually, this subset becomes an empty set. It turns out that the optimal strategy depends on the amount of the monetary resource available to the adversary.

In the improved failure-free model the state of the game is represented by the Boolean function $\mathcal{F}$. If the attack step has failed, the adversary finds himself in the very same state of the game $\mathcal{F}$. Due to this non-adaptive strategies always exist in the set of optimal strategies of the game.

This is not always the case when we consider budget limitations – in general, optimal strategies are adaptive, except for some certain sets of parameters in case of which optimal strategies are non-adaptive. When we consider budget limitations the state of the game is represented by the Boolean function $\mathcal{F}$ and the budget λ. We denote the utility in a certain game state $\langle \mathcal{F}, \lambda \rangle$ with $\mathcal{U}^{\lambda}(\mathcal{F})$. When an attack step fails, the adversary finds himself in an another state of the

game represented by $\mathcal{U}^{\lambda-\mathcal{C}}(\mathcal{F})$, where $\mathcal{C}$ is the cost of the failed attack step. The relation between the utility upper bound $\mathcal{U}^{\infty}(\mathcal{F})$ in [2] and the utility $\mathcal{U}^{\lambda}(\mathcal{F})$ given budget λ is the following:

$$\mathcal{U}^{\infty}(\mathcal{F}) = \lim_{\lambda \to \infty} \mathcal{U}^{\lambda}(\mathcal{F}) \ .$$

In some certain cases optimal strategies are non-adaptive, but in general they are not. This makes computations reasonably complex. When the adversarial budget increases, his utility increases as well and approaches the adversarial utility upper bound in the improved failure-free model [2]. It turns out that in the case of a reasonably big budget the complexity added by the budget limitation does not add any value nor give any additional benefits, as the difference between the utility in the model with budget limitations and the utility upper bound becomes negligible.

In this paper we focus on the three elementary games – the single attack case, the atomic AND and the atomic OR game and show the effect of budget limitations in these games. Even these elementary cases become quite complex when taking budget limitations into account. It becomes doubtful if the practical application of the model with budget limitations is efficient and reliable. Using complex computational procedures we face the risk to make the model inapplicable for the practical cases, while the negligible deviation between the results of the model with budget limitations and the one without them in case of a reasonably big budget (which is the expected case in real-life scenarios) and much less complex and more efficient computations induces us to give preference to the model without budget limitations, despite the fact that it overestimates adversarial power and capabilities for the cases when the adversarial budget is reasonably small.

4.1 Single Atomic Attack Case

In case the adversary may choose from a single available choice, he will continue launching the attack step until it succeeds, or as long as the budget allows it. Such a strategy may be represented in the form of a single-branched BDD as in Fig. 1:

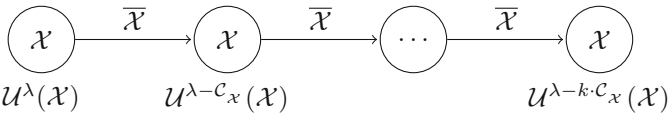

Fig. 1. An adaptive strategy suggesting to iterate attack step $\mathcal{X}$ until it succeeds or as long as the adversarial budget allows to launch the attack step

In accordance with the strategy, the adversary launches an attack step $\mathcal{X}$ with cost $\mathcal{C}$ and success probability p. If it succeeds, the adversary has accomplished

the attack and has won the game. If $\mathcal{X}$ fails, the adversary finds himself in another state of the game $\langle \mathcal{X}, \lambda - \mathcal{C} \rangle$. Thus, adversarial utility may be expressed in the form of the relation (1):

$$\mathcal{U}^{\lambda}(\mathcal{X}) = \max\left\{0,\ \mathcal{U}(\mathcal{X}) + (1-p)\cdot \mathcal{U}^{\lambda-\mathcal{C}}(\mathcal{X})\right\} \quad . \tag{1}$$

It can be seen (see Fig. 2) that the adversarial utility changes in the points where the budget is multiples of the cost of the attack step. In case the adversarial budget is less than the cost of the attack step, the adversary cannot launch a single attack step and thus his utility is 0. The optimal strategy in this case is an empty strategy – the attacker will be better off not trying to attack. In case the budget exceeds the cost of the attack step, the utility grows with each subsequent trial to launch an attack step, as every subsequent trial increases the likelihood of success that the attack step will succeed. Thus, adversarial utility asymptotically approaches the utility upper bound in the model without budget limitations.

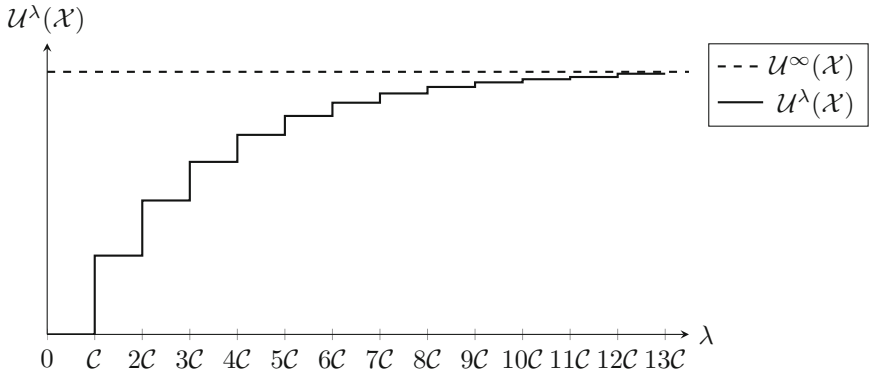

Fig. 2. Single atomic attack case

The utility value that the adversary may achieve, given budget λ, may be expressed in the form of equation (2):

$$\mathcal{U}^{\lambda}(\mathcal{X}) = \left[\mathcal{P} - \frac{\mathcal{C}}{p}\right] \cdot \left[1 - (1-p)^{\lfloor \frac{\lambda}{\mathcal{C}} \rfloor}\right] = \mathcal{U}^{\infty}(\mathcal{X}) \left[1 - (1-p)^{\lfloor \frac{\lambda}{\mathcal{C}} \rfloor}\right] \quad , \tag{2}$$

where $\mathcal{U}^{\infty}(\mathcal{X})$ is the utility upper bound [2].

