Multisource fusion for opportunistic detection and probabilistic assessment of homeland terrorist threats

Kathryn Blackmond Laskey[a] and Tod S. Levitt[b]

[a]SEOR Department, George Mason University, Fairfax, Virginia
[b]Information Extraction and Transport, Inc., Arlington, Virginia

ABSTRACT

Bayesian Network Fragments (BNFrags) provide a practical, computational methodology to encode a distributed library of computer-usable knowledge patterns for automated reasoning about aspects of homeland defense against terrorism. Multi-Entity Bayesian Networks provide a means of encoding repeated patterns and relationships in the form of BNFrags having variables that range over entities of a given type. New evidence either is matched to existing entities or triggers new entities to be hypothesized. BNFrag instances are created by replacing the variables by the names of entities in the situation. These BNFrags are combined to form situation-specific Bayesian networks (SSNs). We propose the use of MEBNs as the inferential cornerstone of a cumulative national, distributed knowledge base (KB) for homeland defense. In this paper we illustrate the use of MEBNs for these purposes with an example concerning a multi-city coordinated biowarfare attack. We show how current trends in the use of on-line reporting by health care and related facilities has the potential to enable opportunistic detection of and response to low probability, high consequence events for which it would otherwise be a practical impossibility to set up specifically directed monitoring capabilities.

Keywords:: Bayesian Networks, Bayesian Network Fragments, Multi-Entity Bayesian Networks, hypothesis space, counter-terrorism, homeland defense, biowarfare, multisource fusion, information fusion

1. INTRODUCTION

In the wake of recent terrorist attacks on the U.S. homeland, the growing array of potentially relevant sources of information concerning possible sources and alerts to terrorist attack on the United States is likely to increase even more rapidly. Concurrently efforts are being made to make these sources available in streaming form on the Internet, and to consolidate data interfaces so that web access is standardized and readily available. Each such source is formed around a core set of expertise in areas such as human or animal diseases, information assurance, chemical warfare, financial transactions supporting terrorist activity, etc.

Fusion of these sources is necessary if we are to detect and respond to patterns and interactions spanning the different areas. For example, biological warfare attacks must be carried out by operatives that are tracked independently of those sources that detect the use of biological weapons. Also, if a multi-site attack were to take place, there is no obvious way in which early detection of the coordination could be determined, yet multiple coordinated activity detection might be the one of the easier ways to get early tip-off and alerting of terrorist attacks.

In this paper we present a multi-source information fusion technique based on Bayesian Network technology, that is capable of providing the technology infrastructure necessary to support a wide-area, asynchronous, automated detection and alerting of such terrorist activities. We posit a notional concept of operations in which this technology is imbedded in a nationwide, distributed knowledge based for cross-source and multi-source detection and alerting of terrorist activities in the U.S.

The technological approach for a distributed homeland defense knowledge base is presented in Section 2. The concept of operations for the distributed KB is described in Section 3. Section 4 presents a realistic biowarfare terrorist scenario executed against multiple sites. Section 5 describes an illustrative model capable of operating against this scenario. The model takes the form of a collection of BNFrags organized as an MEBN. Although the model has been deliberately kept simple and the structure and probabilities have not been validated, it produces reasonable results on the test scenario, and the path to extension is clear.

2. BAYESIAN NETWORK FRAGMENTS AND MULTI-ENTITY BAYESIAN NETWORKS

A Bayesian Network (BN) consists of a dependency graph and a set of local probability distributions.[1,2] The dependency graph encodes qualitative relationships among a set of uncertain hypotheses. The local probability distributions encode

quantitative information about the strength of the dependency. Figure 1 shows a BN for an example used by Max Henrion to illustrate the phenomenon of "explaining away." Maria is visiting a friend when she begins to sneeze. She worries that she is getting a cold. Then she notices scratches on the furniture and relaxes: it is only her cat allergy acting up. The figure shows the dependency graph relating a set of hypotheses relevant to the causes of Maria's sneezing, along with a graphical depiction of the evolving belief states of the hypotheses. Cold and allergy have initial probabilities of about 8% and 3%, respectively. After Maria begins sneezing, they increase to 53% and 20%, respectively. When her sneezing is explained away by the allergy, the probability of the cold explanation drops to about 15%, whereas allergy increases to about 88% probability. This example shows how probability captures the non-monotonic character of plausible inference. No special machinery is required other than the independence assumptions and probability information encoded in the BN. The rapidly growing popularity of probability-based knowledge representations is in large part due to this ability to capture qualitative relationships in a straightforward and natural manner.

