A Generic Bayesian Belief Model for Similar Cyber Crimes

Hayson Tse, Kam-Pui Chow, Michael Kwan

Chapter 17

A GENERIC BAYESIAN BELIEF MODEL FOR SIMILAR CYBER CRIMES

Hayson Tse, Kam-Pui Chow and Michael Kwan

Abstract Bayesian belief network models designed for specific cyber crimes can be used to quickly collect and identify suspicious data that warrants further investigation. While Bayesian belief models tailored to individual cases exist, there has been no consideration of generalized case modeling. This paper examines the generalizability of two case-specific Bayesian belief networks for use in similar cases. Although the results are not conclusive, the changes in the degrees of belief support the hypothesis that generic Bayesian network models can enhance investigations of similar cyber crimes.

Keywords: Bayesian networks, DDoS attacks, BitTorrent file sharing

1. Introduction

One of two alternative strategies is typically employed to collect digital evidence during an investigation [5]. The first is to use staff with limited forensic training and seize everything. The second is to use skilled experts to perform selective acquisition. Given the resource constraints and expanding file storage capacities, it is not always feasible to retrieve all the evidence and to conduct a thorough analysis of all the digital traces. Indeed, there is no option for first responders but to make on-site acquisition decisions.

Sullivan and Delaney [13] recommend that investigators should analyze incomplete information (prior probability distributions), adjust their opinions (conditional probabilities) based on experience (observed information), and incorporate all the relevant information in an analytical process that reflects the extrapolation of experience. Bayesian reasoning supports these recommendations. It provides an investigator with a numerical procedure to revise beliefs based on expert knowledge

and any new evidence that is collected. The investigator computes the probability of an evidentiary item under a given hypothesis and evaluates the likelihood that the evidentiary item is conclusive based on the hypothesis.

This paper examines the feasibility of designing a generic Bayesian network model that applies to similar cyber crimes. Two Bayesian network models are examined, one constructed for a distributed denial-of-service (DDoS) attack case that is used in a denial-of-service (DoS) case, and the other constructed for a BitTorrent file sharing case that is used for an eMule file sharing case. Hypothesis testing of the degrees of belief supports the notion that a generic per-case model can be applied to similar cases.

2. Forensic Case Assessment and Triage

Backlog in digital forensic laboratories is common. In 2009, the United Kingdom Association of Chief Police Officers described the backlog in analyzing seized data "as one of the biggest e-crime problems" [2]. Experience has shown that an increase in the number of staff alone does not reduce backlogs.

Triage is useful in situations involving limited resources. In a medical emergency, if there are insufficient resources to treat all the victims, the casualties are sorted and prioritized. Treatments are targeted towards victims who can benefit the most. Those who are beyond help or do not need treatment urgently are not treated or are treated later. The medical community has adopted methods and protocols for determining how to prioritize and treat victims during triage.

Similarly, triage should be performed when there is insufficient time to comprehensively analyze digital evidence at a crime scene. When performing triage, a first responder would attempt to quickly identify suspicious data that warrants further investigation and eliminate data that is not relevant. Sebastian and Gomez [5] have shown that laboratory workloads can be reduced by performing triage using automated tools. Additionally, Rogers, *et al.* [12] have proposed a model for on-site identification, analysis and interpretation of digital evidence without having to acquire a complete forensic image.

Bayesian belief networks have been used to determine if investigations are worth undertaking [9]. Overill and Silomon [10] use the term "digital metaforensics" to quantify the investigation of digital crime cases. They argue that a preliminary filtering or pre-screening phase could help rank the probable order of evidential strength. Overill, *et al.* [9] emphasize that it is the duty of digital forensic practitioners to retrieve digital

traces to prove or refute alleged computer acts. They maintain that, given the resource constraints, it is not always feasible or necessary to retrieve all the related digital traces and to conduct a thorough digital forensic analysis.