Comparison with the Improved Failure-Free Model

We will investigate the case when the improved failure-free model analysis result states that the system is *insecure*, while the budgeted model result states that the system is *secure*.

According to the improved failure-free model the adversarial utility $\mathcal{U}^{\infty}(\mathcal{X}) = \mathcal{P} - \frac{\mathcal{C}}{p}$. The system is secure in case $\mathcal{P} \leqslant \frac{\mathcal{C}}{p}$ and insecure in case $\mathcal{P} > \frac{\mathcal{C}}{p}$.

$$\begin{cases} \mathcal{U}^{\infty}(\mathcal{X}) &= \mathcal{P} - \frac{\mathcal{C}}{p} > 0 \\ \mathcal{U}^{\lambda}(\mathcal{X}) &= \left[\mathcal{P} - \frac{\mathcal{C}}{p}\right] \left[1 - (1-p)^{\lfloor \frac{\lambda}{\mathcal{C}} \rfloor}\right] \leqslant 0 \end{cases} \tag{3}$$

It can be seen that the condition (3) can be reached only when the adversary has no resources to attack ($\lambda < \mathcal{C}$). Thus limiting adversarial budget does not provide more trustworthy nor more reliable results compared to the improved failure-free model in case of single atomic attack games. If in the case of some positive budget λ the adversarial utility is positive, it will be less or equal to zero in the model with budget limitations only if $\lambda < \mathcal{C}$. In other words, if the system is insecure in the improved failure-free model, it will also be insecure in the model with budget limitations for any adversarial budget, sufficient to launch the attack step at least once.

4.2 Two Attack Steps

In the case of atomic games of 2 possible attack steps $\mathcal{X}_i$ and $\mathcal{X}_j$ and corresponding costs $\mathcal{C}_{\mathcal{X}_i}$ and $\mathcal{C}_{\mathcal{X}_j}$, the adversarial utility changes in the so-called *lattice points* which are the projections of points $(n\,\mathcal{C}_{\mathcal{X}_i}, m\,\mathcal{C}_{\mathcal{X}_j})$ in two-dimensional Euclidean space into one-dimensional space using the formula $\mathcal{L}_i = n\,\mathcal{C}_{\mathcal{X}_i} + m\,\mathcal{C}_{\mathcal{X}_j}$, where $n \in \left\{1, 2, \ldots, \left\lfloor \frac{\lambda}{\mathcal{C}_{\mathcal{X}_i}} \right\rfloor \right\}$, $m \in \left\{1, 2, \ldots, \left\lfloor \frac{\lambda}{\mathcal{C}_{\mathcal{X}_j}} \right\rfloor \right\}$, $\forall i : \mathcal{L}_i \leqslant \lambda$ (see Fig. 3). In the case of three attack steps the utility changes in the projections of points in three-dimensional space into one-dimensional space. Thus with the increase in the amount of possible attack steps the lattice argument space becomes more complex.

It can be shown that the distance between the two adjacent lattice points has a lower bound.

Theorem 1. *If the relation of attack step costs may be expressed in terms of a rational fraction (a fraction of two rational numbers, corresponding cost values may be irrational)* $\frac{\mathcal{C}_{\mathcal{X}_i}}{\mathcal{C}_{\mathcal{X}_j}} = \frac{p}{q}$*, then the distance between two adjacent lattice points* $\mathcal{L}_i$ *and* $\mathcal{L}_{i+1}$ *will be not less than* $\frac{\mathcal{C}_{\mathcal{X}_j}}{q}$.

Proof. The distance δ between the two adjacent lattice points $\mathcal{L}_i$ and $\mathcal{L}_{i+1}$ may be expressed as

$$\delta = |(n-n')\mathcal{C}_{\mathcal{X}_i} + (m-m')\mathcal{C}_{\mathcal{X}_j}| = |\underbrace{(n-n')p + (m-m')q}_{\alpha \in \mathbb{Z}}| \cdot \frac{\mathcal{C}_{\mathcal{X}_j}}{q}$$

$$= \begin{cases} 0 & \text{, if } \alpha = 0, \\ \geqslant \frac{\mathcal{C}_{\mathcal{X}_j}}{q} & \text{, if } \alpha \neq 0. \end{cases}$$

□

If the ratio of the attack step costs is irrational, lattice points appear with increasing frequency eventually positioning infinitely close to each other. In real life we can expect the costs to be rational (it would be difficult to estimate an irrational value for the cost parameter) and for this reason the above mentioned bound exists in the practical cases.