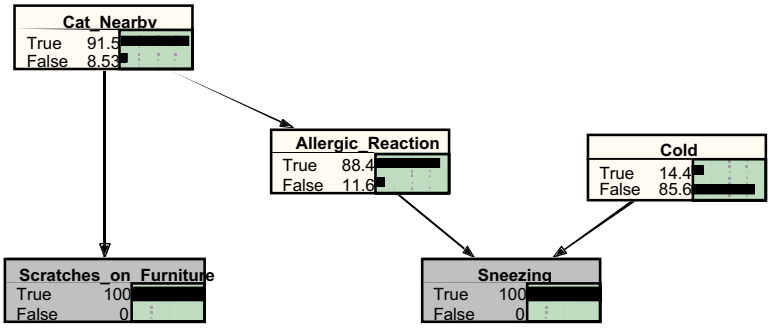
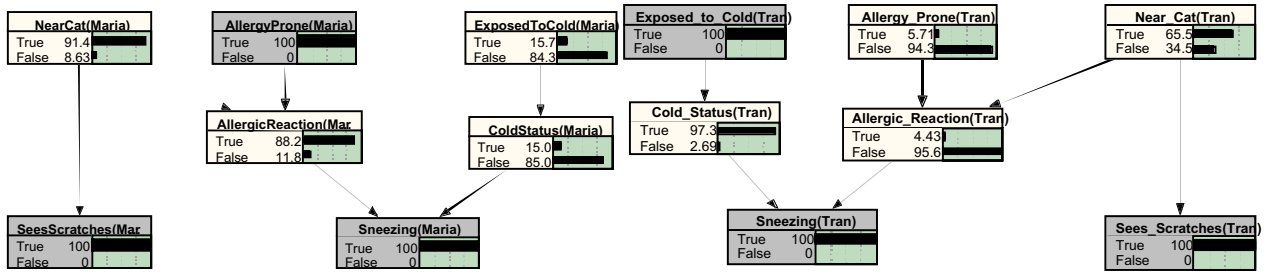


Figure 1 Bayesian Network Example

The BN of Figure 1 was constructed for Maria's particular case. Different probability distributions might well apply to different individuals who were sneezing and saw scratches. A major contributing factor to the success of BNs is their ability to generalize beyond a single individual to classes of similar individuals. If we include background variables, such as whether the person has a history of allergies and has been exposed to a cold, we can extend the BN of Figure 1 to a microworld theory of sneezing that applies to a population of individuals. Figure 2 illustrates how to extend our theory to generate plausibly different results when applied to different individuals in similar situations. Figure 2a shows that Maria, who is allergy prone and whose prior cold exposure is unknown, is probably suffering from an allergy and most likely does not have a cold. Figure 2 b shows that Tran, who also is sneezing and saw scratches, but is not allergy prone and was recently exposed to a cold, probably has a cold and is unlikely to be suffering from an allergy.



a. Maria's Case *b. Tran's Case*

Figure 2 Multi-Entity Bayesian Network Example

Figure 3 shows the probability information that needs to be specified for our microworld theory. It is sufficient to specify a probability that each hypothesis is true given each possible combination of truth-values for the hypotheses on which it depends (represented in the graph as the hypotheses at the tail of arrows pointing into the hypothesis). To specify a fully general probability distribution on seven binary hypotheses, we would have to specify a probability for

each of the $2^7 = 64$ possible combinations of truth-values for the seven hypotheses.* The global independence constraints encoded in the graph and the equality constraints encoded in the local probability distributions reduce the number of free parameters in our microtheory to just 11. More important for scalability, the number of free parameters in a BN scales with the product of the number of hypotheses and the number of probability distributions per hypothesis, whereas the number of free parameters in a general probability model scales exponentially in the number of hypotheses. This dramatic improvement in scalability is another reason for the popularity of BNs as a language for expressing probability information.

Variable	Parent Variable Values		True	False
ExposedToCold(*h*)			10%	90%
HasCold(*h*)	*ExposedToCold*(*h*) = *True*		75%	25%
	ExposedToCold(*h*) = *False*		1%	99%
AllergyProne(*h*)			1%	99%
AllergicReaction(*h*)	*AllergyProne*(*h*) = *True*	*NearCat*(*h*) = *True*	75%	25%
	AllergyProne(*h*) = *False*	*NearCat*(*h*) = *False*	1%	99%
		NearCat(*h*) = *True*		
		NearCat(*h*) = *False*		
Sneezing(*h*)	*AllergicReaction*(*h*) = *True*	*HasCold*(*h*) = *True*	99%	1%
		HasCold(*h*) = *False*		
	AllergicReaction(*h*) = *False*	*HasCold*(*h*) = *True*	5%	95%
		HasCold(*h*) = *False*		
NearCat(*h*)			3%	97%
SeesScratches(*h*)	*NearCat*(*h*) = *True*		60%	40%
	NearCat(*h*) = *False*		1%	99%

Figure 3: Probability Specification for Allergy Example

The generic BNFrag with structure as shown in Figure 2 and probabilities as shown in Figure 3 encodes a common-sense theory of sneezing that applies when Maria and Tran are replaced with any human being *h*. We call such a theory a *BN Fragment* or *"BNFrag" for short*. This BNFrag can be understood as a universally quantified statement:

> ***For every h in the relevant population of human beings, the joint probability distribution over the seven hypotheses represented in Figure 2 is given by the BN shown in Figure 2 and Figure 3.***

