Reasoning about Evidence using Bayesian Networks

Hayson Tse, Kam-Pui Chow, Michael Kwan

Chapter 7

REASONING ABOUT EVIDENCE USING BAYESIAN NETWORKS

Hayson Tse, Kam-Pui Chow and Michael Kwan

Abstract This paper presents methods for analyzing the topology of a Bayesian belief network created to qualify and quantify the strengths of investigative hypotheses and their supporting digital evidence. The methods, which enable investigators to systematically establish, demonstrate and challenge a Bayesian belief network, help provide a powerful framework for reasoning about digital evidence. The methods are applied to review a Bayesian belief network constructed for a criminal case involving BitTorrent file sharing, and explain the causal effects underlying the legal arguments.

Keywords: Digital evidence, Bayesian networks, evidentiary reasoning

1. Introduction

The investigation of a crime and the prosecution of the suspect can be an expensive and time-consuming process. The cost of a mistake can be high – a guilty party may be acquitted; even worse, an innocent individual may be convicted. Accordingly, criminal investigators and prosecutors are required to prove the elements of a case beyond a reasonable doubt. This means that the events involving the suspect and constituting the alleged offense must be reconstructed in a faithful manner from the available clues.

Event reconstruction involves the identification of plausible acts based on the evidence observed by an investigator. During reconstruction, it is often necessary to formulate hypotheses based on the evidence and evaluate the likelihood of the hypotheses; eventually, the evidence and the legal reasoning must be presented in court [4].

In the physical world, the evidence observed by an investigator may be fabricated, removed, forged or altered. The same applies to digital

forensic evidence. Cohen [1] has advocated the development of methods that allow the reliability of evidence to be established, demonstrated and challenged. Such methods should identify the digital processes that created the evidence, assess the weights or degrees of the beliefs of the investigator, and provide reasons in support of the beliefs.

Bayesian belief networks have been applied to digital forensic investigations. de Vel, *et al.* [2] have proposed a combination Bayesian belief network model and hidden Markov model to encode digital forensic evidence during a given time interval and estimate the degree of criminal activity over time. Lee, *et al.* [8] have developed a methodology for transforming the findings in digital forensic reports to graphical representations using a Bayesian belief network. Kwan, *et al.* [6] have used Bayesian belief networks to quantify the strengths of hypotheses formulated during an investigation and their supporting evidence. They demonstrated the utility of a Bayesian belief network model using evidence in a Hong Kong criminal case involving illegal file sharing via BitTorrent.

Any method that is used to support a legal hypothesis would be subject to close scrutiny. In Hong Kong, as in other common law jurisdictions, if a court is to accept the evidence of a specific scientific theory (whether novel or not), then the theory must have a sound scientific basis and must be comprehensible to the court. Also, the methods used to carry out the scientific tests should be safe and reliable, and should follow established protocols (i.e., protocols that have been published, disseminated and acknowledged to be reproducible) [3].

When constructing a Bayesian belief network, the causal structure and conditional probability values come from domain knowledge or empirical data. Therefore, it is necessary to assess the accuracy of the derived model with regard to the structure and the probability values. This begs the question: what makes a model accurate? Issues related to the interactions between the events corresponding to variables are important. The interactions are reflected by the causal structure or topology of a Bayesian belief network.

This paper describes two methods for analyzing the topology of a Bayesian belief network created to qualify and quantify the strengths of investigative hypotheses and their supporting digital evidence. The methods are applied to review a Bayesian belief network constructed for a criminal case involving BitTorrent file sharing, and to clarify the causal effects underlying the legal arguments.

2. BitTorrent Overview

Kwan, *et al.* [6] created a Bayesian belief network for the evidence in a Hong Kong criminal case involving illegal file sharing via BitTorrent. Kwan and colleagues specified the probability distributions of the hypotheses and evidence in the Bayesian belief network, and used the network to quantify the strengths of the investigative hypotheses. Before we describe the method for analyzing the topology of a Bayesian belief network and its application to the BitTorrent case, we briefly review the operation of BitTorrent.

BitTorrent is a peer-to-peer application that uses metadata files known as "torrents." The metadata is used by a BitTorrent client to connect to remote computers and download files.