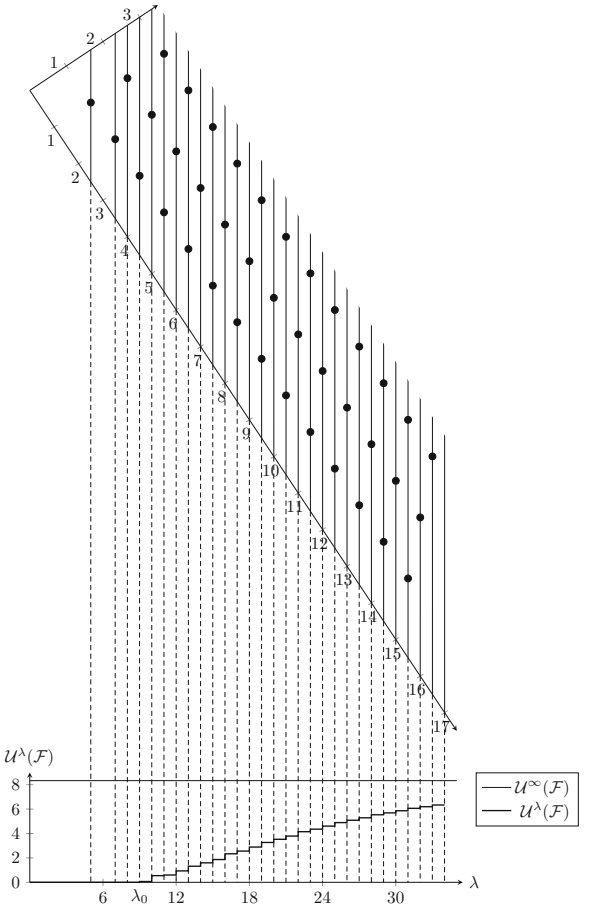

Fig. 3. Projections of the lattice points in the two-dimensional space into the one-dimensional space

Atomic OR Case

In the case of an atomic OR game in order to win it is sufficient that any of the two attack steps, $\mathcal{X} = \{\mathcal{X}_i, \mathcal{X}_j\}$ succeeds. The initial state of the game is $\langle \mathcal{X}_i \vee \mathcal{X}_j, \lambda \rangle$ and the subset of available attack steps to launch is $\{\mathcal{X}_i, \mathcal{X}_j\}$. In each state of the game the player may choose to launch any attack step from

the subset of available attack steps, or to discontinue playing. The attacker launches an attack step $\mathcal{X}_k$ from this set. If $\mathcal{X}_k$ succeeded the game moves into the state $\langle \mathbf{1}, \lambda - \mathcal{C}_k \rangle$, where $\mathcal{C}_k$ is the cost of the launched attack step, and the player has won the game. If the attack has failed, the game moves into the state $\langle \mathcal{X}_i \vee \mathcal{X}_j, \lambda - \mathcal{C}_k \rangle$ and the game goes on while $\mathcal{E}_k \leqslant \lambda$. At some point the current λ will reduce the set of available attacks to one (cheapest) attack, and eventually, the set of possible attacks becomes an empty set. Upon reaching the state in which $\mathcal{E}_k > \lambda$ and the Boolean function of the game has not been satisfied – the player has lost the game.

Adversarial utility may be expressed in the form of the relation (4):

$$\mathcal{U}^{\lambda}(\mathcal{X}_i \vee \mathcal{X}_j) = \max \begin{cases} 0 \ , \\ \mathcal{U}(\mathcal{X}_i) + (1 - p_{\mathcal{X}_i})\, \mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_i}}(\mathcal{X}_i \vee \mathcal{X}_j) \ , \\ \mathcal{U}(\mathcal{X}_j) + (1 - p_{\mathcal{X}_j})\, \mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_j}}(\mathcal{X}_i \vee \mathcal{X}_j) \ . \end{cases} \tag{4}$$

In certain cases under certain conditions the optimal strategy in the atomic OR case is non-adaptive and suggests to repeat one of the attacks independently of the current state of the game. We will bring an example of such a case.

Theorem 2. *If the costs of the attacks are equal, the attack having greater success probability will be best to try in every state of the game.*

Proof. Assume that $\mathcal{C}_{\mathcal{X}_i} = \mathcal{C}_{\mathcal{X}_j} = \mathcal{C}$. The utility of the game may be expressed in the form of

$$\mathcal{U}^{\lambda}(\mathcal{X}_i \vee \mathcal{X}_j) = \max \begin{cases} 0 \ , \\ \mathcal{U}(\mathcal{X}_i) + (1 - p_{\mathcal{X}_i}) \cdot \mathcal{U}^{\lambda - \mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \ , \\ \mathcal{U}(\mathcal{X}_j) + (1 - p_{\mathcal{X}_j}) \cdot \mathcal{U}^{\lambda - \mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \ . \end{cases}$$

Optimal strategy will suggest to try attack $\mathcal{X}_i$ if

$$\mathcal{U}(\mathcal{X}_i) + (1 - p_{\mathcal{X}_i}) \cdot \mathcal{U}^{\lambda - \mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) > \mathcal{U}(\mathcal{X}_j) + (1 - p_{\mathcal{X}_j}) \cdot \mathcal{U}^{\lambda - \mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \tag{5}$$

Solving inequality (5) we reach condition $p_{\mathcal{X}_i} > p_{\mathcal{X}_j}$. □

Algorithm 4.1 outlines the recursive procedure to calculate maximal adversarial utility in the atomic OR game given budget λ according to (4).

We show how the best move changes in the atomic OR game, depending on the current budget λ demonstrating it by several examples:

The first example (Fig. 4) shows that the best move bounces between the two attack steps when the budget is rather small, and sticks to one attack step later on. By $\emptyset$ we mean that the best move is not to start attacking at all.

