Algorithms for Fuzzy Attack & Fault Trees

Thi Kim Nhung Dang
EEMCS
University of Twente
Enschede, the Netherlands
t.k.n.dang@utwente.nl
ORCID 0000-0002-3235-5952

Milan Lopuhaä-Zwakenberg
EEMCS
University of Twente
Enschede, the Netherlands
m.a.lopuhaa@utwente.nl
ORCID 0000-0001-5687-854X

Mariëlle Stoelinga
EEMCS
University of Twente
Enschede, the Netherlands
m.i.a.stoelinga@utwente.nl
ORCID 0000-0001-6793-8165

Abstract—**Fault trees (FTs) and attack trees (ATs) are useful models for risk assessment for safety and security, respectively. Quantitative analysis of FTs and ATs formulates important KPIs such as the system unreliability for FTs, and the most likely and cheapest attacks for ATs. A key bottleneck in quantitative analysis is that the values are usually not known exactly, due to insufficient data and/or lack of knowledge. Fuzzy logic is a prominent framework to handle such uncertain values, with applications in numerous domains.**

Although several studies proposed fuzzy approaches to AT and FT analysis, none of them provided a firm definition of fuzzy metric values or generic algorithms for the computation of fuzzy metrics. Thus, we define a generic formulation for fuzzy metric values that applies to FT reliability, as well as to AT metrics that can be phrased in terms of semirings, which covers almost all existing metrics. In addition, we prove a modular decomposition theorem that yields a bottom-up algorithm to efficiently calculate the AT's/FT's fuzzy metric value.

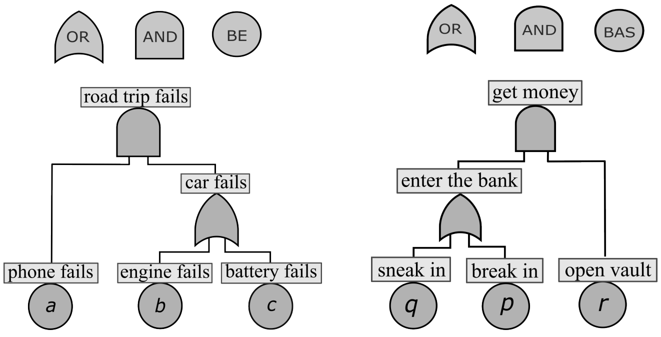
For FTs, this algorithm can be improved computationally by exploiting the concept of α-cuts, on which fuzzy arithmetic operations can efficiently be described using interval arithmetic. We illustrate our algorithm and its performance on synthetic FTs and the case study of a liquid storage tank. Overall, our work provides a framework to both express and calculate the uncertainty that is often present in safety and security risk assessment.

I. Introduction

a) Fault trees: Fault tree analysis (FTA) is a popular method in reliability engineering [1], [2]. It is widely used in industry to assess and improve the dependability of, amongst others, nuclear power plants, self-driving cars, and airplanes. FTA is recommended by several ISO standards and certification bodies, such as the Federal Aviation Administration.

FTs are a systematic, graphical tool that tells why systems fail. A FT breaks down system-level failures into its subcauses, until the root causes are found, represented in the leaves of the tree (*basic events*-BEs). The root of FTs is *the top level even*-TLE. *Intermediate events*-IEs are characterized by *gates*.

b) Attack trees: ATs are a popular tool for modeling and analyzing security risks. They provide a structural way to identify vulnerabilities in a system, by decomposing the attacker's goal into subgoals, down to basic attack steps that a malicious actor can take to reach said objective. Much like FTs, an AT consists of *basic attack steps* (BASes) representing atomic adversary actions, and *intermediate* AND/OR-gates whose activation depends on the activation of their children. The attacker's goal is to activate the root (top node).



(a) (b)

Fig. 1: A simple fault tree (a) and attack tree (b).

c) Quantitative analysis: In this paper, we focus on the tree-structured FTs/ATs i.e., trees without shared events, like the one in Fig. 1. For FTs, we focus on (fixed-time) system reliability, i.e., the probability for a system to fail within a fixed mission time. The system reliability is obtained by equipping each BE e with a failure probability p_e, from which the probability of the TLE p_{T} is computed. The reliability can be computed via a bottom up algorithm that propagates the probability values from the leaves to the top. For ATs we equip each BAS with time, probability, etc. for corresponding security metrics (fastest attack, most probable attack, etc.).

d) Fuzzy FTs/ATs: The key idea behind fuzzy FT/AT analysis is to no longer equip BEs/BASes with single values, but rather with their fuzzy variants. E.g., to compute the system reliability, equip each BE e not with a single probability p, but with a fuzzy number p. Our aim is to compute a fuzzy number for top level failure probability p_{T}. A fuzzy number x is a *membership function* $\mathsf{x}\colon \mathbb{R} \to [0,1]$ of y that assigns to each $y \in X$ the trust we have for the number x to be equal to y. If $\mathsf{x}[y] = 0$ we have no trust that this number is y; if $\mathsf{x}[y] = 0.9$, we are quite sure that the value can be y.

e) Limitations and obstacles: Due to their similarities, many approaches to fuzzy FTA can also be applied to ATs. A

This research has been partially funded by ERC Consolidator grant 864075 CAESAR and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 101008233.

common limitation of existing approaches to fuzzy FTs is that their mathematical formulation is not very precise. In addition, there are no efficient algorithms that calculate dependability metrics for fuzzy parameters. To the best of our knowledge, only approximations exist, and no bounds are given on how much the approximated results deviate from the exact results.