We reason about a particular sneezing episode by replacing the variable *h* by the name of an individual human and conditioning the generic *BNFrag* on evidence specific to the individual, as shown in Figure 2*a* and *b*. The inference method for using a general theory to draw plausible inferences from specific evidence is called *Bayes rule*. It is implemented by one of several known BN solution algorithms.[1,2] These algorithms also solve for maximum utility decision policies when the BNFrags are extended to include value and decision nodes; in which case they are called *decision graphs* or *influence diagrams*.[1,2]

A *Multi-Entity Bayesian Network*, or MEBN, is a collection of BNFrags that satisfy consistency criteria such that the collection specifies a probability distribution over attributes of and relationships among a collection of interrelated entities[3]. An MEBN implicitly encodes a probability distribution over an unbounded number of hypotheses. For any given problem, only a finite subset of these hypotheses will be relevant. To reason about specified target hypotheses given evidence about a particular situation, an ordinary finite Bayesian network, called a *situation-specific network* (SSN), is constructed from an MEBN knowledge base.[3] The SSN construction process is initiated when clusters of reports trigger firing of a *suggestor*. Suggestors are rules that use features of the situation to determine which hypotheses need to be represented. For example, the color of Maria's or Tran's shirt is not relevant to the task of inferring whether an allergy or a cold is present, and therefore need not be represented explicitly. The suggestor triggers retrieval of relevant BNFrags. Actual entities from the situation replace the variables in the BNFrags, as *Maria* and *Tran*

* Actually, only 63 probabilities are needed; the 64th can be obtained from the constraint that the probabilities sum to 1.

replace the variable *h* in the two BNFrags of Figure 2. After retrieval, the BNFrags are combined, possibly along with an already existing SSN, create a current SSN. Next, evidence is applied to the SSN and inferences are drawn about the target hypotheses. Finally, decision nodes are evaluated to determine what action needs to be taken. An architecture for SSN construction is shown in Figure 4.[4]

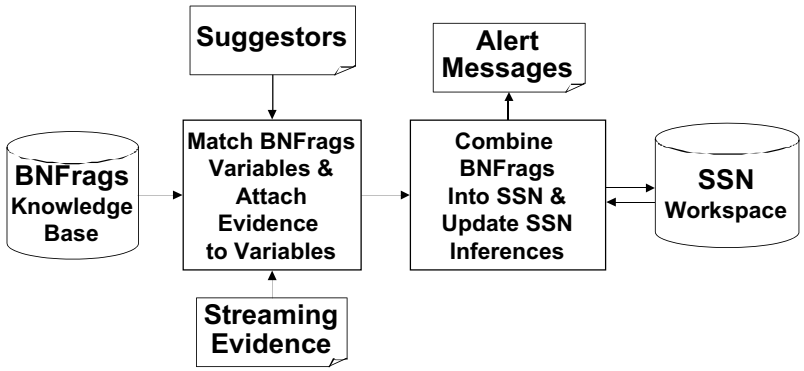


Figure 4: High Level Architecture for SSN Construction from MEBN Knowledge Base

3. NATIONAL KNOWLEDGE BASE FOR HOMELAND DEFENSE

The wide range of potential venues for terrorist attacks implies an equally wide range of areas of expertise that must be invoked to prevent, protect, detect and respond to potential homeland threats and attacks. Given any one threat, there is a virtually infinite number of locations and methods for delivery. Combinations of threats delivered in a coordinated attack make it a practical impossibility to identify and prepare for each possible scenario ahead of time. Nevertheless, there are patterns and regularities that can be exploited to anticipate, detect and head off terrorist incidents. Necessary precursor activities to terrorist incidents (e.g., logistical preparation, financial transactions, training and rehearsal) can be monitored and suspicious patterns of events can trigger alerts. The knowledge necessary to implement such a national monitoring facility exists, but multiple sites and agencies must coordinate reporting and activities to provide an effective indications and warnings capability.

We propose that a national, distributed KB for homeland defense, implemented as a distributed set of BNFrag/MEBN sites, could provide a powerful, opportunistic detection and alerting capability that leverages the bottom up reporting of nuclear, biological, chemical, financial, cultural and other homeland defense data that is increasingly being locally and nationally collected and disseminated.

Figure 5 shows the concept of such a nationally distributed KB, represented in a set of "Homeland Defense Alerting Centers". Each of these would receive KB updates as BNFrags from "Expertise Centers". Expertise Centers would collaborate on a common domain vocabulary for counter-terrorist related detection and alerting, and each would develop and maintain its specialized vocabulary as well. In the Alerting Centers, BNFrags would be created that encompass a wide range of parameterized coordinated attack scenarios that cross special expertise boundaries. For example, a biowarfare attack might be accompanied by a denial of service attack on the Center for Disease Control (CDC) in an effort to inhibit detection of the biowarfare attack by the CDC.