The second example (Fig. 5) demonstrates the case when both of the attack steps are equally good when the budget is rather small and thus there is no difference for the attacker whether to launch attack step $\mathcal{X}_i$ or to launch attack step $\mathcal{X}_j$. But when the budget increases, the adversary has a clear preference for

Algorithm 4.1. Maximal utility of the atomic OR case with the given budget

Input: Attack step $\mathcal{X}_i$ cost *i_cost*
Input: Attack step $\mathcal{X}_i$ probability *i_pr*
Input: Attack step $\mathcal{X}_j$ cost *j_cost*
Input: Attack step $\mathcal{X}_j$ probability *j_pr*
Input: Prize of the game *prize*
Input: Budget *budget*
Output: Maximal adversarial utility value (a real number)

```
Procedure AtomicOr (i_cost, i_pr, j_cost, j_pr, prize, budget)
if budget is less than i_cost and j_cost then
    return (0)
i_utility := -i_cost + i_pr · prize
j_utility := -j_cost + j_pr · prize
if budget is greater than i_cost then
    u_i = i_utility + (1-i_pr) · AtomicOr (i_cost, i_pr, j_cost, J_pr, prize,
    budget-i_cost)
    if u_i is negative then
        u_i := 0
if budget is greater than j_cost then
    u_j = j_utility + (1-j_pr) · AtomicOr (i_cost, i_pr, j_cost, j_pr, prize,
    budget-j_cost)
    if u_j is negative then
        u_j := 0
if u_i is not less than u_j then
    maximal_utility := u_i
else
    maximal_utility := u_j
return (maximal_utility)
```

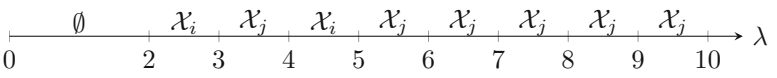

Fig. 4. Atomic OR case with parameters $\mathcal{C}_{\mathcal{X}_i} = 2, p_{\mathcal{X}_i} = 0.3, \mathcal{C}_{\mathcal{X}_j} = 3, p_{\mathcal{X}_j} = 0.48, Prize = 30$

one attack over the other one. By = we mean that launching attack step $\mathcal{X}_i$ is as good as launching attack step $\mathcal{X}_j$.

The third example (Fig. 6) demonstrates the case when the costs of the attacks are irrational, but their relation may be expressed in terms of a fraction of rational numbers. It can be seen that the best move to undertake in a certain state of the game between attack steps $\mathcal{X}_i$ and $\mathcal{X}_j$.

The next example (Fig. 7) demonstrates that there are cases where the optimal strategy is non-adaptive and iterates one single attack step $\mathcal{X}_j$.

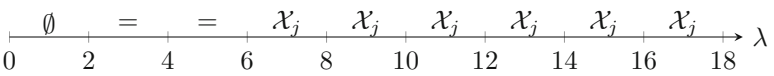

Fig. 5. Atomic OR case with parameters $\mathcal{C}_{\mathcal{X}_i} = 2, p_{\mathcal{X}_i} = 0.05, \mathcal{C}_{\mathcal{X}_j} = 6, p_{\mathcal{X}_j} = 0.9, Prize = 30$

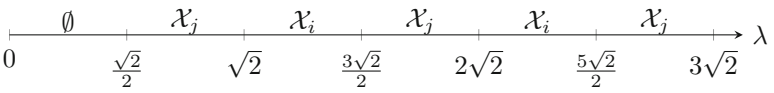

Fig. 6. Atomic OR case with parameters $\mathcal{C}_{\mathcal{X}_i} = \sqrt{2}, p_{\mathcal{X}_i} = 0.8, \mathcal{C}_{\mathcal{X}_j} = \frac{\sqrt{2}}{2}, p_{\mathcal{X}_j} = 0.45, Prize = 30$

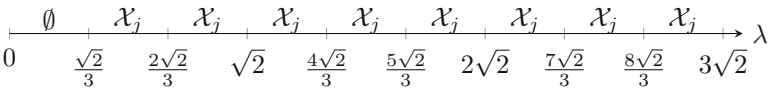

Fig. 7. Atomic OR case with parameters $\mathcal{C}_{\mathcal{X}_i} = \sqrt{2}, p_{\mathcal{X}_i} = 0.1, \mathcal{C}_{\mathcal{X}_j} = \frac{\sqrt{2}}{3}, p_{\mathcal{X}_j} = 0.38, Prize = 30$

Comparison with the Improved Failure-Free Model

We will show that the case when the improved failure-free model analysis result states that the system is *insecure*, while the budgeted model result states that the system is *secure* is impossible. Lets consider adversarial budget $\mathcal{I}$ for which the following inequalities hold:

$$\mathcal{U}^{\mathcal{I}}(\mathcal{X}_i \vee \mathcal{X}_j) > 0 \ , \tag{6}$$
$$\mathcal{U}^{\mathcal{I}-\mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \leqslant 0 \ , \tag{7}$$

where $\mathcal{C}$ is the cost of any of the atomic attacks. Assuming $\mathcal{I}$ is greater than the costs of attacks $\mathcal{X}_i$ and $\mathcal{X}_j$:

$$\mathcal{U}^{\mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \leqslant 0 \ . \tag{8}$$

Let $\mathcal{X}_k$ with cost $\mathcal{C}$ and probability p be the optimal move in the considered state of the game. In this case:

$$\mathcal{U}^{\mathcal{I}}(\mathcal{X}_i \vee \mathcal{X}_j) = \mathcal{U}^{\mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) + (1-p) \cdot \mathcal{U}^{\mathcal{I}-\mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \ . \tag{9}$$

As $\mathcal{U}^{\mathcal{I}-\mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \leqslant 0$ by (7) and $\mathcal{U}^{\mathcal{C}}(\mathcal{X}_i \vee \mathcal{X}_j) \leqslant 0$ by (8), it contradicts with the initial assumption $\mathcal{U}^{\mathcal{I}}(\mathcal{X}_i \vee \mathcal{X}_j) > 0$. Thus it seems that there is no point in limiting adversarial budget in the elementary OR case.