In a typical BitTorrent scenario, an "initial seeder" first creates a torrent using a BitTorrent client or a torrent-making application. The torrent is then posted on a website or forum. Next, the initial seeder distributes small chunks of the file that is to be shared to different machines that are connected via a BitTorrent client.

The connected machines are collectively referred to as a "swarm." After the initial seeder has shared all the data chunks with the swarm, the machines in the swarm can proceed to share the chunks with each other and with other newly connected machines.

A torrent primarily contains three pieces of information: (i) name of the file to be shared; (ii) size of each chunk composing the file and the number of chunks; and (iii) uniform resource locator (URL) of a "tracker." A tracker is a dedicated server that links all the peers in relation to a torrent. Remote individuals download the torrent from a website. When the torrent is opened within a BitTorrent client, the client is referred to the initial seeder using the tracker URL.

Locating a torrent alone on a computer is not evidence of file uploading, downloading or sharing by the computer. This is because there are different ways in which a torrent may be stored on a computer. A user may create a torrent and save it anywhere on a network. Alternatively, a user may open a torrent from a website, which causes the torrent file to be saved in the Temporary Internet Files folder (if Internet Explorer is used as the web browser). A user may also copy a torrent from a website, email, Internet Relay Chat or external storage device to any location on the network.

Since the presence of a torrent alone is not evidence of file uploading, downloading or sharing, investigators need to gather additional evidence to show that the torrent was opened within a client. One piece of ev-

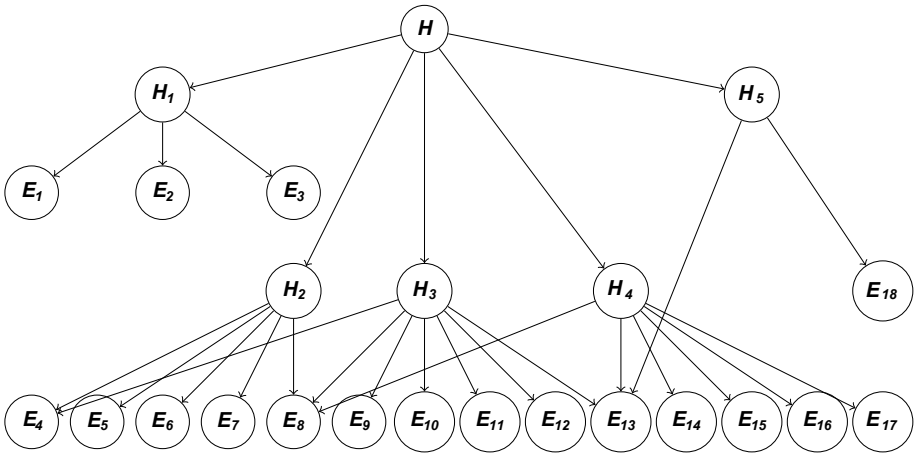


Figure 1. Bayesian network for the BitTorrent case.

idence is a backup torrent, which is often created when a BitTorrent client opens a torrent.

A BitTorrent client also generates a cache file that contains data about the status of a download. These cache files are used as a recovery system so that a torrent can resume from the same point if the downloading process is interrupted. Therefore, cache files provide evidence of the downloading or seeding of specific files.

3. BitTorrent Case

In the BitTorrent case study conducted by Kwan, *et al.* [6], no torrent file, whether the original or the backup, was ever found on the suspect's computer. Also, a cookie pertaining to the newsgroup forum was not found on the suspect's computer. According to the Bayesian belief network model created in the study and on the basis of other observed evidence, there is still a 92.27% chance that the suspect's computer was used as the initial seeder to distribute an infringing movie on a BitTorrent network.

The Bayesian belief network for the BitTorrent case is shown in Figure 1. Tables 1 and 2 list the hypotheses and the evidence involved in the case, respectively.

4. Bayesian Belief Networks

This section examines the semantics of a Bayesian belief network and reviews the topology of the model constructed for the BitTorrent case.

Table 1. Hypotheses in the BitTorrent case.

Hypothesis	Description
H	The seized computer was used by the seeder to share the pirated file on a BitTorrent network
H_1	The pirated file (destination file) was copied from the seized optical disk (source file) to the seized computer
H_2	A torrent was created from the pirated file
H_3	The torrent was sent to a newsgroup for publishing
H_4	The torrent was activated, which caused the seized computer to connect to the tracker server
H_5	The connection between the seized computer and the tracker was maintained

Table 2. Evidence in the BitTorrent case.