An important aspect of this conceptual alerting architecture is that no synchronization is needed or desired. All centers operate simultaneously. As long as a shared vocabulary of variables related to coordinated terrorist activity and alerting is adhered to, and as long as each Expertise Center keeps its vocabulary of random variables consistent as it develops its specialized BNFrag models, then the implementation of the architecture in Figure 4 will work.

It is also necessary that the data interfaces for the evidence sources from the surveillance centers be public and be kept current at the alerting centers. This activity has already been in progress for multiple years. The CDC has multiple surveillance systems in place,[5] including the National Electronic Disease Surveillance Systems (NEDSS) and the Enhanced Surveillance Project (ESP). These and many other surveillance organizations and centers are in the process of coordinating to form a unified reporting and vocabulary for electronic interface.[6]

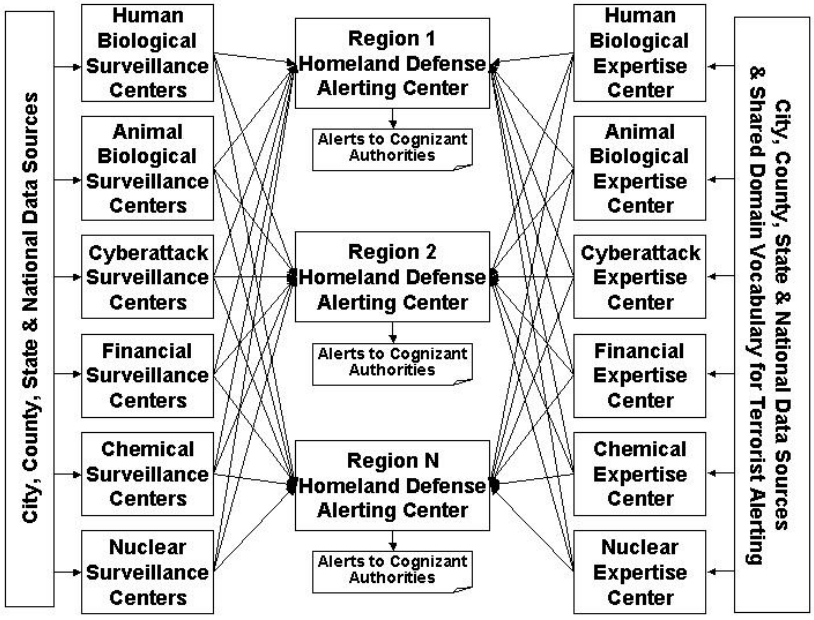


Figure 5 National Counter-Terrorist KB & Supporting Centers Concept

3. COUNTERTERRORIST APPLICATIONS EXAMPLE SCENARIO

3.1 Scenario concept

The following scenario represents a possible coordinated, multi-city, and multiple disease biowarfare terrorist attack on the U.S. Although hypothetical, it is based on the following factual observations.

- A successful foot and mouth disease attack on livestock, e.g. cattle, could cause a trillion dollar financial impact on the economic infrastructure of the United States. Foot and mouth disease spreads rapidly in herds if not quickly checked, and can be spread simply by rubbing the pus from an infected animal onto a healthy one's coat. Only a few grams are required to infect a herd. It is easily transported or obtained in country.[7,8]
- Almost all slaughter of livestock in the U.S. now happens in a relatively small number of places, usually at meatpacking facilities that perform animal-to-product processing. Therefore almost all livestock are eventually concentrated into a set of small regions in stockyards at meatpacking facilities. For cattle, over 95% of all meatpacking industry is concentrated in the "Great Plains" and "Corn Belt" regions of the U.S., and over 50% of all meatpacking is performed at less than 22 facilities in those regions.[9,10] Such facilities are found mainly in large industrial cities including Chicago, Kansas City, Denver, and Dallas/Fort Worth.
- Although foot and mouth is not contagious to humans, cutaneous anthrax, which causes lesions to appear on the skin, can be transmitted to humans. Cutaneous anthrax is not usually fatal to either livestock or humans, but if it was spread at the same time as the foot and mouth, it could delay recognition of the foot and mouth.[11]
- Inhalation anthrax is deadly to both humans and livestock. It is easily spread in aerosol form, although it takes multiple kilograms to afflict a large area. A hand-held aerosol would be adequate to contaminate a herd, but a larger scale dissemination device, such as a small aircraft equipped for crop-dusting, and about 50-100kg of weapons-grade anthrax would be necessary to attack an urban area.[11]
- If large-scale aerosol release of anthrax was performed about the time that alerts of anthrax infection in stockyards near the targeted cities was discovered, it is inevitable that a primary hypothesis be considered that anthrax infection subsequently detected in the human population be linked to the occurrence in livestock,

especially because there is such a short production chain from stockyard to dinner table. This in turn could delay the realization that the human infection is being inflicted by aerosol release from aircraft long enough to enable infection of millions in the target urban areas.

With these facts in mind, the following scenario is used to illustrate the power of BNFrags and MEBNs to opportunistically detect and alert authorities to signs that such a widespread attack was occurring. While unlikely, we do point out that the only theoretically difficult part of this scenario is obtaining multi-kilogram quantities of weapons-grade anthrax in country. However, stockpiles do exist[12] and transporting such quantities into the U.S. is a feasible scenario. In the scenario below, delays between events are based on the latency period of symptoms for diseases such that confusion of actual causes is intended to be maximized.