Atomic AND Case

In the case of atomic AND game in the initial state of the game the adversary has to choose either to launch the attack step $\mathcal{X}_i$, or to launch $\mathcal{X}_j$ or not to start

playing. If the adversary has chosen to launch attack $\mathcal{X}_i$ and it has failed, the game moves into the state $\langle \mathcal{X}_i \wedge \mathcal{X}_j,\ \lambda - \mathcal{C}_{\mathcal{X}_i} \rangle$. If $\mathcal{X}_i$ succeeded, the game moves into the state $\langle \mathcal{X}_i \wedge \mathcal{X}_j|_{\mathcal{X}_i=1},\ \lambda - \mathcal{C}_{\mathcal{X}_i} \rangle$ which is identical to $\langle \mathcal{X}_j,\ \lambda - \mathcal{C}_{\mathcal{X}_i} \rangle$. In this case, the attacker has the following choices: either to launch the remaining attack $\mathcal{X}_j$ (if λ is sufficient for it), or to discontinue playing the game. If $\mathcal{X}_j$ succeeds, the game moves into the state $\left\langle \mathbf{1},\ \lambda - \mathcal{C}_{\mathcal{X}_i} - \mathcal{C}_{\mathcal{X}_j} \right\rangle$ and the adversary has won the game. In case $\mathcal{X}_j$ fails, the game moves into the state $\left\langle \mathcal{X}_j,\ \lambda - \mathcal{C}_{\mathcal{X}_i} - \mathcal{C}_{\mathcal{X}_j} \right\rangle$ and the game continues until the budget λ is sufficient to continue playing. Adversarial utility may be expressed in the form of the relation (10).

$$\mathcal{U}^{\lambda}(\mathcal{X}_i \wedge \mathcal{X}_j) = \max \begin{cases} 0 \\ -\mathcal{C}_{\mathcal{X}_i} + p_{\mathcal{X}_i} \mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_i}}(\mathcal{X}_j) + (1 - p_{\mathcal{X}_i})\, \mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_i}}(\mathcal{X}_i \wedge \mathcal{X}_j) \\ -\mathcal{C}_{\mathcal{X}_j} + p_{\mathcal{X}_j} \mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_j}}(\mathcal{X}_i) + (1 - p_{\mathcal{X}_j})\, \mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_j}}(\mathcal{X}_i \wedge \mathcal{X}_j) \end{cases} \tag{10}$$

where (according to (2)):

$$\mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_i}}(\mathcal{X}_j) = \mathcal{U}^{\infty}(\mathcal{X}_j) \left[1 - (1 - p_{\mathcal{X}_j})^{\left\lfloor \frac{\lambda - \mathcal{C}_{\mathcal{X}_i}}{\mathcal{C}_{\mathcal{X}_j}} \right\rfloor} \right],$$

$$\mathcal{U}^{\lambda - \mathcal{C}_{\mathcal{X}_j}}(\mathcal{X}_i) = \mathcal{U}^{\infty}(\mathcal{X}_i) \left[1 - (1 - p_{\mathcal{X}_i})^{\left\lfloor \frac{\lambda - \mathcal{C}_{\mathcal{X}_j}}{\mathcal{C}_{\mathcal{X}_i}} \right\rfloor} \right].$$

In the atomic AND game the positive utility may not be achieved immediately by the adversary. We call the minimal value of the adversarial budget, sufficient to achieve positive utility the adversarial utility *budget lower bound*, which can be computed as:

$$\lambda_0 = \min \begin{cases} 0\ , \\ \left[\log_{(1-p_{\mathcal{X}_j})} \left[1 - \frac{\mathcal{C}_{\mathcal{X}_i}}{p_{\mathcal{X}_i}\, \mathcal{U}^{\infty}(\mathcal{X}_j)} \right] \right] \cdot \mathcal{C}_{\mathcal{X}_j} + \mathcal{C}_{\mathcal{X}_i}\ , \\ \left[\log_{(1-p_{\mathcal{X}_i})} \left[1 - \frac{\mathcal{C}_{\mathcal{X}_j}}{p_{\mathcal{X}_j}\, \mathcal{U}^{\infty}(\mathcal{X}_i)} \right] \right] \cdot \mathcal{C}_{\mathcal{X}_i} + \mathcal{C}_{\mathcal{X}_j}\ . \end{cases} \tag{11}$$

Algorithm 4.2 outlines the recursive procedure to calculate maximal adversarial utility in the atomic AND game given budget λ according to (10).

We show how the best move changes in the atomic AND game, depending on the current budget λ demonstrating it by several examples

The first example (Fig. 8) shows that there are certain sets of parameters which make the adversary indifferent in whether to launch attack step $\mathcal{X}_i$ or attack step $\mathcal{X}_j$ in every state of the game.

The second example (Fig. 9) demonstrates the case when the best move bounces between attack step $\mathcal{X}_i$ and attack step $\mathcal{X}_j$. In some states of the game both of the attack steps are equally optimal to launch.

