Journal of Physical Security 4(1), 1-9 (2010)

Formal Evaluation of a Majority Voting Concept to Improve the Dependability of Multiple Technology Sensors

Francesco Flammini

Vice-Chair, IEEE Computer Society Italy
francesco.flammini@ieee.org

Abstract. Finding a good trade-off among the probability of detection (POD), the false alarm rate (FAR) and the reliability of detectors is a very important task in physical security system design. Existing solutions try to achieve this aim either by using the most advanced technologies or by combining basic sensors in logical OR/AND relations. However, these approaches are either not cost-effective or they do not allow for the necessary flexibility to obtain the right balance. In this paper I propose a majority voting scheme for multiple technology detectors which I evaluate using stochastic modelling techniques. This solution has the major advantages that it permits good overall dependability while using low-cost detectors, and also enables a precise fine tuning of POD and FAR parameters. To the best of my knowledge, no similar system has been studied in depth in the research literature. I provide a set of results which clearly show the advantages of the proposed approach.

Keywords: physical security, intrusion detection, stochastic modelling, quantitative evaluation, diversity redundancy

1. Introduction

The importance of dependability in physical security systems is increasing as threats escalate, especially in applications related to critical infrastructure protection. One of the most important topics in this research field is the automatic decision fusion to support the task of security operators. In case of diverse redundancy of sensors, a correlation of basic events generated by independent sensors could be used to improve the dependability of alarm generation (see e.g. reference [3]). The aim of this paper is to provide a formal demonstration of this concept in the specific case of a basic majority vote. In particular, I will refer to a straightforward example of volumetric intrusion detectors (also known as "radars"); however, the results are general enough to be used with any sensor combination provided that diverse technologies (and/or detection criteria) are used. Throughout the paper, I will adopt the reference dependability taxonomy (including the concepts of reliability, availability, trustworthiness, survivability, etc.) provided in reference [2].

The usefulness of an intrusion detection system critically depends on its capability to distinguish an alarm condition initiated by an actual unauthorized intruder from either a false alarm, or from an alarm failure caused by noise, atmospheric disturbance, animals, alterations in the placement and state of operability of protected area equipment, and change in actual versus the design range, among other things. For instance, ultrasonic intrusion detection systems are not only subject to false alarms caused by drafts and air movements, but can also be bothered by ultrasonic noises generated by, for example, bells and hissing. Moreover, they are also subject to alarm failures due to changes from nominal range occasioned by variations in the ultrasonic propagation medium.[7] Similarly, microwave intrusion detection systems produce false alarms in response to water movement in plastic pipes, energy received from beyond the protected area due to wall and window penetration, and unwanted reflections, among other things. However, the sources that adversely affect the performance of ultrasonic detection systems are in general different from those that

give rise to false alarms and failures of alarm for microwave detection systems, and conversely. Thus, while drafts, air movements, and ultrasonic noises adversely affect ultrasonic system performance, none of them poses a significant detection problem for microwave systems. And while water movement in plastic pipes, wall or window penetration, and reflections give rise to false alarms for microwave intrusion detection systems, such events are not obstacles to accurate detection for ultrasonic systems. Hence a variety of technologies have been used simultaneously to more reliably detect the presence of an intruder in region under surveillance. Microwave, ultrasonic, photoelectric and passive infrared [10] are some of the more common technologies in current use [8]. Each has certain unique advantages and disadvantages which makes it more or less desirable for a particular environment or application. None is fool-proof, and all are subject to the ever-annoying false alarm. Multiple technology intruder detection systems in AND-type correlation have proven to be substantially more reliable and less susceptible to false alarming than single technology systems, with "common cause" false alarms happening in very rare circumstances (if installed using the right criteria). However, besides the higher cost, it is rarely noticed that AND-type correlations have a negative impact on availability, detection probability and the possibility of spoofing. (It is enough to spoof one of the sensors.) In contrast, OR-type correlations have some advantages (e.g., POD) but also considerable disadvantages, including an unacceptably high rate of false alarms.