3.2 Evolution of the scenario

Day 1: Infiltrated stockyard operatives in Chicago infect cattle herds at target stockyards with cutaneous anthrax by sprinkling several grams of it in the cattle feed.

Day 3: Same operatives infect herds with foot-and-mouth disease by direct application of pus onto multiple cattle.

Day 5: First reports of anthrax and foot-and-mouth symptoms in herds occur. Confusion of symptoms delays cause identification. At end of shift, operatives spray multiple grams of inhalation anthrax at herd with hand held spray device. Infiltrated stockyard operatives in Kansas City infect cattle herds at target stockyards with cutaneous anthrax by sprinkling several grams of it in the cattle feed.

Day 7: Crop duster sprays Chicago with 50kg anthrax aerosol. Kansas City stockyard infected with foot-and-mouth.

Day 8: Cutaneous anthrax confirmed in Chicago stockyard.

Day 9: Kansas City Stockyard sprayed with inhalation anthrax. Denver stockyard infected with cutaneous anthrax.

Day 11: Crop duster sprays Kansas City with 50kg anthrax aerosol.

Day 12: Inhalation anthrax detected at Chicago stockyard. Foot-and-mouth confirmed at Chicago stockyard. Cutaneous anthrax detected in Kansas City stockyard.

Day 13: Unlikeliness of multiple outbreaks in disparate areas triggers MEBN in alerting center. National authorities alerted to possible multi-city biowarfare attack. Analysis of anthrax in Kansas City and Chicago shows weapons grade inhalation anthrax used. Alerts are issued to all cities with major cattle stockyards; local law enforcement engaged for extreme surveillance. Crop dusting alert nationwide.

Day 14: Crop dusting alert finds suspicious operatives planning run in Denver. Dallas/Fort-Worth operation subsequently found and shut down.

5. BNFRAGS & MEBNS SCENARIO APPLICATION

Figure 6 through Figure 8 show a set of example BNFrags for an alerting model for bioattacks. These are simplified BNFrags developed for illustrative purposes, and the probabilities are notional values not intended for use in actual applications. Nevertheless, these BNFrags are representative of the kinds of models that might populate the MEBN knowledge base of an Alerting Center. The BNFrag of Figure 6 is a model for reasoning about the types of attacks the Alerting Center might be concerned about. In our example, we consider only coordinated, multi-site and localized biological attacks. The only agents we consider are inhalation anthrax, cutaneous anthrax, and foot-and-mouth disease. This restricted model is sufficient to handle the example of Section 4, and it is clear how to generalize it to additional types of attacks and additional agents. In this model, coordinated attacks have a much higher probability of involving multiple sites and multiple agents, whereas localized attacks tend to occur at a single location and involve only a single agent. This BNFrag is indexed by a single variable *i*, which is a label referring to a particular incident. In a real scenario, the variable *i* would be replaced by an incident identifier, probably constructed from the date of the incident and other identifying information such as the location(s) of occurrence. The target variable in this BNFrag is

`BioAttackType(i)`, which indicates whether incident *i* is a coordinated bioattack, a localized bioattack, or some other type of incident. Note that the *a priori* probability of any kind of bioattack is extremely small.