Evidence	Description
E_1	Modification time of the destination file was identical to that of the source file
E_2	Creation time of the destination file was after its own modification time
E_3	Hash value of the destination file matched that of the source file
E_4	BitTorrent client software was installed on the seized computer
E_5	File link for the pirated file (shared file) was created
E_6	Pirated file existed on the hard disk of the seized computer
E_7	Torrent creation record was found
E_8	Torrent existed on the hard disk of the seized computer
E_9	Peer connection information was found on the seized computer
E_{10}	Tracker server login record was found
E_{11}	Torrent activation time was corroborated by its MAC time and link file
E_{12}	Internet history record of the torrent publishing website was found
E_{13}	Internet connection was available
E_{14}	Cookie of the website of the newsgroup was found
E_{15}	URL of the website was stored in the web browser
E_{16}	Web browser software was available
E_{17}	Internet cache record regarding the publishing of the torrent was found
E_{18}	Internet history record regarding the tracker server connection was found

A Bayesian belief network is a graphical structure for representing and reasoning about an uncertain domain. The key feature is that a Bayesian belief network provides a method for decomposing a probability distribution into a set of local distributions. In order to construct a

Bayesian belief network, it is necessary to first specify the structure of the domain and then quantify the influences. This is why attention must be paid to the topology of a Bayesian belief network. This section describes two methods for examining the topology of a Bayesian belief network.

The nodes of a Bayesian belief network represent a set of random variables $X = \{X_1, \ldots, X_n\}$ from the domain. A set of directed arcs connect pairs of nodes $X_i \rightarrow X_j$. The structure or topology of the network captures qualitative relationships between variables. Two nodes are connected by a directed arc, which expresses the "direct causal influences" between the two nodes. For example, in Figure 1, H_1 denotes "The pirated file (destination file) was copied from the seized optical disk (source file) to the seized computer" while E_1 denotes "Modification time of the destination file was identical to that of the source file." Since H_1 is a direct cause of E_1, there is a directed arc from H_1 to E_1.

A node is a parent of a child node, if there is an arc from the former to the latter. If there is a directed chain of nodes, one node is an ancestor of another if it appears earlier in the chain. A node is a descendant of another node if it appears later in the chain. For example, in Figure 1, H_2 is the parent of E_5; H is an ancestor of E_5; and E_{18} is a descendant of H.

Since a directed arc connecting two nodes represents a direct causal influence between the two nodes, a parent denotes the direct cause of a child, and the descendants of a node represent the effects of the node.

A Bayesian belief network is a directed acyclic graph (DAG) that expresses conditional independent statements regarding its nodes. Each node is associated with a conditional distribution $P(X_i \mid Parents(X_i))$. Let $Parents(V)$ be the set of the parents of a variable V in a DAG. Let $Descendants(V)$ be the set of the descendants of a variable V in a DAG. Then, a DAG G is a representation of the independent statements: for all variables V in a DAG G: $I(V, Parents(V), NonDescendants(V))$, which means that every variable is conditionally independent of its non-descendants given its parents. In other words, given the direct causes of a variable, the belief in the variable is not influenced by any other variable, except possibly by its effects.

The resulting method, which we call Method 1, is specified as follows: **Method 1**: Given a graphical influence model, the above property can be used to examine whether or not a Bayesian belief network is constructed properly. Each node in a model is examined to check whether or not it is conditionally independent of its non-descendants given its parents.

Algorithm 1: Pearl's network construction algorithm [9].

1: Choose the relevant variables $\{X_1, \ldots, X_n\}$ that describe the domain
2: Choose an ordering on the variables $\{X_1, \ldots, X_n\}$
3: **for all** X_i, $i = 1..n$ **do**
4: Add variable X_i to the network
5: Add arcs to the X_i node from some minimal set of nodes already in the network, $Parents(X_i)$, such that the following conditional independence property holds:

$$P(X_i|X'_1, \ldots, X'_m) = P(X_i|Parents(X_i))$$

where $X'_1, \ldots, X'_m$ are the variables preceding X_i
6: **end for**
7: Define the conditional probabilities for the variables $\{X_1, \ldots, X_n\}$

