Sensitivity Analysis of Bayesian Networks Used in Forensic Investigations

Michael Kwan, Richard Overill, Kam-Pui Chow, Hayson Tse, Frank Law, Pierre Lai

Chapter 18

SENSITIVITY ANALYSIS OF BAYESIAN NETWORKS USED IN FORENSIC INVESTIGATIONS

Michael Kwan, Richard Overill, Kam-Pui Chow, Hayson Tse, Frank Law and Pierre Lai

Abstract Research on using Bayesian networks to enhance digital forensic investigations has yet to evaluate the quality of the output of a Bayesian network. The evaluation can be performed by assessing the sensitivity of the posterior output of a forensic hypothesis to the input likelihood values of the digital evidence. This paper applies Bayesian sensitivity analysis techniques to a Bayesian network model for the well-known Yahoo! case. The analysis demonstrates that the conclusions drawn from Bayesian network models are statistically reliable and stable for small changes in evidence likelihood values.

Keywords: Forensic investigations, Bayesian networks, sensitivity analysis

1. Introduction

Research on applying Bayesian networks to criminal investigations is on the rise [7–9, 12]. The application of Bayes' theorem and graph theory provides a means to characterize the causal relationships among variables [16]. In terms of forensic science, these correspond to the hypothesis and evidence. When constructing a Bayesian network, the causal structure and conditional probability values come from multiple experiments or expert opinion.

The main difficulties in constructing a Bayesian network are in knowing what to ask experts and in assessing the accuracy of their responses. When an assessment is made from incomplete estimations or inconsistent beliefs, the resulting posterior output is inaccurate or "sensitive" [4]. Therefore, when applying a Bayesian network model, the investigator must understand the certainty of the conclusions drawn from the

model. Sensitivity analysis provides a means to evaluate the possible inferential outcomes of a Bayesian network to gain this understanding [11].

This paper applies sensitivity analysis techniques to evaluate the correctness of a Bayesian network model for the well-known Yahoo! case [3]. The Bayesian network was constructed using details from the conviction report, which describes the evidence that led to the conviction of the defendant [7]. The analysis tests the sensitivity of the hypothesis to small and large changes in the likelihood of individual pieces of evidence.

2. Sensitivity Analysis

The accuracy of a Bayesian network depends on the robustness of the posterior output to changes in the input likelihood values [5]. A Bayesian network is robust if it exhibits a lack of posterior output sensitivity to small changes in the likelihood values. Sensitivity analysis is important due to the practical difficulty of precisely assessing the beliefs and preferences underlying the assumptions of a Bayesian model. Sensitivity analysis investigates the properties of a Bayesian network by studying its output variations arising from changes in the input likelihood values [15].

A common approach to assess the sensitivity is to iteratively vary each likelihood value over all possible combinations and evaluate the effects on the posterior output [6]. If large changes in the likelihood values produce a negligible effect on the posterior output, then the evidence is sufficiently influential and has little to no impact on the model. On the other hand, if small changes cause the posterior output to change significantly, then it is necessary to review the network structure and the prior probability values.

Since the probability distributions of the evidence likelihood values and hypothesis posteriors in a Bayesian network constructed for a digital forensic investigation are mostly discrete, parameter sensitivity analysis can be used to evaluate the sensitivity of the Bayesian network for the Yahoo! case. Three approaches, bounding sensitivity function, sensitivity value and vertex proximity, are used to determine the bounding sensitivity of each piece of evidence and its robustness under small and large variations in its likelihood value.

2.1 Bounding Sensitivity Function

Parameter sensitivity analysis evaluates the posterior output based on variations in the evidence provided. It is impractical – possibly, computationally intractable – to perform a full sensitivity analysis that

varies the likelihood values one at a time while keeping the other values fixed [10]. One solution to the intractability problem is to use a bounding sensitivity function to select functions that have a high sensitivity [13].

