UAI-2014

Conference on Uncertainty in Artificial Intelligence
July 23-27, 2014, Quebec City, Canada

Robert Goldman

Logout

Select Your Role: Author Go to Console

Manage Submissions | **View Conference Status** | **Manage Notes**

View Author Feedback For Paper

Paper ID	305
Title	Qualitative Probability for Intrusion Detection

	Question	Response
1	Author Feedback	*** Reviewer 1** **** Anomaly detection** **The paper describes an approach to fuse reports from IDSes; it does not do anomaly detection. MIFD fuses IDS reports from both anomaly- and signature-based IDSes. Perhaps confusion arises from System Z+'s use of the term "surprise" for its measure, which goes up as likelihood goes down.** **** Code and data are not available** **The data will be made available on the web. The code could be made available under limited license for research purposes, making reproduction and comparison feasible.** **** Comparison** **While this would be desirable, existing IDS fusion techniques do not share an input format or output definition. Most simply cluster and do not categorize hypotheses by posterior likelihood. However, it would be simple for other researchers to adapt their systems to our data sets: our synthetic reports would be simple to translate into other input formats.** *** Reviewer 11** **** Clarifications** ***** Three sensors** **You'd noted in the review that we "used three sensors for possible fusion." That's not exactly right --- although we do use a ratio of three sensors detecting each attack in most experiments, we vary that ratio in the first experiment.** ***** Removing event hypotheses and sensor reports** **We'd intended this remark as something of an aside, since (as the paper states) we are not actually doing this cleanup in the system under experimentation.** **The volume of data which IDSs encounter necessitates some sort of garbage collection. You are correct that the timing of such clean up must be carefully considered. In the full system, hypotheses are only purged after an interval since receipt of the last related IDS**

report. All reports and hypotheses are archived in a database.

It would probably be best to simply cut this minor aside from the paper, since garbage-collection plays no role in these experiments.

** Justification for choice of parameter settings

In all cases, the initial settings for the configuration parameters are both typical values for an IDS, and consistent with Z+'s assumptions. The experiments vary these values in ways which we anticipate would be worse for MIFD's performance, to examine our expected performance both under typical conditions, and under less typical conditions approaching worst-case.

** Relation to boosting

Boosting does provide an alternative method for fusion, but is not appropriate to IDS fusion. Boosting is based on learning, but IDS fusion problems do not admit use of ML: we do not get labeled data of attacks, nor do we get reference data showing systems operating without attacks. We will add a citation to papers about the failure of ML for IDS. These challenges (see [Sommer&Paxson,2010;Gates&Taylor,2006] on the challenges of ML in IDS, full cites available upon request) account for our adoption of a qualitative, non-adaptive framework. Also note that different IDSes do not share a single "ontology" of events; part of the function of MIFD's clustering is to align reports with different frames of reference.

** Other suggestions

Thank you for the many thoughtful suggestions for clarification. We will edit the text to address all of these issues.

* Reviewer 4

** Novelty, technical quality, and significance

We respectfully disagree with this review's judgment about the novelty of our work.

It is true that System Z+ is well-studied in the literature, and /proposals/ to apply it to inference problems are common. However, we reviewed the 250+ papers citing the Z+ AIJ paper on Google Scholar (We will make the list of citations available upon request), and found no other paper describing an application of Z+ to a real-world problem. Accordingly, we assert that studying the application, and more to the point, the range of applicability, of System Z+ is novel.

Further, in order to apply an approximation technique such as Z+, one must have a clear understanding of when it will work, when it will fail, and how it will degrade from one to the other. Z+ is based on an idealization of uncertain reasoning, and it is necessary to study how it will work when its simplifying assumptions are violated. Our experiments studied exactly this --- beginning with assumptions in line with both the particular application of IDS and with Z+, and then diverging from them --- not "testing for the sake of testing."

There are numerous useful points of comparison in the literature: Consider how naive Bayesian classification has been studied: Anecdotal experience that useful results were computed even

when violating independence assumptions led to more systematic studies of the integrity of Bayes classification as the independence failed. Heckerman and Horvitz's study of why confidence factors work is in a similar vein. Another point of comparison is big-O analysis: while it is of great utility, there are many cases where the constant factors do matter, and the idealization provides misleading results. Failure to investigate such cases would hamper computer science as a whole.

In this case System Z+ has been believed to be a useful approximation to real probabilities, and the novelty here is to examine the performance of Z+ as its assumptions are increasingly violated (with particular application to sensor fusion).

If we aren't willing to accept research that explores why a technique works or fails to work in practice, we doom applications work to be prescientific. Any single application can be made to work with a large enough investment of one-off labor: generalizing and validating requires follow-up.

Finally, we stress that our results are relevant to sensor fusion applications in general, not just IDS fusion.

We will improve the clarity of these introductory points in the final version of the paper.

**** Quality of writing**

Although it is difficult to address the non-specific claim of poor writing, our incorporation of the specific suggestions from the above reviews may address this reviewer's concerns.