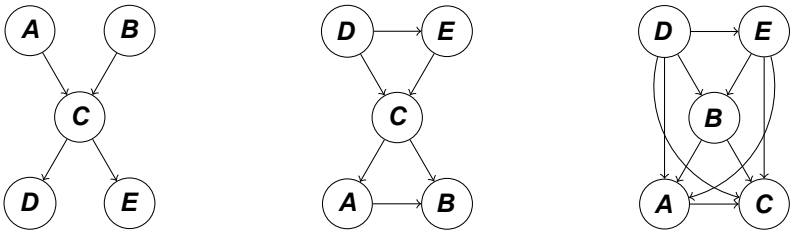
The second method, which we call Method 2, examines whether or not the topology is constructed properly. It uses Pearl's network construction algorithm (Algorithm 1) [9]. Note that Pearl's algorithm requires the user to supply an ordering on the variables.

Method 2: Given a graphic influence model, Pearl's algorithm is used to derive a compact network. This network is compared with the given graphic influence model.

To illustrate the methodology, we use the medical diagnosis example from the "Asia Problem," which was specified by Lauritzen and Spiegelhalter [7] and subsequently modified by Korb and Nicholson [5]. The problem involves a patient who has been suffering from Dyspnoea (shortness of breath). The patient is concerned that he has lung cancer. It is known that pollution and smoking increase the cancer risk. Lung cancer can affect the patient's breathing (Dyspnoea) and increase the chance of the patient having a positive x-ray. The preceding two sentences are referred to as "story statements."

Let A denote "Pollution," B denote "Smoking," C denote "Cancer," D denote "X-ray," and E denote "Dyspnoea." Thus, the set of relevant variables used to construct the Bayesian belief network is: $\{A, B, C, D, E\}$.

First, we choose the ordering $\{A, B, C, D, E\}$. We start with variable A as the root node and add B to the network (Figure 2(a)). According to the story statement, there is no causal relationship between A and B, i.e., they are independent of each other. There is no minimal set of nodes in the network, Parents(X_i), such that the conditional independence property is satisfied. Therefore, no arc is added between A and B.



(a) $\{A, B, C, D, E\}$. (b) $\{D, E, C, A, B\}$. (c) $\{D, E, B, A, C\}$.

Figure 2. Networks generated by various orderings.

The next variable added to the network is C. According to the story statement, pollution (A) and smoking (B) both increase the chance of cancer (C). The minimal set of nodes (parents) such that the conditional independence property is satisfied is $\{A, B\}$. Therefore, arcs are added from A to C and from B to C.

The next variable added is D. According to the story statement, cancer (C) can affect the patient's breathing (Dyspnoea) (E) and increase the chance of having a positive X-ray (D). The minimal set of nodes is $\{C\}$. Therefore, an arc is added from C to D.

Finally, variable E is added. The minimal set of nodes is $\{C\}$ and, therefore, an arc is added from C to E.

As a second example, we choose the ordering $\{D, E, C, A, B\}$. We start with variable D as the root node and add E to the network (Figure 2(b)).

We now ask if E is independent of D. According to the story statement, cancer (C) affects breathing (E) and increases the chance of having a positive x-ray (D). In other words, D and E have a common cause C. If the presence of either D or E is known, this will affect the probability of the other being present. Therefore, an arc is added from D to E.

Next, variable C is added. Since cancer (C) affects breathing (E) and increases the chance of having a positive x-ray (D), C is directly dependent on both D and E. Therefore, two arcs are added from D to C and from E to C.

Next, variable A is added. According to the story statement, pollution (A) or smoking (B) increase the chance of cancer (C). Therefore, an arc is added from C to A.

Finally, variable B is added to the network. According to the story statement, pollution (A) or smoking (B) increase the chance of cancer (C). Therefore, an arc is added from C to B.

At this point, we observe that C is the common cause of A and B, and that A and B are dependent. However, according to the story statement, A and B are independent. Therefore, an additional arc must be added from A to B, which makes A and B independent.

Let us now consider a third example with the ordering $\{D, E, B, A, C\}$. We start with variable D as the root node and add E to the network (Figure 2(c)). Following the same reasoning as in the previous example, an arc is added from D to E.

Next, we add variable B (instead of C in the preceding example). According to the story statement, pollution (A) or smoking (B) increase the chance of cancer (C). Having cancer affects breathing (E) and the chance of having a positive x-ray (D). Therefore, establishing the presence of D or E affects the probability of the presence of B. Thus, we add arcs from D to B and from E to B.