To evaluate the sensitivity of the posterior of the root hypothesis θ to the conditional probability of evidence x, the likelihood value of x given θ ($P(x|\theta)$), denoted by x_0, and the posterior result of θ given x ($P(\theta|x)$), denoted by h_0, are sufficient to compute the upper and lower bounds of the sensitivity function for $P(\theta|x)$. These bounds come from the original values of the parameter under study (x_0) and the probability of interest (h_0) [13]. Any sensitivity function passing through the point (x_0, h_0) is bounded by the two rectangular hyperbolas $i(x)$ and $d(x)$:

$$i(x) = \frac{h_0 \cdot (1 - x_0) \cdot x}{(h_0 - x_0) \cdot x + (1 - h_0) \cdot x_0} \tag{1}$$

$$d(x) = \frac{h_0 \cdot x_0 \cdot (1 - x)}{(1 - h_0 - x_0) \cdot x + h_0 \cdot x_0} \tag{2}$$

The bounds on a sensitivity function $f(x)$ with $f(x_0) = h_0$ are:

$$\min\{i(x_j), d(x_j)\} \leq f(x_j) \leq \max\{i(x_j), d(x_j)\} \tag{3}$$

for all x_j in [0,1]. The point at which the bounds intersect indicates the sensitivity of the function. The sensitivity increases as the intersection approaches zero.

2.2 Sensitivity Value

A sensitivity value provides an approximation to small deviations in the probabilistic likelihood of evidence [10]. The sensitivity value is the partial derivative of the posterior output of the hypothesis with respect to the likelihood of a particular state of the evidence. Mathematically, for a hypothesis θ given evidence e as a function of a probabilistic likelihood x, the posterior probability $P(\theta|e)(x)$ is the sensitivity function $f(x)$ for θ, which is the quotient of two linear functions of x. The sensitivity function is given by:

$$f(x) = P(\theta|e)(x) = \frac{P(\theta \wedge e)(x)}{P(e)(x)} = \frac{a \cdot x + b}{c \cdot x + d} \tag{4}$$

where the coefficients a, b, c and d are derived from the original (unvaried) parameters of the Bayesian network [14, 17, 18].

The sensitivity of a likelihood value is the absolute value of the first derivative of the sensitivity function at the original likelihood value [14]:

$$\left| \frac{a \cdot d - b \cdot c}{(c \cdot x + d)^2} \right| \tag{5}$$

This sensitivity value describes the change in the posterior output of the hypothesis for small variations in the likelihood of the evidence under study. The larger the sensitivity value, the less robust the posterior output of the hypothesis [14]. In other words, a likelihood value with a large sensitivity value is prone to generate an inaccurate posterior output. If the sensitivity value is less than one, then a small change in the likelihood value has a minimal effect on the result of the posterior output of the hypothesis [17].

2.3 Vertex Proximity

Even if a Bayesian network is robust to small changes in its evidence likelihood values, it is also necessary to assess if the network is robust to large variations in the likelihood values [17]. The impact of a larger variation in a likelihood value, the vertex proximity, depends on the location of the vertex of the sensitivity function. Calculating the vertex proximity assumes that the sensitivity function has a hyperbolic form expressed as:

$$f(x) = \frac{r}{x - s} + t \qquad \text{where } s = -\frac{d}{c}; t = \frac{a}{c}; r = \frac{b}{c} + s \cdot t \tag{6}$$

Given a sensitivity function defined by $0 \leq f(x) \leq 1$, the two-dimensional space $(x, f(x))$ is bounded by the unit window [0,1] [14]. The vertex is a point where the sensitivity value ($|\ \frac{a \cdot d - b \cdot c}{(c \cdot x + d)^2}\ |$) is equal to one. Because the rectangular hyperbola extends indefinitely, the vertical asymptotes of the hyperbola may lie outside the unit window, either $s < 0$ or $s > 1$.