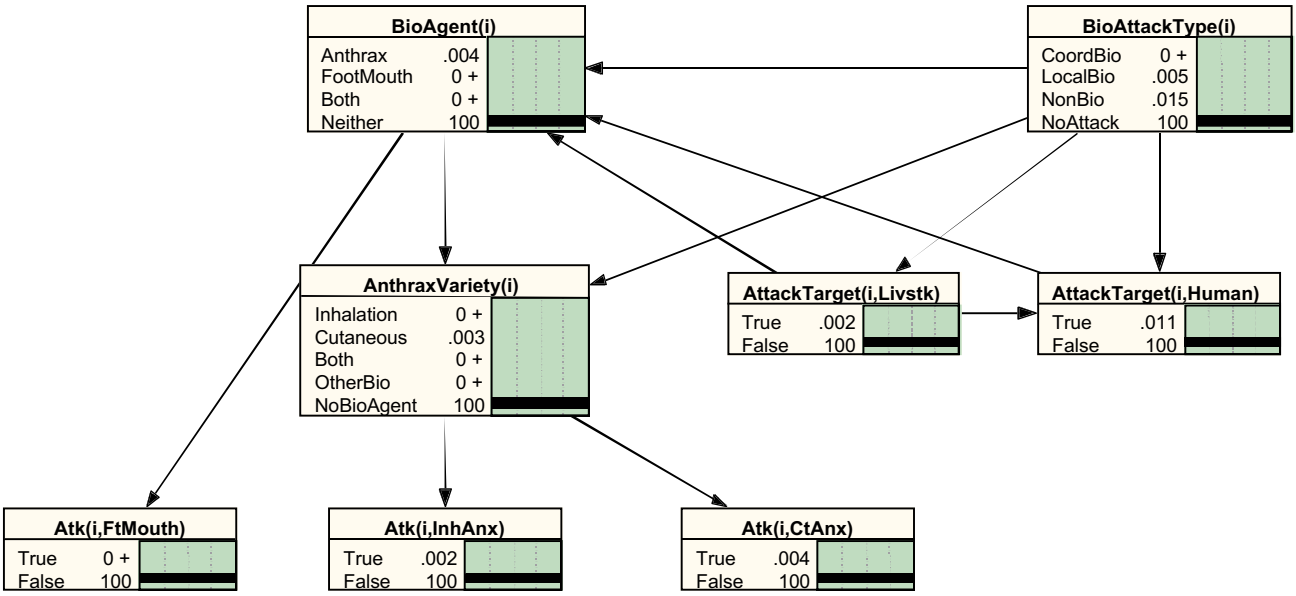


Figure 6: Attack Type BNFrag for Incident *i*

Figure 7 shows a generic BNFrag structure for reasoning about a particular attack involving a given agent *a* (where *a* can stand for inhalation anthrax, cutaneous anthrax, or foot-and-mouth disease), aimed at a particular target *t* (where *t* can stand for livestock or human), in a given city *c* (in our example the cities are Chicago, Kansas City, Dallas/Ft. Worth, and Denver). The shaded hypotheses with italicized names are *input hypotheses* to the BNFrag. Their distributions are specified in the BNFrag of Figure 6, but they are needed in this BNFrag because the conditional distributions of the *resident* variables in the BNFrag depend on the values they take on. The primary target variable in this BNFrag is `Outbr(i,a,t,c)`, which indicates whether incident *i* involves an outbreak of agent *a* occurring in the target *t* population (human or livestock) in city *c*. Another variable that may be a target is `AttackLoc(i,c)`, which indicates whether incident *i* involves city *c*. The evidence variable for this BNFrag is `SpTest(i,a,t,c)`, which takes on the value `Positive` if a test specific to agent *a* gives a positive result when administered to sick individuals of the target *t* population in city *c* and `Negative` otherwise. This generic model would be specialized in a real application to particular tests for the agents in question. Probability distributions in the model may be different for different agents, targets, and cities.

Figure 8 shows BNFrags for non-specific indicators that tend to occur early in an attack. Figure 8*a* shows non-specific evidence indicating an outbreak of some agent of concern in the livestock population in city *c*. Figure 8*b* shows a similar BNFrag for the human population. Note that foot-and-mouth disease does not affect humans, and so it does not occur in the BNFrag of Figure 8*b*.

Figure 9 combines the portions of these BNFrags needed to reason about the evidence in the example scenario. Note that the parts of the model not needed to reason from the evidence to the target variables are not included. To illustrate how this model can be used for reasoning about the attack, we summarize the sequential introduction of evidence as shown below in Figure 10.

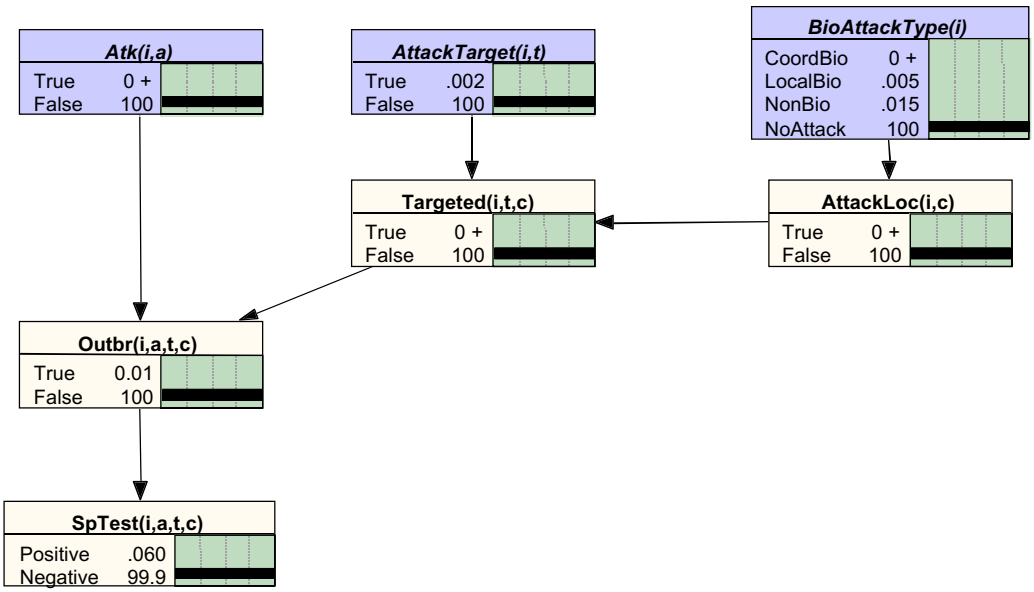
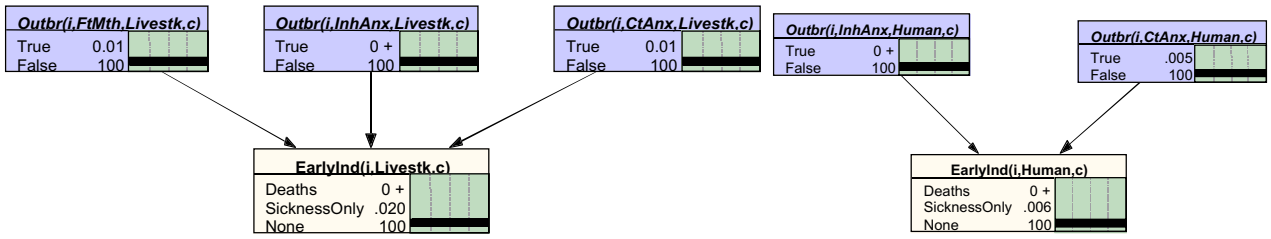