Next, we add variable A. According to the story statements, pollution (A) or smoking (B) increase the chance of cancer (C). Having cancer (C) affects breathing (E) and the chance of having a positive x-ray (D). Therefore, we add two arcs from D to A and from E to A.

At this point, we observe in the resulting network that D is the common cause of A and B, while E is the common cause of A and B; this implies that A and B are dependent. Since A and B are independent according to the story statement, an additional arc is added from B to A to make A and B independent.

Next, we add variable C. Using the same reasoning as above in relation to A, we finally obtain the network in Figure 2(c).

The three examples demonstrate that different node orderings can result in different network structures. Intuitively, it is desirable to build the most compact network possible. Korb and Nicholson [5] provide three reasons for constructing compact networks. First, the more compact the network, the fewer the probability values that require to be specified (probability updates are more efficient from the computational point of view). Second, an overly dense network may not represent independence in an explicit manner. Third, an overly dense network may fail to represent the causal dependencies in the domain.

According to Pearl [9], if the ordering of variables reflects causal reasoning, then the algorithm arrives at the most compact network possible, which enables easier assessments of the probability distributions. Of the three examples discussed above, only the first ordering $\{A, B, C, D, E\}$ is consistent with cause and effect. Since the orderings in the second and third examples are not consistent with cause and effect, the resulting Bayesian belief networks are not compact.

5. BitTorrent Model Revisited

We apply the two methods discussed in the previous section to the model in Figure 1. Since there are 24 nodes in the model, there are 24 conditional independence statements. The following conditional independence statements correspond to the five nodes, H, H_1, H_2, E_1 and E_8:

- $I(H, \emptyset, \emptyset)$
- $I(H_1, H, \{H_2, \ldots, H_5, E_4, \ldots, E_{18}\})$
- $I(H_2, H, \{H_1, H_3, \ldots, H_5, E_1, \ldots, E_3, E_9, \ldots, E_{18}\})$
- $I(E_1, H_1, \{E_2, E_3, H_2, H_3, \ldots, H_5, E_4, \ldots, E_{18}\})$
- $I(E_4, \{H_2, H_3\}, \{H, H_1, H_3, \ldots, H_5, E_1, \ldots E_3, E_5, \ldots, E_{18}\})$

We use the last independence statement regarding E_4 to analyze the topology of the DAG in Figure 1. First, we ask if it is true that given H_2, H_3 (i.e., parent of E_4), our belief in E_4 would be conditionally independent of its non-descendants. In order to answer this, we look for non-descendants that may affect E_4. If one is found, then the topology regarding E_4 in Figure 1 does not satisfy the requirement of $I(V, Parents(V), NonDescendants(V))$.

Next, we create the Bayesian belief network using Pearl's algorithm. To simplify the problem, we discard H and use the set of variables $\{H_i, E_1, \ldots, E_{18}\}$.

Upon applying the algorithm, we discover that H_3 should not be the parent of E_4. Also, H_4 should be the parent of E_{11}.

In other words, "The torrent was sent to a newsgroup for publishing" (H_3) does not directly cause "BitTorrent client software was installed on the seized computer" (E_4). Therefore, the arc between them in Figure 1 should be removed. Also, "The torrent was activated which caused the seized computer to connect to the tracker server" (H_4) directly causes "Torrent activation time was corroborated by its MAC time and link file" (E_{11}). Therefore, an arc is created to connect the cause (H_4) to the effect (E_{11}).

We reconstruct the Bayesian belief network using the variables in [6]. The new Bayesian network is shown in Figure 3.