The solution proposed in this paper aims at finding a good compromise between those contrasting requirements by adopting a '2 out of 3' ('2oo3') majority voting concept. See Figure 1. It will be shown through the analytical evaluation of a formal stochastic model that this approach features several advantages with respect to alternate techniques, including the AND-type correlations widespread in multiple technology sensors. Results will be provided as quantitative parameters, i.e. non-functional dependability attributes. Among other things, significant advantages will be demonstrated for the POD, in the resistance to spoofing, and in the higher survivability, with only a modest disadvantage in cost and FAR compared to AND-type correlations. The results are general enough to be valid in any multiple technology sensor correlation, where the so called "diverse redundancy" is adopted (possibly also at the software levels). It should be noticed that the concept of 'majority voting' is also employed in safety-related fields for different purposes, including an increase in safety and availability.[5]

This paper is organized as follows: Section 2 provides some introductory definitions and theoretical results about AND-type, OR-type, and majority-voting event correlation. Section 3 introduces the reference model used for the analysis, the choice of parameters, and the evaluation results, which are discussed in detail. Section 4 summarizes the impact of the results and draws conclusions.

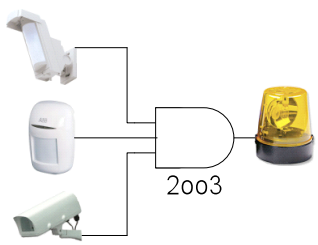

Figure 1. A schematic of the majority voting scheme for alarm correlation.

2. Basic definitions and description of the approach

The majority voting approach presented in this paper is based on the assumption that diverse technologies feature false alarms of differing natures, which is generally true

(as also stated in the previous section). More formally, the following two equations must hold for conditional probabilities[1]:

$$P\,(\text{false alarm from 1} \mid \text{false alarm from 2}) \approx P\,(\text{false alarm from 1})$$

$$P\,(\text{false alarm from 2} \mid \text{false alarm from 1}) \approx P\,(\text{false alarm from 2})$$

This allows obtaining some interesting theoretical results (see also [8]). If I define:

- P^1_F as the probability of false alarm of sensor 1
- P^2_F as the probability of false alarm of sensor 2

In case of diversity, I can assume that such probabilities for the two detection devices are (almost totally) independent from each other, therefore obtaining for the "AND" correlation the following result:

$$P^{1\ \mathrm{AND}\ 2}{}_F \approx P^1_F \cdot P^2_F$$

In the realistic assumption that[2]:

- $P^1_F << 1$
- $P^2_F << 1$

Then I can state that:

$$P^{1\ \mathrm{AND}\ 2}{}_F << P^1_F$$

$$P^{1\ \mathrm{AND}\ 2}{}_F << P^2_F$$

In other words, the resulting FAR for the 'AND' correlation is substantially less than the FAR of the single sensors.

Similarly, it is possible to demonstrate that the probability of detection is negatively affected. In fact, if I define:

- P^1_D as the probability of detection of sensor 1
- P^2_D as the probability of detection of sensor 2

Then I can state (basing on the diversity assumption):

$$P^{1\ \mathrm{AND}\ 2}{}_D \approx P^1_D \cdot P^2_D$$

Hence the result is that:

$$P^{1\ \mathrm{AND}\ 2}{}_D < P^1_D$$

$$P^{1\ \mathrm{AND}\ 2}{}_D < P^2_D$$

However, since it is realistic to assume[3]:

- $P^1_D <\approx 1$
- $P^2_D <\approx 1$

then the loss in POD is not as important as the gain in FAR reduction, so the trade-off is generally advantageous (as demonstrated by the results provided in the following section). The opposite holds true for the 'OR' correlation, which can be only advantageous when the priority is on event detection, and false alarms can be tolerated. This means that, generally speaking, AND-type and OR-type correlations feature contrasting specifications which do not allow for a fine tuning of the POD/FAR ratio or other dependability attributes (as it will be shown in the following).

---

[1] The '|' symbols stands for "given that", while the '≈' symbol means "almost equal".
[2] The '<<' symbols stands for "much minor than".
[3] The symbol '<≈' means "minor than but almost equal to" or rather "not much minor than".