The vertex proximity expression:

$$x_v = \{s + \sqrt{|r|} \text{ if } s < 0 \text{ or } s - \sqrt{|r|} \text{ if } s > 1\} \tag{7}$$

is based on the vertex value with respect to the likelihood value of s [17]. If the original likelihood value is close to the value of x_v, then the posterior output may possess a high degree of sensitivity to large variations in the likelihood value [17].

3. Bayesian Network for the Yahoo! Case

This section describes the application of the bounding sensitivity, sensitivity value and vertex proximity techniques to evaluate the robustness of a Bayesian network constructed for the Yahoo! case [7]. Constructing a Bayesian network for a forensic investigation begins with the establishment of the top-most hypothesis. Usually, this hypothesis represents the main issue to be resolved. In the Yahoo! case, the hypothesis H is that the seized computer was used to send the subject file as an email attachment using a specific Yahoo! email account.

The hypothesis H is the root node of the Bayesian network and is the ancestor of every other node in the network. The unconditional (prior) probabilities are: $P(H = \text{Yes}) = 0.5$ and $P(H = \text{No}) = 0.5$.

There are six sub-hypotheses that are dependent on the main hypothesis H. The six sub-hypothesis are events that should have occurred if the file in question had been sent by the suspect's computer via Yahoo! web-mail. The sub-hypotheses (states: Yes and No) are:

- $\boldsymbol{H_1}$: Linkage between the subject file and the suspect's computer.
- $\boldsymbol{H_2}$: Linkage between the suspect and the computer.
- $\boldsymbol{H_3}$: Linkage between the suspect and the ISP.
- $\boldsymbol{H_4}$: Linkage between the suspect and the Yahoo! email account.
- $\boldsymbol{H_5}$: Linkage between the computer and the ISP.
- $\boldsymbol{H_6}$: Linkage between the computer and the Yahoo! email account.

Table 1 lists the digital evidence DE_i (states: Yes, No and Uncertain) associated with the six sub-hypotheses.

Since there are no observations of the occurrences of the six sub-hypotheses, their conditional probability values cannot be predicted using frequentist approaches. Therefore, an expert was asked to subjectively assign the probabilities used in this study (Table 2).

Table 3 presents the conditional probability values of the fourteen pieces of digital evidence given the associated sub-hypotheses.

3.1 Posterior Probabilities

Figures 1 and 2 show the posterior probabilities of H when $H_1 \ldots H_6$ are Yes and No, respectively. The upper and lower bounds of H – the seized computer was used to send the subject file as an email attachment via the Yahoo! email account – are 0.972 and 0.041, respectively. However, these posterior results are not justified until the sensitivity of the Bayesian network is evaluated.

Table 1. Sub-hypotheses and the associated evidence.

Sub-Hypot.	Evidence	Description
H_1	DE_1	Subject file exists on the computer
H_1	DE_2	Last access time of the subject file is after the IP address assignment time by the ISP
H_1	DE_3	Last access time of the subject file is after or is close to the sent time of the Yahoo! email
H_2	DE_4	Files on the computer reveal the identity of the suspect
H_3	DE_5	ISP subscription details (including the assigned IP address) match the suspect's particulars
H_4	DE_6	Subscription details of the Yahoo! email account (including the IP address that sent the email) match the suspect's particulars
H_5	DE_7	Configuration settings of the ISP Internet account are found on the computer
H_5	DE_8	Log data confirms that the computer was powered up at the time the email was sent
H_5	DE_9	Web browser (e.g., Internet Explorer) or email program (e.g., Outlook) was found to be activated at the time the email was sent
H_5	DE_{10}	Log data reveals the assigned IP address and the assignment time by the ISP to the computer
H_5	DE_{11}	Assignment of the IP address to the suspect's account is confirmed by the ISP
H_6	DE_{12}	Internet history logs reveal that the Yahoo! email account was accessed by the computer
H_6	DE_{13}	Internet cache files reveal that the subject file was sent as an attachment from the Yahoo! email account
H_6	DE_{14}	IP address of the Yahoo! email with the attached file is confirmed by Yahoo!