Figure 4 shows the results obtained when all the evidence in the new model is set to 100% "Yes." In particular, we obtain 97.67% "Yes" for H_1; 99.64% "Yes" for H_2; 99.86% "Yes" for H_3; 98.94% "Yes" for H_4; and 98.48% "Yes" for H_5. On the other hand, if all the evidence is set to 100% "Yes" in the original model, the corresponding results are 99.7%

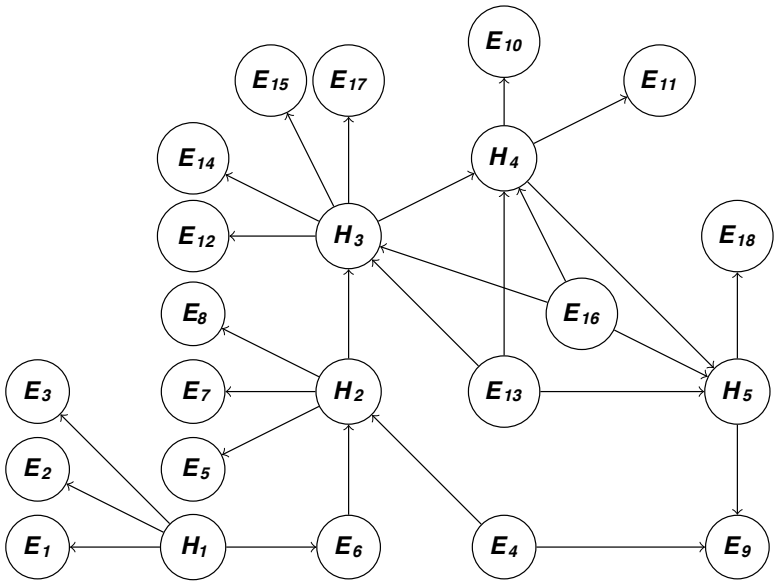


Figure 3. Revised Bayesian network for the BitTorrent case.

"Yes" for H_1; 99.9% "Yes" for H_2; 99.9% "Yes" for H_3; 99.8% "Yes" for H_4; and 94.1% "Yes" for H_5.

Figure 5 shows the results obtained with the new model when there is no evidence of E_8 and E_{10}. In particular, we obtain 97.67% "Yes" for H_1; 96.91% "Yes" for H_2; 99.85% "Yes" for H_3; 83.68% "Yes" for H_4; and 98.44% "Yes" for H_5. On the other hand, if there is no evidence of E_8 and E_{10} in the original model, the corresponding results are 92.7% "Yes" for H_1; 99.7% "Yes" for H_2; 98.3% "Yes" for H_3; 99.8% "Yes" for H_4; and 94.1% "Yes" for H_5.

The drop for H_4 from 99.8% "Yes" in the original model to 83.68% "Yes" in the new model is significant. The drop, which is due to the change in the network topology, does not necessarily imply that the new model is more sensitive. Nevertheless, the two methods help create better models that depict direct causation and help visualize the relationships between various hypotheses and pieces of evidence in a complex legal argument. In the case of a large network, the two methods provide systematic approaches by which an investigator may establish, demonstrate and negate challenges to the reliability of findings based on the digital evidence.