Overill, *et al.* [9] and Cohen [3] have specified cost-effectiveness metrics for conducting cost-benefit analyses of forensic investigations, including cost-efficiency [9] and return-on-investment studies [3]. In particular, Overill, *et al.* [9] have proposed a two-phase schema for performing digital forensic examinations at minimal cost. The first phase of the schema is pre-processing, which is the detection of digital traces. Pre-processing includes enumerating the set of traces that are expected to be present in a seized computer; the enumeration is based on the type of computer crime that is suspected of having been committed. The second phase of the schema is the analysis of the traces, for which a Bayesian belief network is used.

3. Bayesian Networks

A Bayesian network offers several advantages to digital forensic practitioners. After a Bayesian network has been constructed, it is easy to understand and apply, which can speed up an investigation. Also, a Bayesian network ensures that all the available information is considered. This can prevent human error in overlooking small, but nevertheless, vital factors. A Bayesian network can also be used to make inferences and find patterns that may be too complicated for human practitioners.

Bayesian networks are graphical structures that represent probabilistic relationships between a number of variables and support probabilistic inference with the variables [8]. According to Heckerman, *et al.* [6], the Bayesian probability of an event x is a person's "degree of belief" in the event. Data is used to strengthen, update or weaken the belief.

The nodes in a Bayesian network represent a set of random variables $X = \{X_1, \ldots X_i, \ldots, X_n\}$ defined by two components:

- **Qualitative Component:** A directed acyclic graph (DAG) in which each node represents a variable in the model and each edge linking two nodes (i.e., variables) indicates a statistical dependence between the nodes.
- **Quantitative Component:** A conditional probability distribution $p(x_i|pa(x_i))$ for each variable X_i, $i = 1, \ldots, n$, given its parents in the graph $pa(x_i)$.

A DAG represents a set of conditional independence statements regarding the nodes. Each node is annotated with a conditional distri-

bution $P(X_i \mid Parents(X_i))$. Let $Parents(V)$ be the set of parents of a variable V in a DAG G and let $Descendants(V)$ be the set of the descendants of variable V. Then, the DAG G expresses the independence statements: for all variables V in G: $I(V, Parents(V), NonDescendants(V))$ [11], 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 beliefs in the variable are not influenced by any other variable except possibly by its effects.

A Bayesian network yields a complete joint probability distribution for all possible combinations of variables over X given by:

$$P(X_1, \ldots, X_i) = \prod_{i=1}^{n} P(X_i | Parents(X_i)).$$

Constructing a Bayesian network involves three tasks. First, the variables and their initial probabilities are identified. Second, the relationships between the variables are identified and expressed in a graphical structure; this is usually done by domain experts and is comparable to knowledge engineering. Third, the probabilities required for the quantitative analysis are assigned. The probabilities are generally obtained from statistical data, the research literature and human experts. Automated construction of a Bayesian network is feasible when there is an adequate amount of unbiased data.

4. Generic Bayesian Network Crime Model

At the start of an investigation, a Bayesian network model for the crime must be available. The first responders at the crime scene use the Bayesian network to quickly identify relevant information.

Figure 1 shows an example Bayesian network for a DDoS attack created using the SamIam 3.0 modeling tool [1]. In a Bayesian network, "No" indicates that the event described by the corresponding variable did not occur; "Yes" indicates that the event occurred; and "Uncertain" indicates that there is doubt if the event occurred or not. All the available evidence is entered into the network by selecting a state for each variable and, if necessary, entering a probability distribution.

During an investigation, if a first responder finds evidence associated with all the variables in the Bayesian network, then all the nodes in the network would be set to "Yes." Upon propagating the probability computations in the example Bayesian network, the probabilities that the hypotheses H_1, H_2 and H are "Yes" become 99.73%, 100.00% and 93.26%, respectively. The result is shown in Figure 2.