Algorithm 4.2. Maximal utility of the atomic AND case with the given budget

Input: Attack step $\mathcal{X}_i$ cost *i_cost*
Input: Attack step $\mathcal{X}_i$ probability *i_pr*
Input: Attack step $\mathcal{X}_j$ cost *j_cost*
Input: Attack step $\mathcal{X}_j$ probability *j_pr*
Input: Prize of the game *prize*
Input: Budget *budget*
Output: Maximal adversarial utility value (a real number)

```
Procedure AtomicAnd (i_cost, i_pr, j_cost, j_pr, prize, budget)
if budget is less than the sum of i_cost and j_cost then
    return (0)
i_inf := prize − i_cost / i_pr
j_inf := prize − j_cost / j_pr
i_rep := i_inf · [1 − (1 − j_pr)^⌊(budget-i_cost)/j_cost⌋]
j_rep := j_inf · [1 − (1 − i_pr)^⌊(budget-j_cost)/i_cost⌋]
ui = -i_cost + i_pr · j_rep + (1-i_pr) · AtomicAnd (i_cost, i_pr, j_cost, j_pr, prize,
budget-i_cost)
if ui is negative then
    ui := 0
uj = -j_cost + j_pr · i_rep + (1-j_pr) · AtomicAnd (i_cost, i_pr, j_cost, j_pr, prize,
budget-j_cost)
if uj is negative then
    uj := 0
if ui is not less than uj then
    maximal_utility := ui
else
    maximal_utility := uj
return (maximal_utility)
```

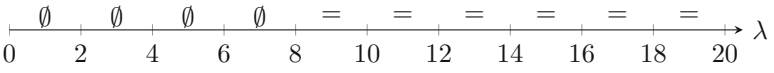

Fig. 8. Atomic AND case with parameters $\mathcal{C}_{\mathcal{X}_i} = 2, p_{\mathcal{X}_i} = 0.05, \mathcal{C}_{\mathcal{X}_j} = 6, p_{\mathcal{X}_j} = 0.9, Prize = 30$

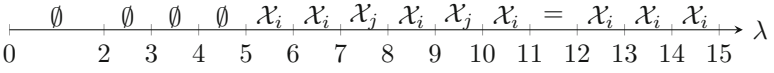

Fig. 9. Atomic AND case with parameters $\mathcal{C}_{\mathcal{X}_i} = 2, p_{\mathcal{X}_i} = 0.3, \mathcal{C}_{\mathcal{X}_j} = 3, p_{\mathcal{X}_j} = 0.48, Prize = 30$

The third example (Fig. 10) demonstrates the case when the costs of the attacks are irrational, but their relation may be expressed in terms of a fraction of rational numbers. It can be seen that with the given parameters optimal strategy will suggest to iterate attack step $\mathcal{X}_j$ and thus the optimal strategy is non-adaptive.

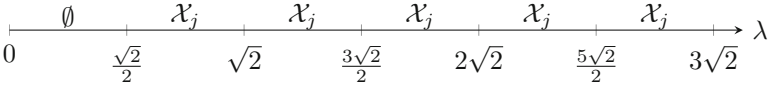

Fig. 10. Atomic AND case with parameters $\mathcal{C}_{\mathcal{X}_i} = \sqrt{2}, p_{\mathcal{X}_i} = 0.8, \mathcal{C}_{\mathcal{X}_j} = \frac{\sqrt{2}}{2}, p_{\mathcal{X}_j} = 0.45, Prize = 30$.

The next example (Fig. 11) demonstrates the case when the optimal strategy is adaptive and the best move to undertake in a certain state of the game alternates between attack step $\mathcal{X}_i$ and attack step $\mathcal{X}_j$.

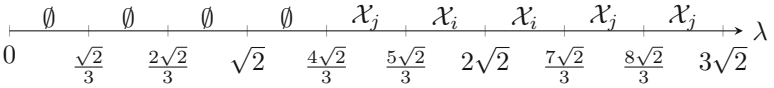

Fig. 11. Atomic AND case with parameters $\mathcal{C}_{\mathcal{X}_i} = \sqrt{2}, p_{\mathcal{X}_i} = 0.1, \mathcal{C}_{\mathcal{X}_j} = \frac{\sqrt{2}}{3}, p_{\mathcal{X}_j} = 0.38, Prize = 30$

Comparison with the Improved Failure-Free Model

We will investigate the case when the improved failure-free model analysis result states that the system is *insecure*, while the budgeted model result states that the system is *secure*. According to the improved failure-free model the adversarial utility $\mathcal{U}^{\infty}(\mathcal{X}_i \wedge \mathcal{X}_j) = \mathcal{P} - \frac{\mathcal{C}_{\mathcal{X}_i}}{p_{\mathcal{X}_i}} - \frac{\mathcal{C}_{\mathcal{X}_j}}{p_{\mathcal{X}_j}}$. The system is secure in case $\mathcal{P} \leqslant \frac{\mathcal{C}_{\mathcal{X}_i}}{p_{\mathcal{X}_i}} + \frac{\mathcal{C}_{\mathcal{X}_j}}{p_{\mathcal{X}_j}}$ and insecure in case $\mathcal{P} > \frac{\mathcal{C}_{\mathcal{X}_i}}{p_{\mathcal{X}_i}} + \frac{\mathcal{C}_{\mathcal{X}_j}}{p_{\mathcal{X}_j}}$.