Figure 7: BNFrag for Bioattack Incident *i* with Agent *a*, Target type *t* (human or livestock) in City *c*

In the early part of the attack it is impossible to make a positive determination that a biological attack is underway because the evidence is consistent with many alternative scenarios not involving biological attack. However, belief mounts rapidly for some kind of biological attack as evidence accrues. By the time inhalation anthrax is discovered in Chicago in addition to the cutaneous anthrax, there is a 33% chance that either a localized or a coordinated biological attack is underway. When anthrax is discovered in a second city, the probability jumps to 97% that a coordinated attack is underway. At this point, there is a 58% chance that the attack will involve each of Denver and Dallas / Fort Worth. We have not included the decision portion of the model or confirmation of the attack upon apprehension of the suspects. The model could easily be extended to handle these aspects of the problem, but for purposes of this paper we restricted the model to detection of the attack using evidence about observed symptoms and medical and veterinary tests.



a. Livestock Attack *b. Human Attack*

Figure 8: BNFrag for Early Bioattack Indicators

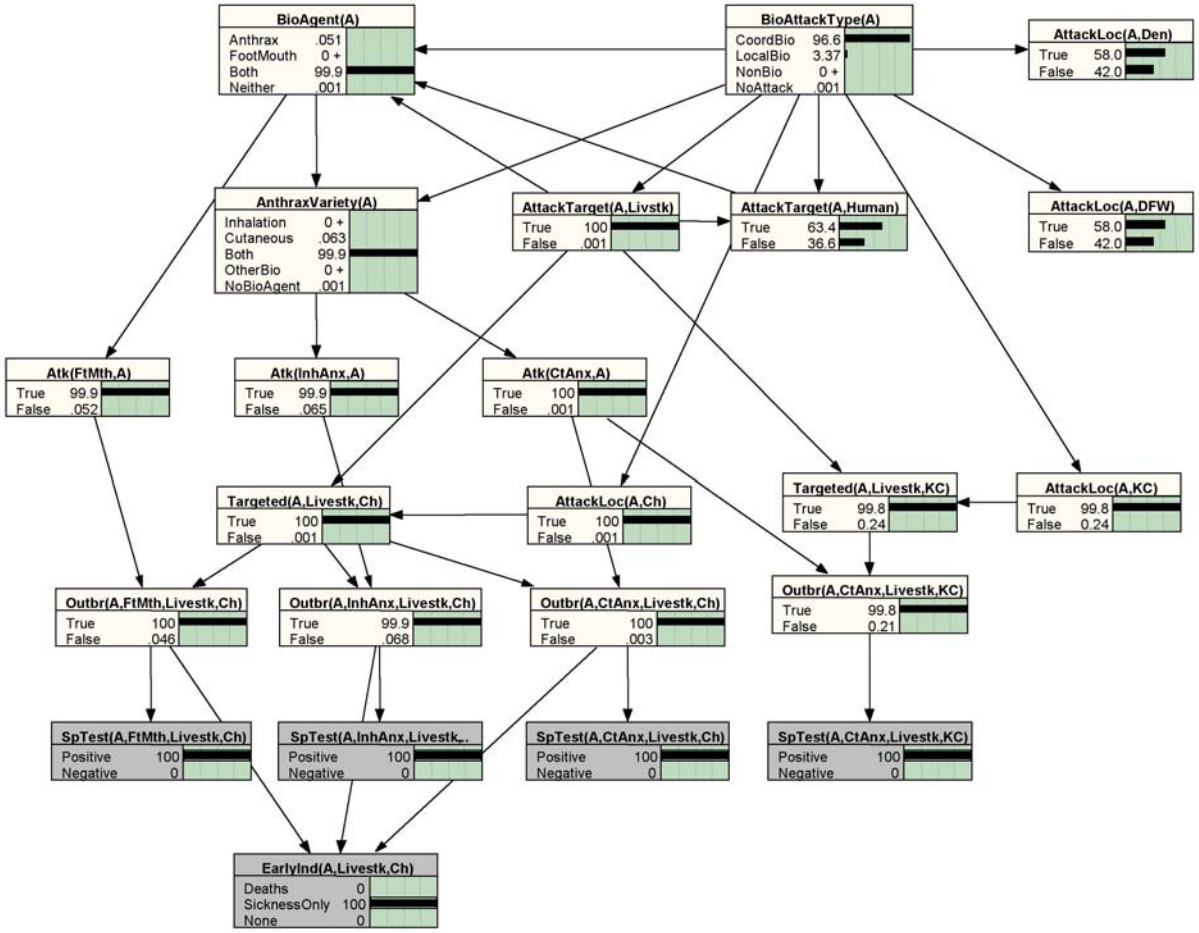


Figure 9: Situation-Specific Network for Example Scenario

	Coordinated Biological Attack	Localized Biological Attack	Neither
Initial probabilities	< 0.01%	0.01%	99.99%
Sick animals observed in Chicago stockyards	0.01%	0.07%	99.9%
Cutaneous anthrax confirmed in Chicago stockyards	0.02%	0.09%	99.9%
Inhalation anthrax confirmed in Chicago stockyards	11%	22%	67%
Foot-and-mouth disease confirmed in Chicago stockyards	34%	66%	< 1%
Cutaneous anthrax discovered in Kansas City stockyards	97%	3%	< 0.001%

Figure 10: Introduction of Evidence into Situation-Specific Network

6. SUMMARY & CONCLUSIONS

We have developed an application of multi-entity Bayesian networks to multi-source fusion for counter-terrorist homeland defense. We have described how this technology could be incorporated into a national distributed knowledge base for homeland defense. Such a knowledge base could provide support for accumulating evidence for indications and warnings for unfolding threat situations. It could also provide automated alerts when threat levels rise above a threshold value, decision support for planning a national-level response to threats, and assistance in coordinating the efforts of multiple distributed response teams.

7. ACKNOWLEDGEMENTS