Table 2. Likelihood of $H_1 \ldots H_6$ given H.

	H_1, H_5, H_6		H_2, H_3, H_4	
H	Y	N	Y	N
Y	0.65	0.35	0.8	0.2
N	0.35	0.65	0.2	0.8

4. Sensitivity Analysis Results

This section presents the results of the sensitivity analysis conducted on the Bayesian network for the Yahoo! case.

Table 3. Probabilities of $DE_1 \ldots DE_{14}$ given H_i.

H_i	Y	N	U	Y	N	U	Y	N	U
	$DE_1, i=1$			$DE_2, DE_3, i=1$			$DE_4, i=2$		
Y	0.85	0.15	0.00	0.80	0.15	0.05	0.75	0.20	0.05
N	0.15	0.85	0.00	0.15	0.80	0.05	0.20	0.75	0.05
	$DE_5, i=3$			$DE_6, i=4$			$DE_7, DE_8, DE_{10}, i=5$		
Y	0.70	0.25	0.05	0.10	0.85	0.05	0.70	0.25	0.05
N	0.25	0.70	0.05	0.05	0.90	0.05	0.25	0.70	0.05
	$DE_9, DE_{11}, i=5$			$DE_{12}, DE_{13}, i=6$			$DE_{14}, i=6$		
Y	0.80	0.15	0.05	0.70	0.25	0.05	0.80	0.15	0.05
N	0.15	0.80	0.05	0.25	0.70	0.05	0.15	0.80	0.05

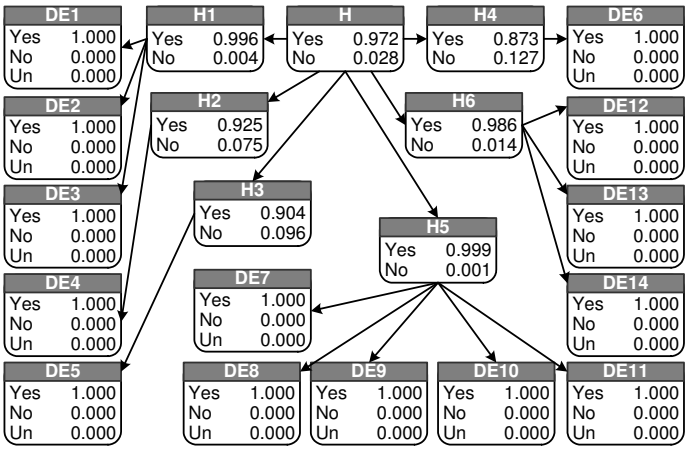


Figure 1. Posterior probabilities when $DE_1 \ldots DE_{14}$ are Yes.

4.1 Bounding Sensitivity Analysis

The sensitivity of the posterior outputs of the root hypothesis H to the conditional probabilities of evidence $DE_1 \ldots DE_{14}$ is computed using Equation (4). To illustrate the process, we compute the bounding sensitivity function for H against the likelihood of DE_1.

From Table 3, the likelihood of DE_1 (subject file exists on the suspect's computer) given H_1 (linkage between the subject file and the computer), i.e., $P(DE_1|H_1)$ is equal to 0.85 (x_0). As shown in Figure 3, if DE_1 is observed, the posterior output of the root hypothesis H, i.e., DE_1 ($P(H|DE_1)$), is equal to 0.60 (h_0).