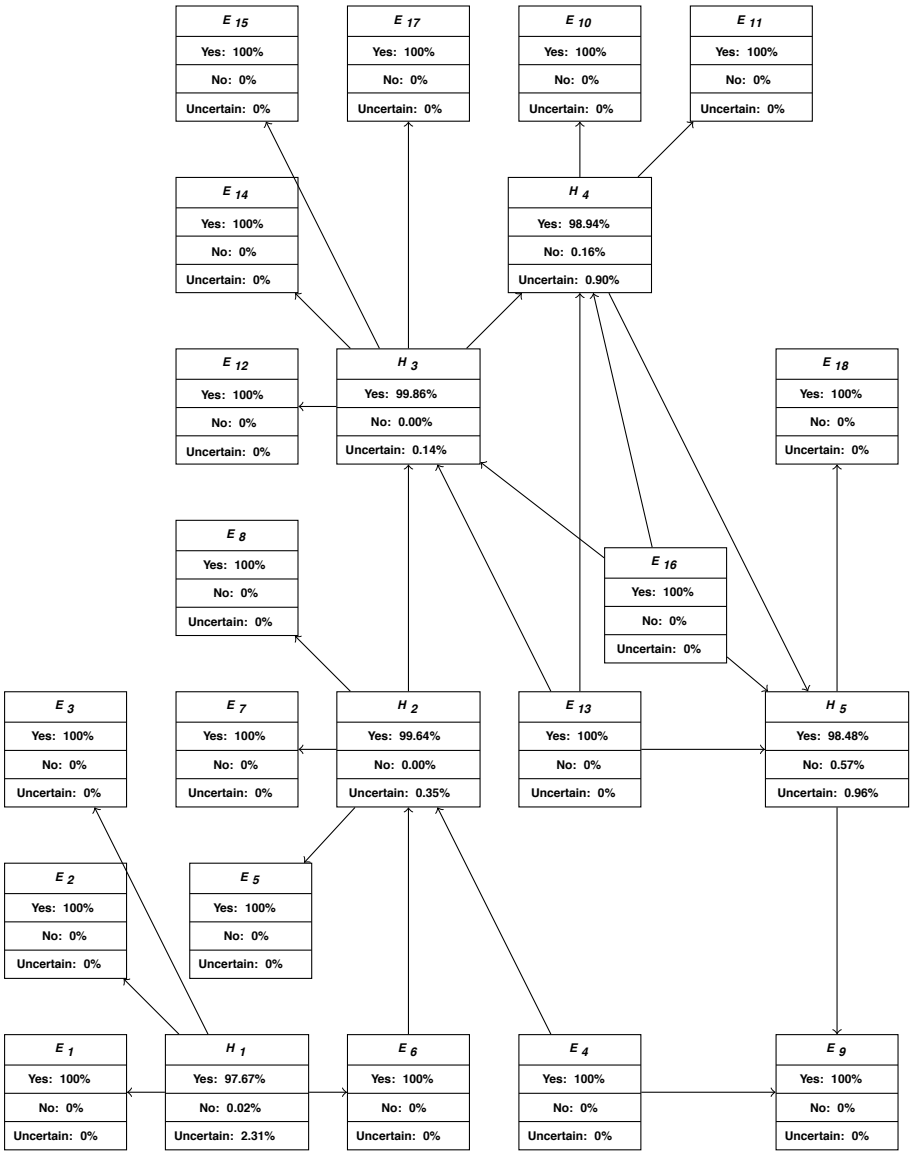


Figure 4. All evidence set to 100% "Yes."

6. Conclusions

The two methods presented for analyzing Bayesian belief network topologies enable investigators to systematically construct, demonstrate and challenge Bayesian belief networks, thereby providing a powerful framework for reasoning about digital evidence. The methods are im-