Let the adversarial budget λ suffice to launch m attack steps in total and the adversarial strategy may be the one as shown in Fig. 12 and for the sake of simplicity lets assume that $\mathcal{C}_{\mathcal{X}_i} = \mathcal{C}_{\mathcal{X}_j} = \mathcal{C}$ and $p_{\mathcal{X}_i} = p_{\mathcal{X}_j} = p$.

Adversarial utility may in this case be computed as shown in (12).

$$\begin{aligned} \mathcal{U}^{m\times\mathcal{C}}(\mathcal{X}_i \wedge \mathcal{X}_j) &= \left[\mathcal{U}^{\infty}(\mathcal{X}_j) - \frac{\mathcal{C}}{p}\right]\left[1-(1-p)^{m-1}\right] - (m-1)(1-p)^{m-1}\left[p\,\mathcal{U}^{\infty}(\mathcal{X}_j)\right] \\ &= \left[\mathcal{P} - \frac{2\mathcal{C}}{p}\right]\left[1-(1-p)^{m-1}\right] - (m-1)(1-p)^{m-1}\left[p\,\mathcal{P} - \mathcal{C}\right] \end{aligned} \tag{12}$$

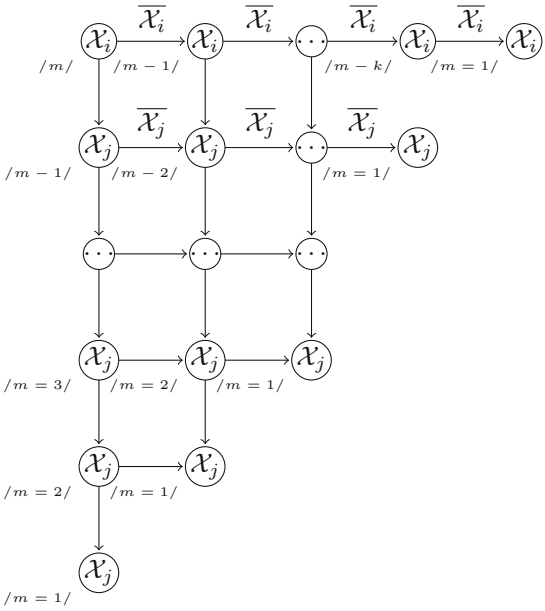

Fig. 12. An adaptive strategy consisting of two attack steps $\mathcal{X}_i$ and $\mathcal{X}_j$, with adversarial budget λ

According to the budgeted model the strategy is not profitable for an attacker, while the improved failure-free model states that the strategy is profitable if:

$$\frac{2\mathcal{C}}{p} < \mathcal{P} \leqslant \frac{2\mathcal{C}}{p} \cdot \frac{1-[1+\mathcal{C}(m-1)]\,(1-p)^{m-1}}{1-[1+p(m-1)]\,(1-p)^{m-1}} \quad . \tag{13}$$

Inequality (13) shows the interval for the value of prize within which the result of the limited budget model and result of the improved failure-free models differ. We will show what happens to the results of the analysis of both models in the broader view.

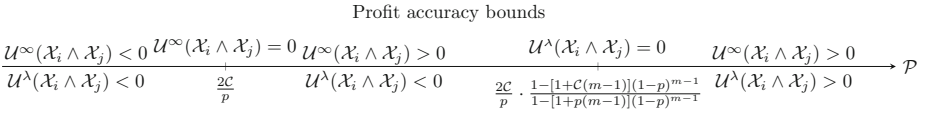

Fig. 13. Comparison of the improved failure-free model to the limited budget model

Thus, Fig. 13 shows that if prize is less than $\frac{2\mathcal{C}}{p}$ then the system is *secure* according to both models. If prize is greater than $\frac{2\mathcal{C}}{p} \cdot \frac{1-[1+\mathcal{C}(m-1)](1-p)^{m-1}}{1-[1+p(m-1)](1-p)^{m-1}}$ then the system is *insecure* according to both models. Only when the prize is between $\frac{2\mathcal{C}}{p}$ and $\frac{2\mathcal{C}}{p} \cdot \frac{1-[1+\mathcal{C}(m-1)](1-p)^{m-1}}{1-[1+p(m-1)](1-p)^{m-1}}$ the limited budget model may produce result different from the result of the improved failure-free model.

We have experimented with various parameters and observed that the prize interval (13) becomes negligibly small – less than 1 €. In practice, as a rule, it is practically impossible to estimate the value of the protected assets with the precision of less than €1 and for this reason we think that the limited budget model may produce false-positive results in case analysts are unable to estimate prize with required precision and this makes us give preference to the failure-free models which provides reliable utility upper bounds.

Table 1 demonstrates an example of such calculations. It can be seen that already with rather small increase in budget (approximately 3 times greater than the costs of the attack steps) the prize must be estimated with precision less than €1 in order to ensure reliability of the results.

The first column in a table describes the monetary budget of the adversary. The second column describes the interval for possible prize values, the column named span shows the length of such an interval. Precision is the length of uncertainty interval divided by mean value.

5 Conclusions and Future Research

We have analyzed the 3 kinds of elementary games – the single attack game, the atomic OR and the atomic AND, assuming that the adversarial budget is limited. In the result of limiting adversarial budget the model and computations become reasonably complex that makes it doubtful that this approach is applicable for real-life case analysis. Additionally, in case of atomic AND we have to be able to estimate the *prize* parameter quite precisely – if we fail to do that, the analysis results will be unreliable. In practice it is very hard to estimate the cost of an asset or information with the desired precision and thus is it doubtful if it is reasonable to face the complexities of budget limitations and its false positive results which might happen in the case of AND type games.