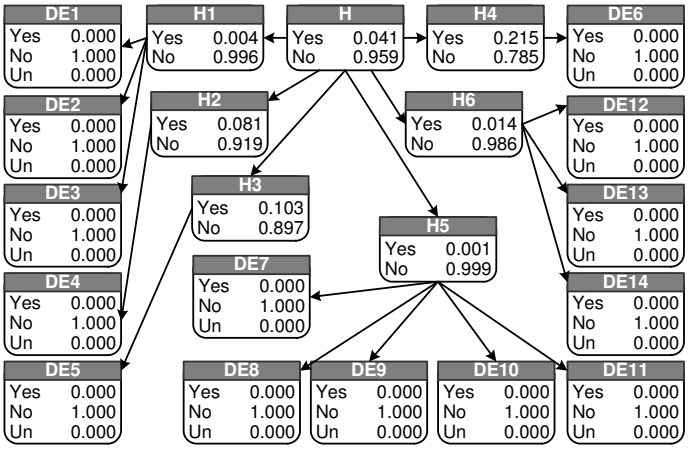


Figure 2. Posterior probabilities when $DE_1 \ldots DE_{14}$ are No.

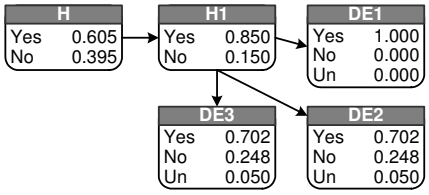


Figure 3. Posterior probability of H when DE_1 is Yes.

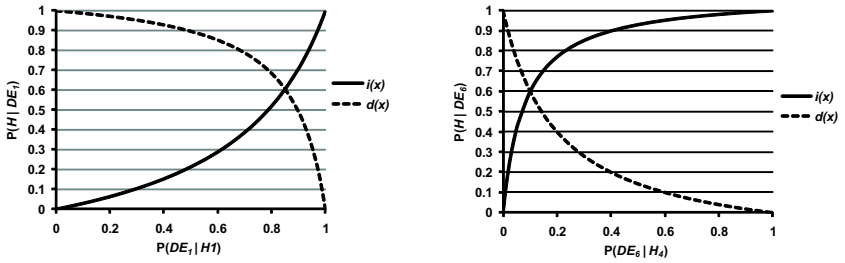
Upon applying Equations (1) and (2), the sensitivity functions $i(x)$ and $d(x)$ are given by:

$$i(x) = \frac{h_0 \cdot (1 - x_0) \cdot x}{(h_0 - x_0) \cdot x + (1 - h_0) \cdot x_0} = \frac{0.09075x}{0.33575 - 0.245x} \tag{8}$$

$$d(x) = \frac{h_0 \cdot x_0 \cdot (1 - x)}{(1 - h_0 - x_0) \cdot x + h_0 \cdot x_0} = \frac{0.51425 - 0.51425x}{0.51425 - 0.455x} \tag{9}$$

Figure 4(a) presents the bounding sensitivity functions for the posteriors of hypothesis H to $P(DE_1|H_1)$. In particular, it shows the plot of the $i(x)$ and $d(x)$ functions, which is the bounding sensitivity of $P(H|DE_1)$ against $P(DE_1|H_1)$. Note that a significant shift in the estimated bounds for $P(H|DE_1)$ occurs when $P(DE_1|H_1)$ is greater than 0.85. Because the shift is large, the hypothesis is not sensitive to changes in DE_1.

The bounds of $P(H|DE_2) \ldots P(H|DE_{14})$ and the bounds of $P(DE_2|H_2) \ldots P(DE_{14}|H_6)$ do not produce significant changes in the bounds for the posterior output and are not sensitive to changes in the likeli-



(a) (b)

Figure 4. Bounding sensitivity functions.

hood values. The most sensitive bound is for the sensitivity function of $P(H|DE_6)$, which is less than 0.1 according to Figure 4(b). Note that Figure 4(b) shows the bounding sensitivity for the posterior probabilities of the root hypothesis H to $P(DE_6|H_4)$. Although the likelihood of DE_6 is more sensitive than the likelihoods of the other pieces of digital evidence, the robustness of the posterior results with respect to the elicited conditional probabilities in the Yahoo! Bayesian network is still not clear. Therefore, the sensitivity values and vertex proximities for the evidence must also be assessed to ascertain the robustness of the Bayesian network.