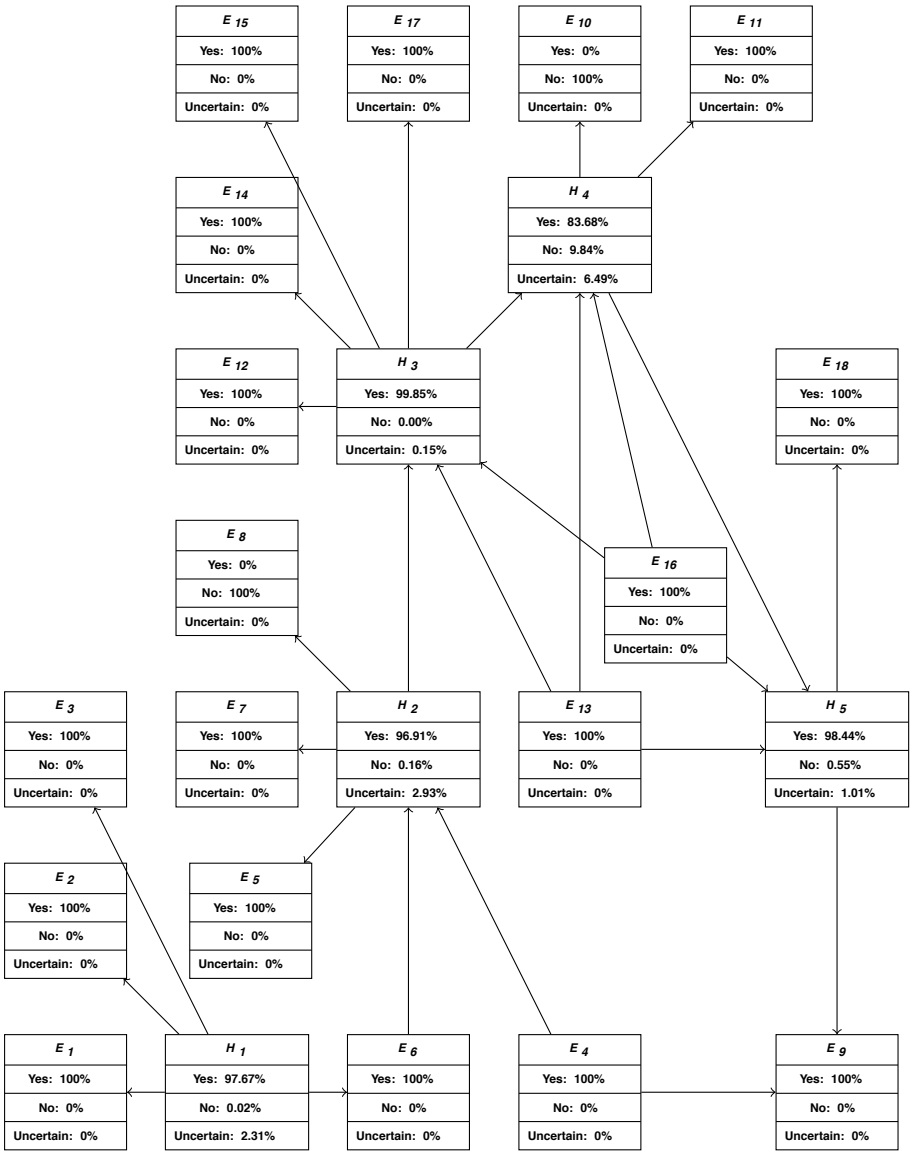


Figure 5. Evidence E_8 and E_{10} set to 100% "No."

portant because if any reasoning based on a Bayesian belief network is presented in court, it will be required to demonstrate that the method used to create the network is robust, reliable and follows an established protocol. In particular, since subjectivity is involved in constructing a

Bayesian belief network, there should be adequate justification for the choices made in network construction.

Method 1 described in this paper ensures that the nodes in a Bayesian belief network satisfy the key requirement that every variable is conditionally independent of its non-descendants given its parents. In other words, given the direct causes of a variable, the belief in a variable is not influenced by any other variable, except possibly by its effects. Method 2 uses Pearl's algorithm to ensure that a Bayesian belief network is constructed properly. Specifically, it guarantees the generation of the most compact network if the ordering on the variables reflects causal reasoning. Moreover, the method can be used to verify and explore the relationships existing between network nodes.

Cohen [1] has stated that the science of digital forensic examination is in its infancy. For the science to become more mature, important questions such as "What makes a digital evidence reasoning model appropriate?" should be asked and answered. Our work on analyzing Bayesian belief network topologies is a first step in this direction with regard to Bayesian models for legal reasoning. Our future research will explore other issues such as model refinement, probability adjustment, irrelevant factor elimination, latent factor addition and causal relationship adjustment.

References

[1] F. Cohen, Two models of digital forensic examination, *Proceedings of the Fourth IEEE International Workshop on Systematic Approaches to Digital Forensic Engineering*, pp. 42–53, 2009.

[2] O. de Vel, N. Liu, T. Caelli and T. Caetano, An embedded Bayesian network hidden Markov model for digital forensics, *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, pp. 459–465, 2006.

[3] Hong Kong Special Administrative Region High Court, Probation Action Judgment, Wang Din Shin v. Nina Kung alias Nina T. H. Wang, HCPA No. 8 of 1999 (Chapter 20, paragraphs 1–8), Hong Kong, China (`legalref.judiciary.gov.hk/doc/judg/word/vetted/other/en/1999/HCAP000008A_1999.doc`), 1999.

[4] J. Keppens, Q. Shen and B. Schafer, Probabilistic abductive computation of evidence collection strategies in crime investigation, *Proceedings of the Tenth International Conference on Artificial Intelligence and Law*, pp. 215–224, 2005.

[5] K. Korb and A. Nicholson, *Bayesian Artificial Intelligence*, Chapman and Hall/CRC, Boca Raton, Florida, 2011.

[6] 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.

[7] S. Lauritzen and D. Spiegelhalter, Local computations with probabilities on graphical structures and their applications to expert systems, *Journal of the Royal Statistics Society, Series B (Methodological)*, vol. 50(2), pp. 157–224, 1988.

[8] R. Lee, S. Lang and K. Stenger, From digital forensic report to Bayesian network representation, *Proceedings of the IEEE International Conference on Intelligence and Security Informatics*, pp. 303–306, 2009.

[9] J. Pearl, *Probabilistic Reasoning in Intelligent Systems*, Morgan Kaufmann, San Francisco, California, 1997.