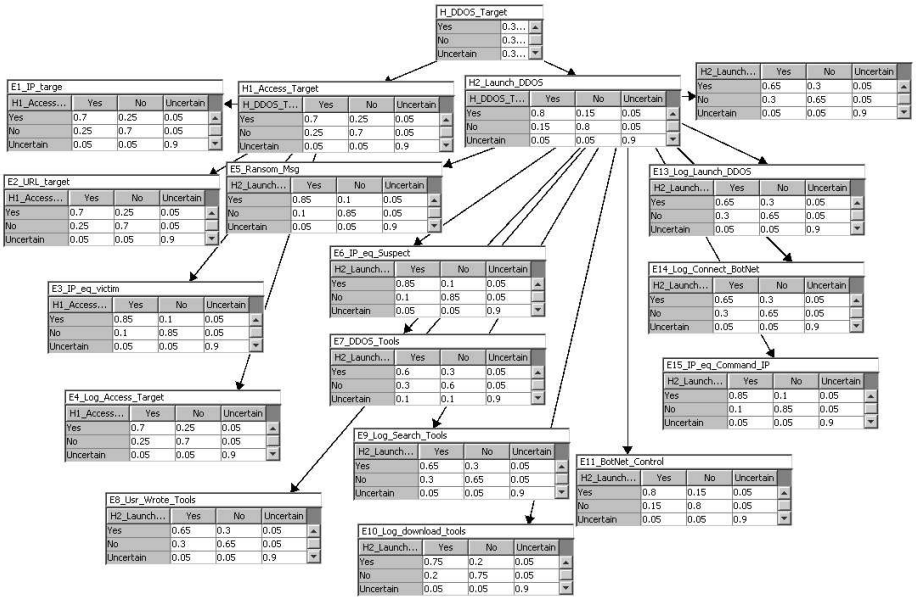

Figure 1. Bayesian network for a DDoS attack.

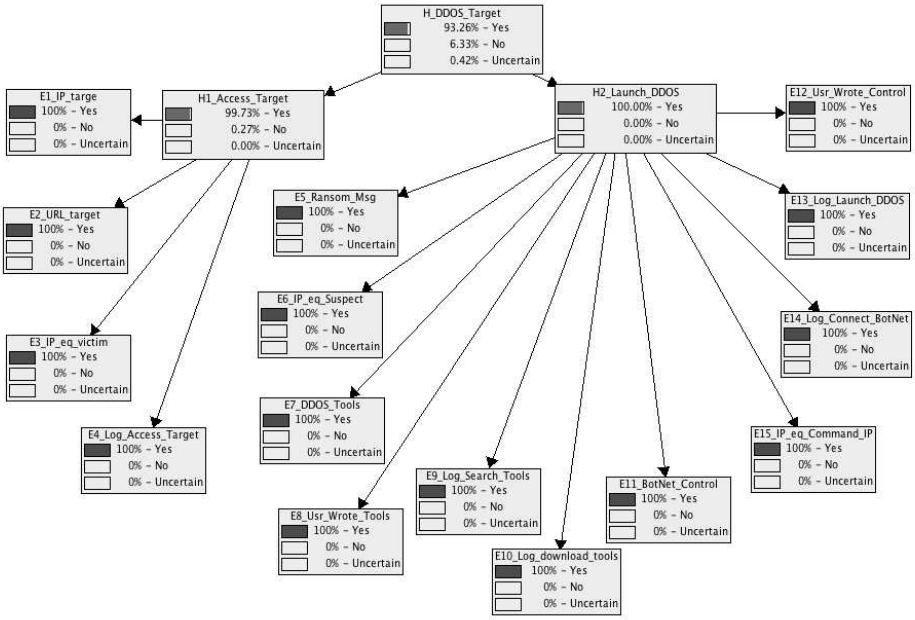

Figure 2. Bayesian network for a DDoS attack (variables set to "Yes").

Of course, if the first responder finds evidence associated with some of the variables, then only the associated nodes in the network would be set to "Yes." The values of the hypotheses H_1, H_2 and H would change accordingly.

Bayesian networks cannot be expected to give perfect answers. A Bayesian network is a simplification of a complicated situation, operating on information that is uncertain in the first place. Furthermore, a network only gives the likelihood of occurrence of a particular event (e.g., hypothesis).