Now, let me formally define the majority voting scheme proposed in this paper. A Boolean variable X_{2oo2} is said to be related to other 3 Boolean variables X_1, X_2 and X_3 through a '2 out of 3' correlation logic when the following formula holds[4]:

$$X_{2oo2} = (X_1 \wedge X_2) \vee (X_1 \wedge X_3) \vee (X_2 \wedge X_3)$$

This function can be specified using the so-called "truth table" shown in Table 1.

LOGIC VALUE 1	LOGIC VALUE 2	LOGIC VALUE 3	2OO3 LOGIC
FALSE	FALSE	FALSE	FALSE
FALSE	FALSE	TRUE	FALSE
FALSE	TRUE	FALSE	FALSE
FALSE	TRUE	TRUE	TRUE
TRUE	FALSE	FALSE	FALSE
TRUE	FALSE	TRUE	TRUE
TRUE	TRUE	FALSE	TRUE
TRUE	TRUE	TRUE	TRUE

Table 1. Description of the '2oo3' logic function.

In the case of sensors based on different detection technologies, the '2oo3' logic allows us to:

- Generate an alarm only when at least two of the three sensors agree on event detection, thus intuitively improving the detection reliability and decrease the false alarm rate of a single sensor.
- Increase the availability, mean useful life, and/or the survivability of the detector since it can continue working in a dual or even single technology configuration (with reduced performance) when, respectively, one or two sensors stop working. This allows for a fail-safe or fall-back mechanism until the failed sensor is replaced (assuming the electrical connections are designed not to feature a "stuck-at-alarm" on failed sensors).
- Reduce the likely success of tampering, blinding, or shielding attempts which could spoof single or (even more easily) dual technology sensors used in AND configurations (by far the most widespread).

Therefore, the '2oo3' logic can potentially improve the overall system dependability in terms of several relevant parameters, allowing us to achieve a set of non-functional (i.e. quantitative) specifications which would be impossible or very expensive to obtain using a single technology. This statement will be formally demonstrated in the following section using a model-based evaluation approach.

The implementation of the '2oo3' logic circuit is straightforward and introduces very little extra cost. An abstract scheme (and a comparison with more traditional designs) using an electrical representation is depicted in

Figure 2, where the symbols labelled with A, B and C represent 'switches' or 'circuit breakers' [1]. The actual design depends on other factors, including the type of contacts (e.g. voltage free or not, normally open/closed, etc.) and the latency of the alarm signals. More complex designs could also include the possibility of detecting and excluding a faulty sensor when the "disagreement rate" is above a certain threshold (i.e., it is generating too many false alarms).

Finally, please note that even though the independence assumption regarding false alarms is very important to ensure stochastic independence in event detection, in he next section, I will also evaluate the impact of slight dependencies on the occurrence of false alarms.

[4] ' $\wedge$ ' is the logic symbol of the 'AND' operator, while ' $\vee$ ' represents the 'OR' operator.

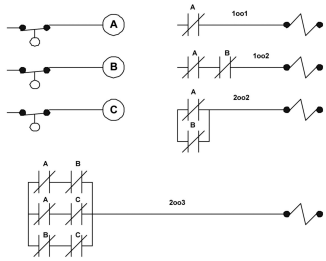

Figure 2. Electrical representation of voting schemes.

3. Modelling, evaluation and discussion of the results

In this section, I report the results of the quantitative evaluation of the proposed approach using a formal (or "analytical") stochastic modelling method based on Bayesian Networks (BN).[4] Bayesian Networks are a well known method for probabilistically modelling uncertainty in many scientific or engineering problems. With respect to other possible approaches, including the ones based on extensions of the Fault Tree formalism, BN allows us to express any kind of dependence among stochastic variables, to obtain more compact models, and to avoid the use of state-based modelling techniques when they are not strictly necessary (as in this case).

As for the sensor related data, I have checked some prior work on detection reliability evaluation, but none of them looked general enough to be considered as a reference source, since the results are highly dependant on the specific technologies, manufacturers, and applications (see e.g. reference [8]). Therefore, I have merged data coming form different papers and component data-sheets, and also from my testing experience only to get some "order of magnitude" estimates for POD, FAR and availability indices, which have been used as parameters to populate the BN models used for the analyses (as reported in Table 2); in other words, I have not used real data but I have used realistic pseudo-data. The conclusions which I will draw are valid regardless of the specific values of the parameters.