4.2 Sensitivity Value Analysis

To illustrate the sensitivity value analysis technique, we evaluate the sensitivity of sub-hypothesis H_1 (linkage between the subject file and the suspect's computer) to the likelihood value of evidence DE_1 (subject file exists on the computer). The sensitivity value analysis evaluates the probability of interest, $P(H_1|DE_1)$, for a variation in the likelihood value of $P(DE_1|H_1)$. This requires a sensitivity function that expresses $P(H_1|DE_1)$ in terms of $x = P(DE_1|H_1)$:

$$P(H_1|DE_1)(x) = \frac{P(DE_1|H_1)P(H_1)}{P(DE_1)} \tag{10}$$

Rewriting the numerator $P(DE_1|H_1)P(H_1)$ as $P(H_1)x + 0$ yields the coefficient values $a = P(H_1)$ and $b = 0$. Rewriting the denominator as $P(DE_1) = P(DE_1|H_1)P(H_1) + P(DE_1|\overline{H_1})P(\overline{H_1}) = P(H_1)x + P(DE_1|\overline{H_1})P(\overline{H_1})$ yields the coefficient values $c = P(H_1)$ and $d = P(DE_1|\overline{H_1})P(\overline{H_1})$.

Since $P(H_1) = 0.5$ and $P(DE_1|\overline{H_1}) = 0.15$ (from Table 3), the coefficients of the sensitivity function are: $a = 0.5$, $b = 0$, $c = 0.5$

Table 4. Sensitivity values and effects on posterior outputs.

Evidence	Elicited Value	Sensitivity Function Coefficients				Sensitivity Value	Effect on Posterior
		a	b	c	d		
DE_1	0.85	0.5	0	0.5	0.075	0.150	Hardly changes
DE_2	0.80	0.5	0	0.5	0.075	0.166	Hardly changes
DE_3	0.80	0.5	0	0.5	0.075	0.166	Hardly changes
DE_4	0.75	0.5	0	0.5	0.100	0.222	Hardly changes
DE_5	0.70	0.5	0	0.5	0.125	0.250	Hardly changes
DE_6	0.10	0.5	0	0.5	0.025	0.045	Hardly changes
DE_7	0.70	0.5	0	0.5	0.125	0.250	Hardly changes
DE_8	0.70	0.5	0	0.5	0.125	0.250	Hardly changes
DE_9	0.80	0.5	0	0.5	0.075	0.166	Hardly changes
DE_{10}	0.70	0.5	0	0.5	0.125	0.250	Hardly changes
DE_{11}	0.80	0.5	0	0.5	0.075	0.166	Hardly changes
DE_{12}	0.70	0.5	0	0.5	0.125	0.250	Hardly changes
DE_{13}	0.70	0.5	0	0.5	0.125	0.250	Hardly changes
DE_{14}	0.80	0.5	0	0.5	0.075	0.166	Hardly changes

and $d = 0.075$. Upon applying Equation (5), the sensitivity value of $P(H_1|DE_1)$ against $P(DE_1|H_1)$ is:

$$\left|\frac{a \cdot d - b \cdot c}{(c \cdot x + d)^2}\right| = \left|\frac{0.5 \cdot 0.075 - 0 \cdot 0.5}{(0.5 \cdot 0.85 + 0.075)^2}\right| = 0.15 \tag{11}$$

As noted in [17], if the sensitivity value is less than one, then a small change in the likelihood value has a minimal effect on the posterior output of a hypothesis. Table 4 shows sensitivity values that express the effects of small changes in evidence likelihood values on the posterior outputs of the related sub-hypotheses. Note that all the sensitivity values are less than one. Therefore, it can be concluded that the Bayesian network is robust to small variations in the elicited conditional probabilities. Since priors of the evidence are computed from the elicited probabilities, it can also be concluded that the Yahoo! Bayesian network is robust to small variations in the evidence likelihood values.