Generic Bayesian network models of similar types of cyber crimes can be used when conducting triage at crime scenes. Experienced Hong Kong criminal investigators have developed Bayesian networks to represent the relationships between events and hypotheses in a DDoS attack case and in a BitTorrent file sharing case. The two networks are used to explore the feasibility of employing generic Bayesian networks in criminal investigations. In the case of the first network, we assume that a DoS attack is an example of a DDoS attack in that a DoS attack is from a single source rather than from multiple sources. The second network explores the generalizability of the BitTorrent Bayesian network to the eMule peer-to-peer (P2P) file sharing network.

In the case of the Bayesian network for a DDoS attack, the main hypothesis H is:

- H: Seized computer was used to launch a DDoS attack against a target computer.

The sub-hypotheses are:

- H_1: Seized computer was used to access the target computer.
- H_2: Seized computer was used to launch a DDoS attack.

The evidence supporting H_1 is:

- E_1: IP address of the target computer was found on the seized computer.
- E_2: URL of the target computer was found on the seized computer.
- E_3: IP address of the target computer matched the accessed IP address (revealed by the ISP) at the material time.
- E_4: Log file records were found on the seized computer indicating that the target computer was accessed at the material time.

The evidence supporting H_2 is:

- E_5: Ransom messages were found on the seized computer for extorting money (or other benefits) from the victim.
- E_6: IP address of the seized computer matched the attacking IP address (revealed by the ISP) at the material time.
- E_7: DDoS tools were found on the seized computer.
- E_8: Evidentiary data was found on the seized computer indicating that the computer user wrote the DDoS tools.

- E_9: Log file records were found on the seized computer indicating that the computer user searched for DDoS tools on the Internet.
- E_{10}: Log file records were found on the seized computer indicating that the computer user downloaded DDoS tools from the Internet.
- E_{11}: The command and control program of a botnet was found on the seized computer.
- E_{12}: Evidentiary data was found on the seized computer indicating that the computer user wrote the command and control program of a botnet.
- E_{13}: Log file records were found on the seized computer indicating that the computer was used to launch a DDoS attack against the target computer via a botnet.
- E_{14}: Log file records were found on the seized computer indicating that the computer was connected to a botnet.
- E_{15}: IP address of the seized computer matched the botnet command and control IP address (revealed from the attacking bots) at the material time.

Our first evaluation assumes that a DoS attack is an example of a DDoS attack. The analysis uses evidence from an actual DoS attack case [4].

The case involved an individual who, on August 12, 2011 and August 13, 2011, launched DoS attacks on the Hong Kong Exchange website for 390 seconds and 70 seconds, respectively. On the suspect's computer, law enforcement authorities found a UDP flooder program, Internet connection logs and screen prints of the websites being attacked.

Based on the evidence, the values of E_1 to E_8 are set to "No" and E_9 to E_{15} are set to "Yes." The probabilities of H_1, H_2 and H given the evidence variables compute to 0.93%, 86.07% and 57.11%, respectively, as shown in Figure 3. Although the values are well below 100%, the suspect was convicted after a trial. At the trial, the suspect admitted that he flooded the website and made records of the attacks for educational purposes.

Our second evaluation uses a Bayesian network model created to explore the evidence observed by crime investigators in a Hong Kong criminal case regarding illegal file sharing using BitTorrent [7, 15]. Kwan, *et al.* [7] established the probability distributions of the hypotheses and evidentiary variables in the case. This enabled the quantification of the evidentiary strengths of the various hypotheses. Tse, *et al.* [14] revised the model and examined two methods for determining whether or not the Bayesian network could be refined. This analysis uses the model established by Tse, *et al.* [14], which is shown in Figure 4. The model incorporates the following hypotheses:

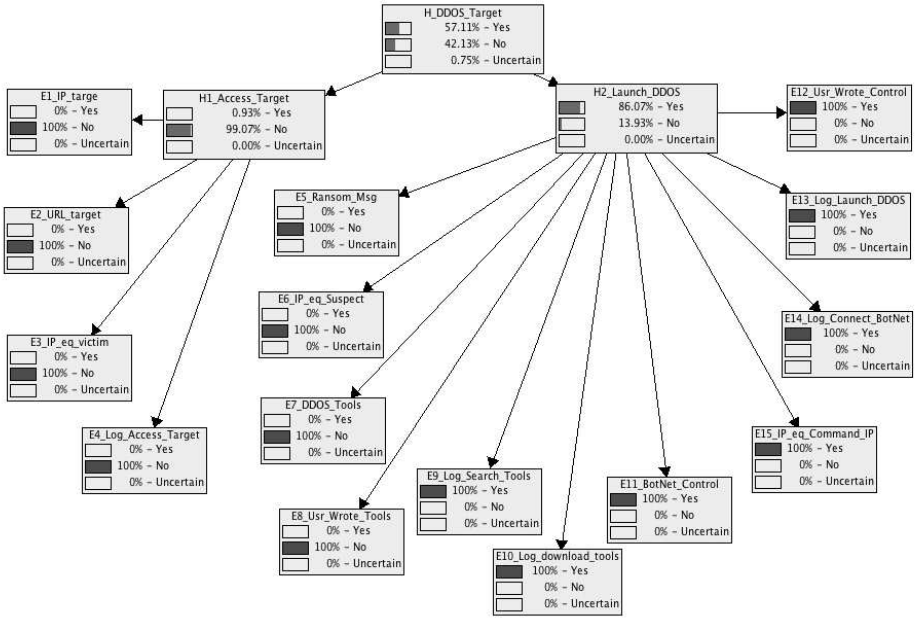

Figure 3. Bayesian network for the DoS attack (based on case evidence).

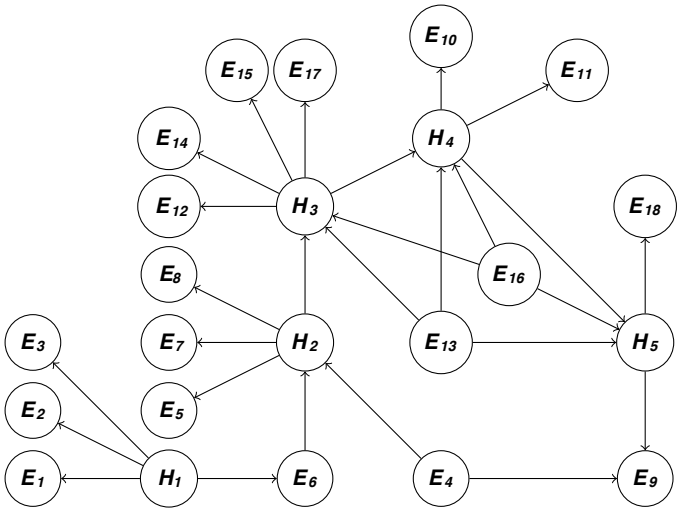

Figure 4. Bayesian network for the BitTorrent case.

- H: Seized computer was used by the seeder to share the pirated file on the BitTorrent network.
- H_1: Pirated file (destination file) was copied from the seized optical disk (source file) to the seized computer.
- H_2: Torrent was created from the pirated file.
- H_3: Torrent was sent to a newsgroup for publishing.
- H_4: Torrent was activated causing the seized computer to connect to the tracker server.
- H_5: Connection between the seized computer and the tracker was maintained.

The evidentiary variables in the model are:

- 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.

Figure 5 shows the revised BitTorrent Bayesian network when all the evidentiary variables are set to "Yes." The resulting probabilities for the hypotheses being "Yes" are 97.67% for H_1, 99.64% for H_2, 99.86% for H_3, 98.94% for H_4 and 98.48% for H_5.