As for the support modelling and evaluation tool, I have used Netica by Norsys [9]. The Conditional Probability Table (CPT) for the '2oo3' connection has been directly derived from Table 1. I have chosen three example single technologies which vary in their overall dependability and cost, from an 'entry-level' (technology 3) to a 'top-level' (technology 1), passing through an "average-level" (technology 2). The AND-type (i.e. '2oo2') correlations have been evaluated both for 1-2 (best) and 2-3 (worst) combinations. The OR-type correlations (e.g. '1oo2' or '1oo3') have not been taken into account in the analysis because I have shown that their advantages are rather limited.

Figure 3 reports the results of the analysis regarding the FAR parameter in the complete independence assumption, while Figure 4 shows the effect of a slight correlation on the same parameter. The results clearly show that a little correlation (less than 20%) has negligible effects on the results. The results show that the lowest FAR is obtainable using a '2oo2' design (AND-type correlation); however a significant improvement (by a factor ranging from 2 to 16) over single technologies can be achieved by the '2oo3' design.

Figure 5 reports the results of POD evaluation. Here the best result (99.7%) is achieved by the '2oo3' design (with a significant advantage of over 2 points compared to the best '2oo2'), which slightly improves the POD of the best single technology, even using additional technologies which are not as good as the best one.

Figure 6 presents the results of the steady-state availability evaluation, which gives a measure of how much the system is "survivable", that is, able to remain operational (even in a degraded state, i.e. with reduced performance) without requiring a

maintenance intervention. In this case, the winner is '2oo3' with an availability of about '4 nines'[5], which is better than any single technology. Please note that any '2oo2' design significantly worsens this parameter, halving the availability value with respect to single sensors.

Figure 7 shows the results of "spoof rate" evaluation, the assumption here being that an intruder is able to spoof with a certain probability one or more technologies. The conservative assumption is that the best technology is also the hardest to spoof—which could be untrue. Nevertheless, the results show that, as intuition suggests, the '2oo2' design significantly worsens the resistance of detectors to spoofing by a factor ranging from approximately 1.5 to 3, which is difficult to achieve in practice. Instead, the '2oo3' approach reduces the success rate of spoofing attempts with respect to the best single technology (3.3% instead of 5%).

Finally, Table 2 summarizes the results obtained by the analyses, and compares them with original data for single technologies. The best results for each column (cost, availability, spoofing success rate, POD, and FAR) are highlighted in bold style, while the cells associated with the '2oo3' design are shaded in light grey. Regarding the cost, I have neglected the (small) overhead due to the correlation circuits.

It is clear that the '2oo3' design wins over the other technologies for all the parameters except cost and FAR, and is the only approach which always ensures better results with respect to the single technologies. In contrast, the '2oo2' approach provides inferior results with the exception of FAR, which can be significantly better with respect to any other design. In conclusion, considering the small cost increase of '2oo3' designs with respect to '2oo2' ones, the results clearly show that the '2oo3' approach allows advantageous trade-offs between dependability parameters required for detectors (or any other event-sensing devices). This makes the '2oo3' designs attractive for a wide range of physical security applications.

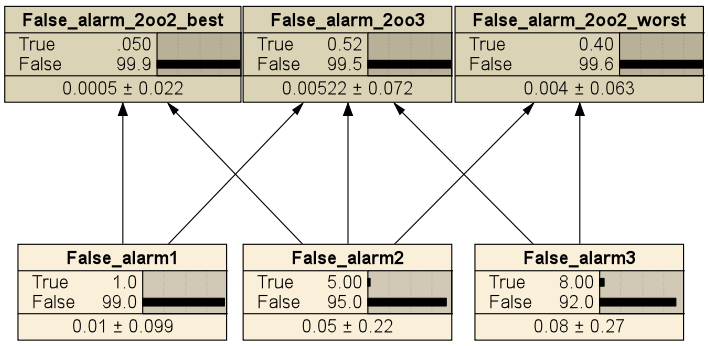

Figure 3. FAR evaluation of majority voting.