The improved failure-free model is, on the contrary, less complex and provides reliable upper bounds. Due to the fact that when the move fails the player finds himself in the very same instance of the game results in the existence of non-adaptive strategies in the set of optimal strategies of the game and the ordering of the attack steps in non-adaptive optimal strategies is irrelevant. In the model

Table 1. *Initial setting: Prize: €30 Cost: €2 Probability: 0.3*

Lambda (#)	$\mathcal{P}$ Domain (€)	Span (€)	Deviation (€)	Precision (%)
2	(13.(3), 28.(8)]	15.(5)	±7.(7)	0.518519
3	(13.(3), 22.4074]	9.07407	±4.537035	0.302469
4	(13.(3), 19.242]	5.9087	±2.95435	0.196957
5	(13.(3), 17.4047]	4.07139	±2.035695	0.135713
6	(13.(3), 16.232]	2.89863	±1.449315	0.0966211
7	(13.(3), 15.4386]	2.10531	±1.052655	0.0701772
8	(13.(3), 14.8816]	1.54822	±0.77411	0.0516073
9	(13.(3), 14.4806]	1.14723	±0.573615	0.038241

with budget limitations the subset of non-adaptive strategies exists in the set of all strategies. Non-adaptive strategies are relatively easy to derive and compute. One of the open questions is to figure out how well the most optimal strategy from the subset of non-adaptive strategies $\mathcal{U}^{\lambda}_{na}(\mathcal{G})$ might approximate the optimal strategy from the set of all possible strategies $\mathcal{U}^{\lambda}(\mathcal{G})$. If $\mathcal{U}^{\lambda}_{na}(\mathcal{G})$ provides pretty good approximation to $\mathcal{U}^{\lambda}(\mathcal{G})$, then there exists infinitely small α such that:

$$\mathcal{U}^{\lambda}_{na}(\mathcal{G}) \leqslant \mathcal{U}^{\lambda}(\mathcal{G}) \leqslant \alpha \cdot \mathcal{U}^{\lambda}_{na}(\mathcal{G}) \leqslant \mathcal{U}^{\infty}(\mathcal{G}) \ .$$

If this holds, it might enable calculation of acceptably precise result without facing the complexity and the computational overhead introduced by the precise utility calculation routines.

Secondly, it would be interesting to see when the optimal move in certain states of the game changes by bouncing between the two possible moves thus following some pattern. Additionally, to verify the hypothesis that this might happen in the theoretical case when the ratio of the costs of the move is irrational.

The bigger the adversarial budget λ is, the more adversarial utility approaches the utility upper bound in the improved failure-free model. Optimal strategies in the improved failure-free model are non-adaptive and do not depend on the ordering of the attack steps. In the case of big λ optimal strategies are likely to behave non-adaptively as well in the limited budget model. This means that optimal move in certain states of the game is likely to bounce changing from one attack to another, but with increase in λ the optimal move remains the same. It also means that the utility of various strategies, beginning with different moves, become closer to each other with the increase in λ and there should exist infinitely small δ such that

$$|\,\mathcal{U}^{\lambda}(\mathcal{S}_i) - \mathcal{U}^{\lambda}(\mathcal{S}_j)\,| \leqslant \delta \ ,$$

where $\mathcal{S}_i$ and $\mathcal{S}_j$ are the two strategies from the set of all strategies of the game.

The improved failure-free model provides reliable utility upper bounds, however this results in systems that might be over-secured. It has not been studied how much extra cost the upper-bound oriented methods cause. The assumption that the adversarial budget is limited is natural, as this is what happens in reality. Models assuming limited budget model the adversarial strategic decision making in a better way, which is more close to the one likely to be observed in real life and the research on the adaptive strategies with limited budget is an important research area in quantitative security analysis based on attack trees.

References

1. Buldas, A., Laud, P., Priisalu, J., Saarepera, M., Willemson, J.: Rational choice of security measures via multi-parameter attack trees. In: López, J. (ed.) CRITIS 2006. LNCS, vol. 4347, pp. 235–248. Springer, Heidelberg (2006)
2. Buldas, A., Lenin, A.: New efficient utility upper bounds for the fully adaptive model of attack trees. In: Das, S.K., Nita-Rotaru, C., Kantarcioglu, M. (eds.) GameSec 2013. LNCS, vol. 8252, pp. 192–205. Springer, Heidelberg (2013)

3. Buldas, A., Stepanenko, R.: Upper bounds for adversaries' utility in attack trees. In: Grossklags, J., Walrand, J. (eds.) GameSec 2012. LNCS, vol. 7638, pp. 98–117. Springer, Heidelberg (2012)
4. Jürgenson, A., Willemson, J.: Computing exact outcomes of multi-parameter attack trees. In: Meersman, R., Tari, Z. (eds.) OTM 2008, Part II. LNCS, vol. 5332, pp. 1036–1051. Springer, Heidelberg (2008)
5. Jürgenson, A., Willemson, J.: On fast and approximate attack tree computations. In: Kwak, J., Deng, R.H., Won, Y., Wang, G. (eds.) ISPEC 2010. LNCS, vol. 6047, pp. 56–66. Springer, Heidelberg (2010)
6. Mauw, S., Oostdijk, M.: Foundations of attack trees. In: Won, D., Kim, S. (eds.) ICISC 2005. LNCS, vol. 3935, pp. 186–198. Springer, Heidelberg (2006)
7. Schneier, B.: Attack trees. Dr. Dobb's Journal of Software Tools 24(12), 21–22, 24, 26, 28–29 (1999)