4.3 Vertex Proximity Analysis

Although the Yahoo! Bayesian network is robust to small changes in evidence likelihood values, it is also necessary to assess its robustness to large variations in the conditional probabilities. Table 5 shows the results of the vertex likelihood (x_v) computation using Equation (7) for $DE_1 \ldots DE_{14}$.

Table 5. Sensitivity values and effects on posterior outputs.

Evidence	**Elicited Value** (x_0)	s	t	r	x_v	$\lvert x_v - x_0 \rvert$
DE_1	0.85	-0.15	1	-0.15	0.237	0.613
DE_2	0.80	-0.15	1	-0.15	0.237	0.563
DE_3	0.80	-0.15	1	-0.15	0.237	0.563
DE_4	0.75	-0.20	1	-0.20	0.247	0.503
DE_5	0.70	-0.25	1	-0.25	0.250	0.450
DE_6	0.10	-0.05	1	-0.05	0.174	0.074
DE_7	0.70	-0.25	1	-0.25	0.250	0.450
DE_8	0.70	-0.25	1	-0.25	0.250	0.450
DE_9	0.80	-0.15	1	-0.15	0.237	0.563
DE_{10}	0.70	-0.25	1	-0.25	0.250	0.450
DE_{11}	0.80	-0.15	1	-0.15	0.237	0.613
DE_{12}	0.70	-0.25	1	-0.25	0.250	0.450
DE_{13}	0.70	-0.25	1	-0.25	0.250	0.450
DE_{14}	0.80	-0.15	1	-0.15	0.237	0.563

Table 5 shows sensitivity values expressing the effects of large changes in evidence likelihood values on the posterior outputs of related sub-hypotheses. Based on the small sensitivity values in Table 4 and the lack of vertex proximity shown in Table 5, the posterior outputs of the sub-hypotheses H_1, H_2, H_3, H_5 and H_6 are not sensitive to variations in the likelihood values of $DE_1 \ldots DE_5$ and $DE_7 \ldots DE_{14}$.

However, for digital evidence DE_6 and sub-hypothesis H_4, the elicited probability of 0.1 is close to the vertex value of 0.174; thus, the elicited probability of DE_6 exhibits a degree of vertex proximity. In other words, the posterior result of H_4 (linkage between the suspect and the Yahoo! email account) is sensitive to the variation in the likelihood value of DE_6 even though the sensitivity value for DE_6 is small.

Although the Yahoo! Bayesian network is robust, the elicitation of the likelihood value of DE_6 (subscription details of the Yahoo! email account match the suspect's particulars) given sub-hypothesis H_4 ($P(DE_6|H_4)$) is the weakest node in the network. The weakest node is most susceptible to change and is, therefore, the best place to attack the case. This means that digital evidence DE_6 is of the greatest value to defense attorneys and prosecutors.

5. Conclusions

The bounding sensitivity function, sensitivity value and vertex proximity are useful techniques for analyzing the sensitivity of Bayesian networks used in forensic investigations. The analysis verifies that the

Bayesian network developed for the celebrated Yahoo! case is reliable and accurate. The analysis also reveals that evidence related to the hypothesis that the subscription details of the Yahoo! email account match the suspect's particulars is the most sensitive node in the Bayesian network. To ensure accuracy, the investigator must critically review the elicitation of this evidence because a change to this node has the greatest effect on the network output.

The one-way sensitivity analysis presented in this paper varies one likelihood value at a time. It is possible to perform n-way analysis of a Bayesian network, but the mathematical functions become very complicated [17]. Given that digital evidence is becoming increasingly important in court proceedings, it is worthwhile to conduct further research on multi-parameter, higher-order sensitivity analysis [2] to ensure that accurate analytical conclusions can be drawn from the probabilistic results obtained with Bayesian networks.