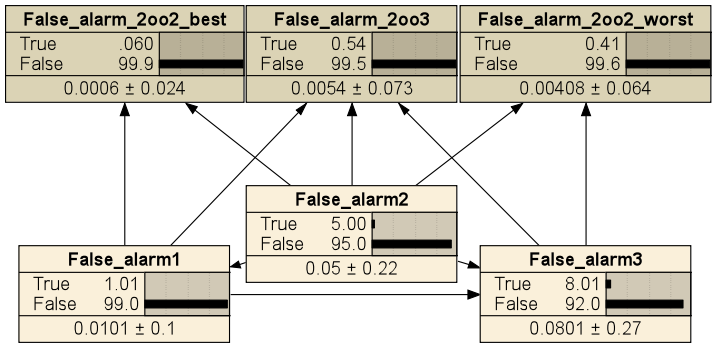

Figure 4. Effect of a slight correlation (10÷20%) on the false alarm rate.

[5] The expression '4 nines' means 0.9999 (or 99.99%).

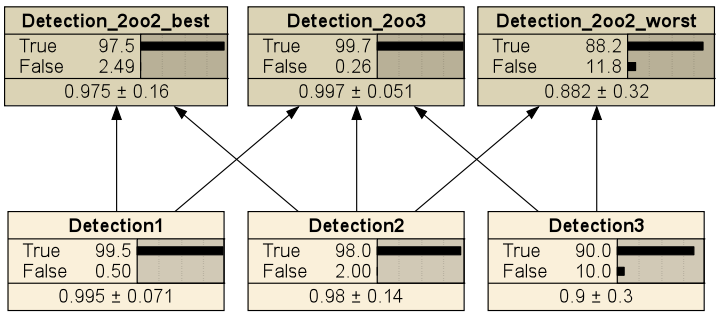

Figure 5. POD evaluation of majority voting.

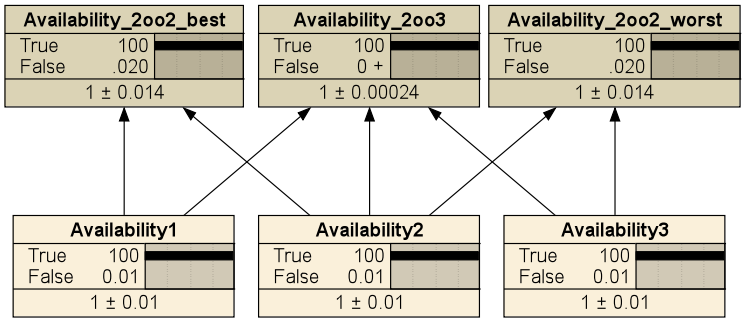

Figure 6. Availability evaluation.

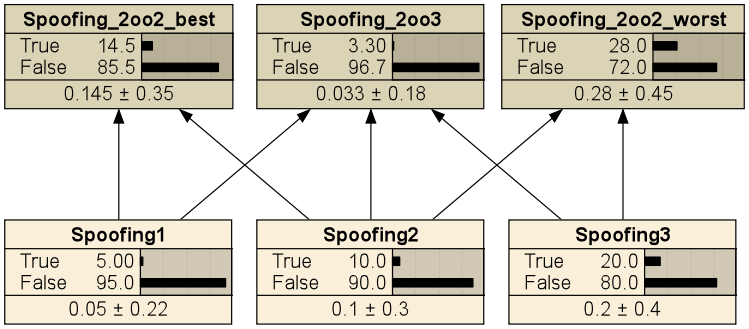

Figure 7. Spoofing success rate evaluation.

TECHNOLOGY	COST [€] BETTER ↓	AVAILABILITY [%] BETTER ↑	SPOOF [%] BETTER ↓	POD [%] BETTER ↑	FAR [%] BETTER ↓
SINGLE (BEST)	500	99.990	5	99.5	1
SINGLE (AVERAGE)	200	99.990	10	98	5
SINGLE (WORST)	**100**	99.990	20	90	8
DUAL (2OO2, BEST)	700	99.020	14.5	97.5	**0.05**
DUAL (2OO2, WORST)	300	99.020	28	88.2	0.4
TRIPLE (2OO3)	800	**99.999**	**3.30**	**99.7**	0.52

Table 2. Summary of results and comparison of technologies.