In a P2P file sharing network, each computer in the network acts as a client or server. Individuals who want files and individuals who have files are all connected in the network. In the case of the eMule P2P network, the hashes of shared files are maintained in hash lists at eMule servers. Individuals search the servers for files of interest and are presented with the filenames and unique hash identifiers. The individuals then query

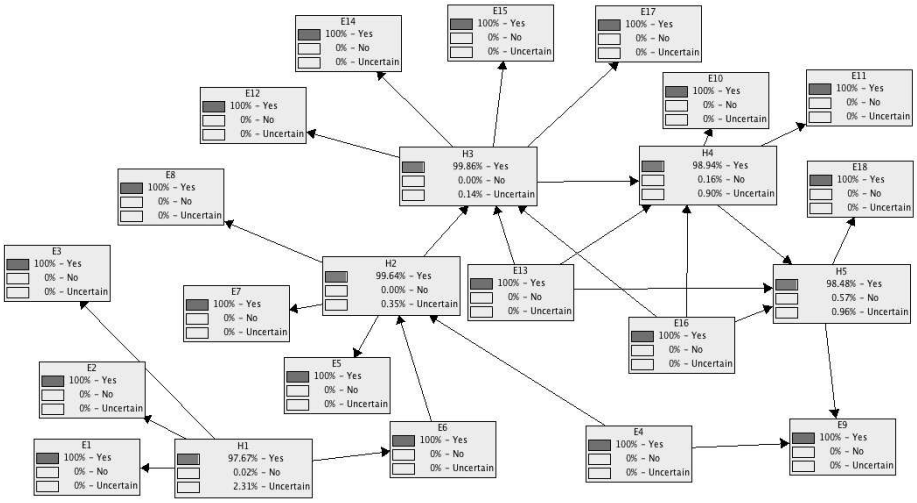

Figure 5. Revised BitTorrent Bayesian network (variables set to "Yes").

the servers for clients that have files that match the hash identifiers. The servers return sets of IP addresses with the locations of the clients. Chunks of the files are then swapped until the individuals who want the files have complete copies of the files.

If A has a complete version of a file that is of interest to B, C, D and E, then a P2P system would enable A to feed B with the first part (say one-quarter) of the file, feed C with the second quarter, D with the third quarter and E with the fourth quarter. Then, B, C, D and E would exchange what they have received from A until all four have the complete file. If A were to cut the connection after it distributed the four chunks, then B, C, D and E could still distribute the file amongst themselves. However, if A were to cut the connection before it distributed all four chunks, then B, C, D and E could distribute what they received amongst themselves, but they would be unable to obtain the complete file until another client joins the network with the complete file.

There are some differences between the BitTorrent and eMule P2P networks. In a BitTorrent network, there is no centralized location for a file or a hash list that is searched to locate files. Instead, users must receive or locate a file on an indexing website and download a file tracker (`.torrent` file). All the users who wish to share the complete file use the tracker to create the P2P network for the file. However, both BitTorrent and eMule need a central location to exchange information regarding the file identity and the IP addresses of users. The concepts of creating

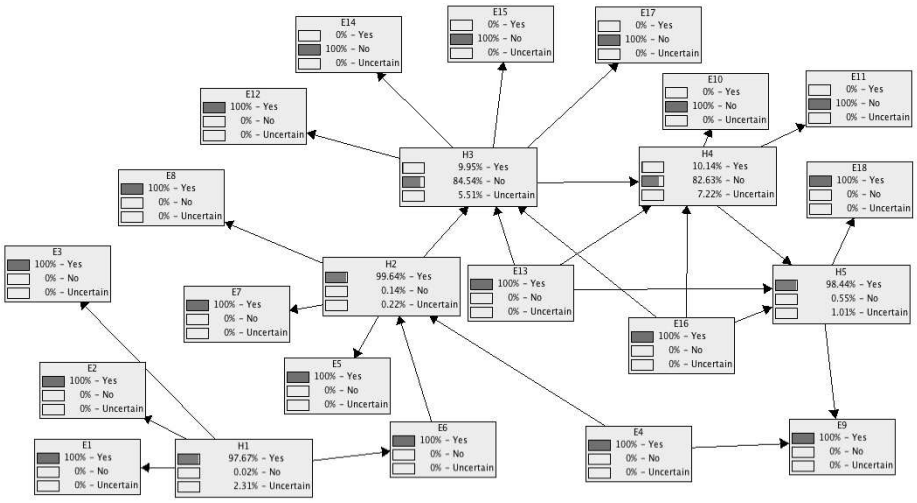

Figure 6. Revised BitTorrent Bayesian network (based on the eMule evidence set).

and using a hash list in eMule are equivalent to creating and using a `.torrent` file in BitTorrent.

