An Advanced System for Modeling Asymmetric Threats

Satnam Singh, William Donat, Haiying Tu, Jijun Lu, Dr. Krishna Pattipati and Dr. Peter Willett

Abstract: ***In this paper, we introduce an advanced software tool for modeling asymmetric threats, the Adaptive Safety Analysis and Monitoring (ASAM) system. The ASAM system is a hybrid model-based system for assisting intelligence analysts to identify asymmetric threats, to predict possible evolution of the suspicious activities, and to suggest strategies for countering threats. It employs a novel combination of hidden Markov models (HMMs) and Bayesian networks (BNs) to compute the likelihood that a certain threat exists. It provides a distributed processing structure for gathering, sharing, understanding, and using information to assess and predict adversary network states. We illustrate the capabilities of the ASAM system by way of application to a hypothetical model of development of nuclear weapons program by an unknown hostile country. The simulation results show that the ASAM system is able to detect the modeled pattern with a high performance (greater than 95% clutter suppression capability).***

I. INTRODUCTION

The evidence (or observations or transactions) available from an intelligence database represents any kind of travel, task, trust, or communication among people, places, or items of suspicious origin. As transactions are observed, links representing them are activated in the transaction space. The premise of the ASAM system is that adversaries leave detectable clues about their activities in the information space, which can be related, linked, and tracked over time. A pattern of these transactions and its dynamic evolution over time is a potential realization of a suspicious activity.

The ASAM system is an advanced model-based tool designed to counter asymmetric threats. The expression "asymmetric threats" refers to tactics employed by countries (“rogue and/or failed states”), terrorist groups, or individuals to carry out attacks on a superior opponent while trying to avoid direct confrontation. The goal of the ASAM system is to combine information from different intelligence organizations about the adversary to improve our understanding of their capabilities in order to prevent possible attacks. The ASAM system utilizes attribute-aided tracking and HMMs to identify suspicious activities that are consistent with an *a priori* threat template model. A probabilistic matching of modeled attributes with the observed attributes provides an ability to identify the suspicious persons, places, or other details. Using the ASAM system, potential threat scenarios are postulated and the analysis results are used to prioritize counter-terrorism efforts to reduce the asymmetric threats.

In this paper, we focus on the software modules of the ASAM system. In Section I, we briefly introduce the ASAM process. The software architecture of the ASAM system is discussed in Section II. The ASAM system operation consists of five steps. This concept of operations is discussed in Section III. Section IV shows the application of the ASAM system to a hypothetical model of development of nuclear weapons program (DNWP) by a hostile country. A detailed description of the modeling process using the Testability Engineering and Maintenance System (TEAMS®) software is provided in Section V. Section VI describes the simulation results for the DNWP model via the ASAM website. Finally, we conclude the paper with a summary and key findings in Section VII.

II. ASAM PROCESS

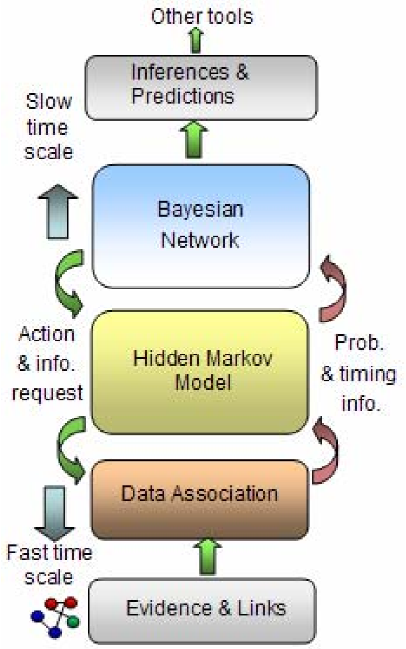


Fig. 1. Hierarchy of the ASAM process

As shown in Fig. 1, the ASAM process is hierarchical, where the lower levels correspond to HMMs, and the higher levels are modeled via BNs (these, in turn, can be hierarchical as well). In other words, the BN represents the overarching threat, and the HMMs, which are associated with BN nodes, represent detailed sub-activities.

The BN represents an intuitive and modular representation of knowledge through causal links among nodes. Thus, it is a directed acyclic graph (DAG) consisting of nodes and links. A BN node represents a random variable, and it has a finite set of states that are mutually exclusive and exhaustive. Each state is associated with a conditional probability of the node,

Satnam Singh, William Donat, Jijun Lu, Dr. Krishna Pattipati and Dr. Peter Willett are with University of Connecticut, Storrs, Connecticut 06226 USA (phone: 001-860-486-2890, fax: 001-860-486-5585, e-mail: krishna@engr.uconn.edu).
Haiying Tu was with the University of Connecticut, Storrs, Connecticut 06226 USA. She is now with Qualtech Systems Inc., Wethersfield, Connecticut 06109 USA (tu@teamqsi.com).