This paper is dedicated to the memory of journalist Danny Pearl, brutally murdered in Pakistan in February 2002, and to the pioneering research of his father Judea Pearl, inventor of the Bayesian network representation language and computational architecture. Danny Pearl's spirit will live on in the work of those who apply his father's research to protecting the open society for which he gave his life. Thanks are due to Bruce D'Ambrosio, Suzanne Mahoney, Masami Takikawa, Dan Upper, and Ed Wright for helpful discussions on the methods and modeling approaches applied in this paper.

8. REFERENCES

[1] Jensen, F. *Bayesian Networks and Decision Graphs*, New York: Springer-Verlag, 2001.

[2] Pearl, J., *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, San Mateo, CA: Morgan Kaufmann, 1988.

[3] Laskey, K.B., Mahoney, S.M. and Wright, E. "Hypothesis Management in Situation-Specific Network Construction," *Uncertainty in Artificial Intelligence: Proceedings of the Seventeenth Conference*, San Mateo, CA: Morgan Kaufmann, 2001.

[4] D'Ambrosio, B., Takikawa, M. and Upper, D. (2000) "Dynamic Situation Modeling," In *DISCEX 2001: DARPA Information Survivability Conference and Exposition*. Rosslyn, VA: Information Extraction and Transport, Inc.

[5] http://www.bt.cdc.gov/EpiSurv/index.asp

[6] Capital Consulting Corporation, "NEDSS 'A network of networks for a healthier nation' 2nd National Stakeholders' Meeting Report", Center for Disease Control and Prevention, Atlanta Georgia, April, 2001.

[7] USDA Animal and Plant Health Inspection Service Veterinary Service Factsheet, "Emergency Response: Foot-and-Mouth Disease and Other Foreign Animal Diseases", January 2002.

[8] USDA Animal and Plant Health Inspection Service Veterinary Service Factsheet, "Foot-and-Mouth Disease", January 2002.

[9] USDA Economic Research Service, "Beefpacker Concentration", U.S. Beef Industry/TB-1874, 1996.

[10] MacDonald, James, M., Michael E. Ollinger, Kenneth E. Nelson, and Charles R. Handy. "Consolidation in U.S. Meatpacking", *Food and Rural Economics Division, Economic Research Service*, U.S. Department of Agriculture. Agricultural Economic Report No. 785, 1999.

[11] Inglesby, T.V., D.A. Henderson, J.G. Bartlett, M.S. Ascher, E.Eitzen, A.M. Friedlander, J.Hauer, J. McDade, MT. Osterholm, T. O'Toole, G. Parket, T.M. Perl, P.K. Russell, K. Tonat; "Anthrax as a Biological Weapon: Consensus Statement of the AMA Working Group on Civilian Biodefense", *J. American Medical Association*, **281**(18), 1999.

[12] Alibek, Kenneth, *Biohazard: The Chilling True Story of the Largest Covert Biological Weapons Program in the World—Told from Inside by the Man Who Ran It*, Random House, New York, 1999.