For the purpose of the second analysis, in order to use the BitTorrent Bayesian network for an eMule case, the evidentiary items E_{10}, E_{11}, E_{14}, E_{15} and E_{17} are set to "No" while the remaining evidentiary items are set to "Yes." Figure 6 shows the updated Bayesian network. The probabilities that the hypotheses are "Yes" are: 97.67% for H_1, 99.64% for H_2, 9.95% for H_3, 10.14% for H_4 and 98.44% for H_5.

Although the changes to the degrees of belief in the two analyses are not conclusive, they provide support for our hypothesis that a generic Bayesian network model can be used quite effectively to analyze similar cyber crimes.

5. Conclusions

Generic Bayesian network models can be used to improve the quality of cyber crime investigations while reducing the effort and cost. The results of the evaluation of two Bayesian network models, one constructed for a DDoS attack case that was used in a DoS case, and the other constructed for a BitTorrent file sharing case that was used for an eMule file sharing case, support the notion that a generic case-specific model can be applied to similar cases.

Our future research will explore how a generic Bayesian network can be created to accommodate a larger number of similar cyber crimes. This network should be constructed carefully because, as the number of causal

nodes increases, the sizes of the probability matrices of the nodes grow exponentially. Our research plans also involve designing a dedicated user interface with abstraction support to enable law enforcement officers to interact with Bayesian networks in a flexible and intuitive manner.

References

[1] Automated Reasoning Group, SamIam, University of California at Los Angeles, Los Angeles, California (`reasoning.cs.ucla.edu/samiam`), 2010.

[2] R. Blincoe, Police sitting on forensic backlog risk, says top e-cop, *The Register* (`www.theregister.co.uk/2009/11/13/police_forensics_tool`), November 13, 2009.

[3] 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.

[4] District Court of the Hong Kong Special Administrative Region, HKSAR against Man-Fai Tse, Criminal Case No. 1318 of 2011, Hong Kong, China, 2012.

[5] L. Gomez, Triage in-Lab: Case backlog reduction with forensic digital profiling, *Proceedings of the Argentine Conference on Informatics and Argentine Symposium on Computing and Law*, pp. 217–225, 2012.

[6] D. Heckerman, A Tutorial on Learning with Bayesian Networks, Technical Report MSR-TR-95-06, Microsoft Research, Advanced Technology Division, Microsoft, Redmond, Washington, 1996.

[7] 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.

[8] R. Neapolitan, *Learning Bayesian Networks*, Prentice-Hall, Upper Saddle River, New Jersey, 2003.

[9] 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.

[10] R. Overill and J. Silomon, Digital meta-forensics: Quantifying the investigation, *Proceedings of the Fourth International Conference on Cybercrime Forensics Education and Training*, 2010.

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

[12] M. Rogers, J. Goldman, R. Mislan, T. Wedge and S. Debrota, Computer Forensics Field Triage Process Model, *Journal of Digital Forensics, Security and Law*, vol. 1(2), pp. 19–37, 2006.

[13] R. Sullivan and H. Delaney, Criminal investigations – A decision-making process, *Journal of Police Science and Administration*, vol. 10(3), pp. 335–343, 1982.

[14] H. Tse, K. Chow and M. Kwan, Reasoning about evidence using Bayesian networks, in *Advances in Digital Forensics VIII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 99–113, 2012.

[15] Tuen Mun Magistrates Court of the Hong Kong Special Administrative Region, HKSAR against Nai-Ming Chan, Criminal Case No. 1268 of 2005, Hong Kong, China, 2005.

[16] Y. Xiang and Z. Li, An analytical model for DDoS attacks and defense, *Proceedings of the International Multi-Conference on Computing in the Global Information Technology*, p. 66, 2006.