4. Conclusions

The most important goals in the design of physical security systems are to maximize the detection probability, and to minimize the occurrence of false alarms, in order to achieve optimal performance. In this paper, I have demonstrated using an analytical approach how a cost-effective solution can be achieved by exploiting diverse

redundancy in sensor technology and alarm correlation for majority voting. Majority voting allows us to improve the probability of detection of even the most advanced single sensor technology, as well as the overall detection availability, at the cost of slightly more false alarms only with respect to dual technology (i.e., AND-type correlation); furthermore, majority voting also improves robustness to spoofing attempts.

The correlation studied in this paper can be implemented using simple programmable logic devices, software programs controlling computer digital I/O cards, or any COTS (Commercial Off The Shelf) integrated circuits meeting the correlation logic needs (3-input OR gate and 3 two-input AND gate). An effective solution can be obtained by holding the input values of the sensors for a few seconds (e.g., using timed flip-flops) in order to allow for the necessary detection latencies from the diverse technologies. In some cases, triple technology sensors in a single enclosure can be already available as COTS. In these cases the output of the single sensors can be accessed singularly and correlated in a '2oo3' configuration, as explained in this paper, instead of using the less effective AND/OR logic.

Other possible majority voting schemes (e.g., '3oo4', '4oo5', etc.), sometimes used in mission/safety-critical systems, are likely to introduce a far higher complexity in system design, but they could fit the needs of specific applications and can be evaluated using the same approach presented in this paper.

I have motivated the approach basing on cost-effectiveness principles, since a linear reliability growth usually implies an exponential cost growth. However, some modern detection technologies (e.g., audio-video analytics) are not yet very reliable, regardless of the manufacturer experience and testing effort. One idea is to combine more diverse artificial intelligence algorithms (e.g., object tracking, neural networks, etc.) and a majority voting scheme for event detection in order to get better results.

Finally, majority voting is not necessarily Boolean: a (possibly weighted) average of measured values can be considered in the case of continuous numerical values. Such an application is currently under analysis for networks of smart wireless sensors.

References

1. Adamsky, B.: Design critical control or emergency shut down systems for safety and reliability. White Paper. http://www.ips.invensys.com/en/knowledge/Documents/white-papers/IPS_GL_UP_SS_WP_12-08_DesignCriticalControl.pdf (last access January 6th 2010)
2. Avizienis, A., Laprie, J.C., Randel B.: Fundamental Concepts of Dependability. LAAS Report n. 01-145, 2001
3. Bocchetti, G., Flammini, F., Pappalardo, A., Pragliola, C.: Dependable integrated surveillance systems for the physical security of metro railways. In: Proc. 3rd ACM/IEEE International Conference on Distributed Smart Cameras (ICDSC 2009), 30 August - 2 September, 2009, Como (Italy): pp. 1-7
4. Charniak, E.: Bayesian Networks without Tears. In: AI Magazine, 12(4), 1991: pp. 50-63
5. Flammini, F., Marrone, S., Mazzocca, N., Vittorini, V.: Evaluating the Hazardous Failure Rate of majority voting computer architectures by means of Bayesian Network models. In: Risk, Reliability and Societal Safety - Aven & Vinnem (eds), Proc. ESREL'07, Stavanger, Norway, June 25-27, 2007: pp. 1715-1721
6. Garcia, M.L., The Design and Evaluation of Physical Protection Systems, Butterworth-Heinemann, 2001
7. Li, Y. P., Yang, J., Li, X.D., Tian, J.: Ultrasonic Intruder Detection System for Home Security. In: LNCS Vol. 344/2006: pp. 1108-1115
8. Martin, P.T., Feng, Y., Wang, X.: Detector Technology Evaluation. http://www.mountain-plains.org/pubs/pdf/MPC03-154.pdf, 2003 (last access January 6th 2010)

9. Norsys Netica Web Site: http://www.norsys.com/netica.html (last access January 6th 2010)
10. Rogalski, A.: Infrared detectors: status and trends. In: Progress in Quantum Electronics, Vol. 27, Issues 2-3, 2003: pp. 59-210