References

[1] J. Berger, An Overview of Robust Bayesian Analysis, Technical Report 93-53C, Department of Statistics, Purdue University, West Lafayette, Indiana, 1993.

[2] H. Chan and A. Darwiche, Sensitivity analysis in Bayesian networks: From single to multiple parameters, *Proceedings of the Twentieth Conference on Uncertainty in Artificial Intelligence*, pp. 67–75, 2004.

[3] Changsha Intermediate People's Court of Hunan Province, Reasons for Verdict, First Trial Case No. 29, Changsha Intermediate Criminal Division One Court, Changsha, China (www.pcpd.org.hk/english/publications/files/Yahoo_annex.pdf), 2005.

[4] M. Druzdzel and L. van der Gaag, Elicitation of probabilities for belief networks: Combining qualitative and quantitative information, *Proceedings of the Eleventh Conference on Uncertainty in Artificial Intelligence*, pp. 141–148, 1995.

[5] J. Ghosh, M. Delampady and T. Samanta, *An Introduction to Bayesian Analysis: Theory and Methods*, Springer, New York, 2006.

[6] J. Gill, *Bayesian Methods: A Social and Behavioral Sciences Approach*, Chapman and Hall, Boca Raton, Florida, 2002.

[7] M. Kwan, K. Chow, P. Lai, F. Law and H. Tse, Analysis of the digital evidence presented in the Yahoo! case, in *Advances in Digital Forensics V*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 241–252, 2009.

[8] M. Kwan, K. Chow, F. Law and P. Lai, Reasoning about evidence using Bayesian networks, in *Advances in Digital Forensics IV*, I. Ray and S. Shenoi (Eds.), Springer, Boston, Massachusetts, pp. 275–289, 2008.

[9] M. Kwan, R. Overill, K. Chow, J. Silomon, H. Tse, F. Law and P. Lai, Evaluation of evidence in Internet auction fraud investigations, in *Advances in Digital Forensics VI*, K. Chow and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 121–132, 2010.

[10] K. Laskey, Sensitivity analysis for probability assessments in Bayesian networks, *IEEE Transactions on Systems, Man and Cybernetics*, vol. 25(6), pp. 901–909, 1995.

[11] M. Morgan and M. Henrion, *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, Cambridge, United Kingdom, 1992.

[12] R. Overill, M. Kwan, K. Chow, P. Lai and F. Law, A cost-effective model for digital forensic investigations, in *Advances in Digital Forensics V*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 231–240, 2009.

[13] S. Renooij and L. van der Gaag, Evidence-invariant sensitivity bounds, *Proceedings of the Twentieth Conference on Uncertainty in Artificial Intelligence*, pp. 479–486, 2004.

[14] S. Renooij and L. van der Gaag, Evidence and scenario sensitivities in naive Bayesian classifiers, *International Journal of Approximate Reasoning*, vol. 49(2), pp. 398–416, 2008.

[15] A. Saltelli, M. Ratto, T. Andres, F. Campolongo, J. Cariboni, D. Gatelli, M. Saisana and S. Tarantola, *Global Sensitivity Analysis: The Primer*, John Wiley, Chichester, United Kingdom, 2008.

[16] F. Taroni, C. Aitken, P. Garbolino and A. Biedermann, *Bayesian Network and Probabilistic Inference in Forensic Science*, John Wiley, Chichester, United Kingdom, 2006.

[17] L. van der Gaag, S. Renooij and V. Coupe, Sensitivity analysis of probabilistic networks, in *Advances in Probabilistic Graphical Models*, P. Lucas, J. Gamez and A. Salmeron (Eds.), Springer, Berlin, Germany, pp. 103–124, 2007.

[18] H. Wang, I. Rish and S. Ma, Using sensitivity analysis for selective parameter update in Bayesian network learning, *Proceedings of the AAAI Spring Symposium on Information Refinement and Revision for Decision Making: Modeling for Diagnostics, Prognostics and Prediction*, pp. 29–36, 2002.