One obstacle in fuzzy FTA is that performing exact calculations for nonlinear operations is computationally expensive. A major problem is that many common mathematical operators result in fuzzy numbers that are not of the same shape as the operands [5], [4], [3]. E.g., if we multiply two triangular functions (via the canonical Zadeh extension), then the result is no longer triangular [4]. Some works [6], [5] do try to obtain results for fuzzy operations by assuming that the operators preserve the shape of the operands, but these assumptions hardly ever hold.

A second obstacle is that standard binary-decision diagram-based (BDD-based) algorithms cannot be applied directly to fuzzy numbers. Fuzzy extensions do not satisfy the distributivity laws that current BDD methods rely on.

Contributions Summarized our contributions are:

1) A rigorous definition of fuzzy unreliability metric and fuzzy security metrics;
2) A proof of modular decomposition theorem that yields a bottom-up algorithm to efficiently calculate the top fuzzy metric value;
3) A bottom-up algorithm for computing fuzzy unreliability in tree-like FTs based on α-cuts;
4) A counter example showing why a straight forward extension of BDD-based methods for reliability calculations (resp. security metric calculation) does not work for fuzzy FTs (resp. ATs);
5) Experiments show that the computation time of the algorithm based α-cuts is linear in FT size.

II. Fuzzy unreliability

Our approach First, we present a clear, mathematically rigorous definition of the fuzzy unreliability metric. The definition is valid for general fuzzy numbers, rather than specific types such as triangular numbers. The definition follows Zadeh's extension principle [7], a general approach to apply functions and arithmetic operations on sets to fuzzy numbers.

We then propose a bottom-up algorithm for calculating fuzzy unreliability metric for tree-structured FTs. During the calculation procedure, fuzzy attribution is discretised horizontally and saved as α-cut series. Arithmetic operations are performed on these α-cut series representing fuzzy numbers. Output of the algorithm is an α-cut series approximation of a fuzzy number. This approximate computational technique works for fuzzy numbers that can be expressed as α-cut interval and is applicable when performing operations on fuzzy numbers of different types.

III. Fuzzy metrics for attack trees

Our approach Our first contribution is a clear, mathematically rigorous definition of fuzzy AT metrics. Because these are defined for general fuzzy numbers, rather than specific subtypes such as triangular fuzzy numbers, we sidestep the problem that these subtypes are not preserved under AT metric operations; instead, our definition works for the generic semiring framework defined in [8]. We show that our definition naturally follows from Zadeh's extension principle [7], a general approach for extending functions to fuzzy numbers.

Having defined fuzzy AT metrics, we furthermore develop a linear-time, bottom-up algorithm for calculating them for tree-shaped ATs. We show the validity of this algorithm by showing that fuzzy AT metrics are susceptible to *modular analysis*: when an AT has a module, i.e., a minimally connected subcomponent, a fuzzy metric can be computed by first calculating the metric for the module and then for its complement. When an AT has many modules, this substantially speeds up computation. When an AT is tree-shaped, every node is a module, proving the validity of the algorithm.

IV. Conclusion and future work

In this paper, we define a mathematical formulation for deriving fuzzy unreliability values for FTs (resp. security metric values for ATs). The definitions are explicit and generic for general fuzzy attribution. We also introduce an efficient algorithm to calculate FT fuzzy unreliability metric and security metrics. The algorithm works for tree-like structure models with any type of fuzzy attribute that can be expressed as α-cut intervals. Experiments on the practical model show that the algorithm provides a considerably precise solution and thus preserves the nonlinearity of the resulting fuzzy number.

In the future, we want to develop an algorithm for fuzzy unreliability (resp. security metrics) computation on DAG FTs (resp. ATs). For this aim, we employ the BDD method that is often used for the quantitative computation of directed acyclic graphs. Our approach is to use α-cuts method on BDD. To do this, we need to ensure the semiring property on each α-cut of ATs and the independence of fuzzy probability on α-cuts of FTs.

References

[1] Stamatelatos, M., Vesely, W., Dugan, J., Fragola, J., Minarick, J., Railsback, J.: *Fault tree handbook with aerospace applications* (2002).

[2] Ruijters, E., Stoelinga, M.: *Fault tree analysis: A survey of the state-of-the-art in modeling, analysis and tools*. Computer Science Review (2015).

[3] Basiura, B., Duda, J., Gaweł, B., Opiła, J., Pełech-Pilichowski, T., Rebiasz, B., Skalna, I.: *Fuzzy Numbers*, pp. 1–26. Springer Inter. Publishing, Cham (2015).

[4] Liang, G.S., Wang, M.J.J.: *Fuzzy fault-tree analysis using failure possibility*. Microelectronics Reliability 33(4), 583–597 (1993).

[5] Tanaka, H., Fan, L.T., Lai, F.S., Toguchi, K.: *Fault-tree analysis by fuzzy probability*. IEEE Transactions on Reliability R-32(5), 453–457 (1983).

[6] Peng, Z., Xiaodong, M., Zongrun, Y., Zhaoxiang, Y.: *An approach of fault diagnosis for system based on fuzzy fault tree*. In: Proceedings of MMIT '08, IEEE Computer Society, USA (2009).

[7] Zadeh, L.: *Fuzzy sets. Information and Control* 8(3), 338–353 (1965).

[8] Lopuhaä-Zwakenberg, M., Budde, C.E., Stoelinga, M.: *Efficient and generic algorithms for quantitative attack tree analysis*. IEEE TDSC pp. 1-18 (2022).