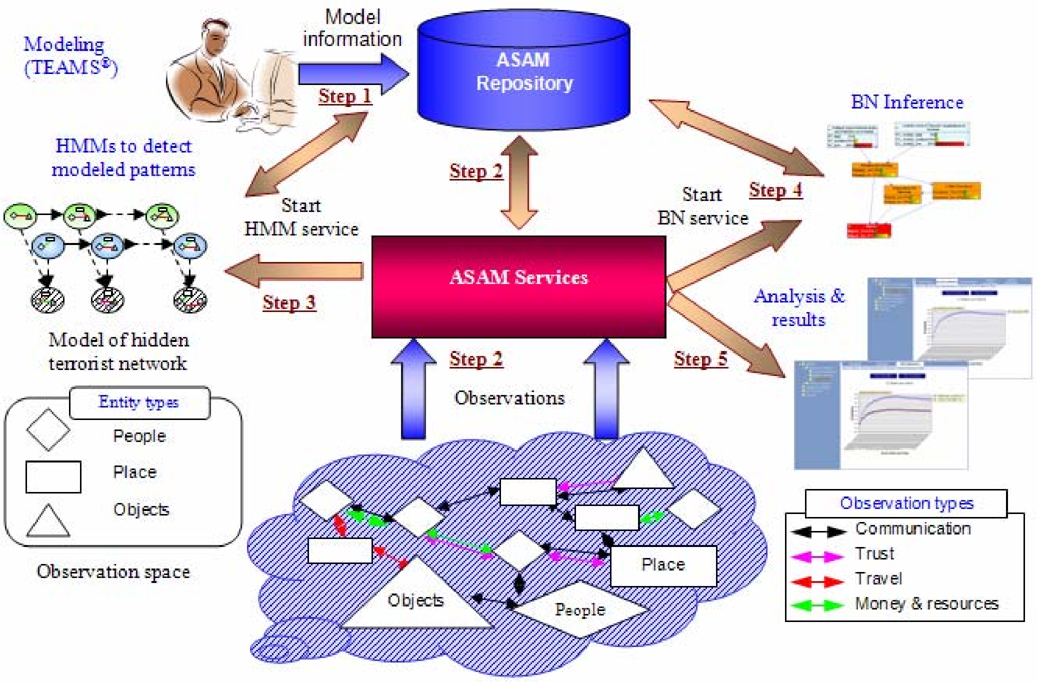


Fig. 2. Concept of operations and software architecture of the ASAM system

given its parent nodes. The causal links between BN nodes represent direct probabilistic dependence, and the absence of a link indicates conditional independence. A node is conditionally independent of all its non-descendants given its parents. Probabilities of nodes in BNs are updated whenever new evidence arrives via BN inference algorithms. Detailed discussions about the BNs are provided in [1].

HMMs are used to model the dynamic evolution of the suspicious activities based on partially observed "signal" (important transactions) embedded in "noise" (benign transactions). They are especially suited for situations that can be modeled as an underlying (hidden) sequence of states, from which only partial observations of the process are available. HMMs belong to a subclass of state space models which are most effective for discrete-valued time series data. Baum and his colleagues developed these theoretical tools in the mid 60s and early 70s. Later, their applicability was popularized by the speech processing community [2]. After this, a growing number of successful applications have been found in almost every field of signal processing. Briefly, a HMM is a stochastic model used to evaluate the probability of a sequence of events, to determine the most likely state transition path, and to estimate those parameters which produce the best representation of the most likely path. An excellent tutorial on HMMs is [2].

In the ASAM system, the HMMs send soft evidence to BN nodes, and the BN inference algorithms integrate the soft evidence from multiple HMMs into an overall assessment of an asymmetric threat. We use Page's test or the Cumulative Sum (CUSUM) method to detect a switch from ordinary noise ("benign") transactions to those modeled by signal ("threat activity") transactions. Detailed discussions about the ASAM technology are available in our earlier publications [3], [4] and [5].

III. SOFTWARE ARCHITECTURE

The ASAM system employs a service-oriented architecture. The web-services based architecture provides a decentralized, loosely coupled, and highly interoperable collaboration among the various software modules of the ASAM system. Following are various software modules in the ASAM system that is also shown in Fig. 2:

- HMM web service is a hidden Markov model inference engine, which is developed using the C# software language.
- BN web service is a Bayesian network inference engine, which is developed using the Visual C++ software language.
- The ASAM client interface is a website developed using ASP.NET and C# software language.
- The ASAM repository is a MySQL® database, which stores transactions, models, and results.
- Off-line modeling is implemented using an extended version of TEAMS® [6].

IV. CONCEPT OF OPERATIONS

The ASAM system operates in five steps, which are illustrated in Fig. 2. The first step involves constructing models (hypotheses) of threats using TEAMS® software. In order to detect suspicious activities, the ASAM system must be given *a priori* information about potential adversary activities ("template models"), which are to be monitored. This information is provided in the form of HMM and BN models, which describe specific threats. Real-world events, such as terrorist attacks, are characterized as partially observable and uncertain signals. Their signals, or electronic signature, are a series of transactions. We represent each transaction as a line connected with two shapes. The shapes (diamond, rectangle, and triangle) represent the entities such as people, places, and objects. The transactions are of various types, such as communications, trust, travel or money & resources and they are shown by different colors of the line. While referring to the transactions, we define some terms: *true transactions*, *noise*, *gated false alarms* and *clutter*. The *true transactions* represent a pattern of a threat, which is defined by an analyst in the template model. The *noise* is defined as transactions, whose details (transaction type, etc) do not match the template model. The *gated false alarms* are the transactions, which have transaction details (transaction type, entity types and attributes) similar to true transactions and the number of gated false alarms is below a threshold i.e. probability of gated false alarms. The *clutter (or true false transactions)* consists of *noise* and *gated false alarms*. The objective of the ASAM system is to detect a pattern of *true transactions* (a colored graph) embedded in the large amount of *clutter*.

The second step is the retrieval of model and transactions from the repository. In an operational scenario, the ASAM system will use an intelligence database created and maintained by intelligence analysts.

The third step is the detection of a suspicious activity by HMMs by matching a pattern between the template model and the observations. The HMM web service determines whether the monitored activity exists. If the activity is consistent with any of the HMM template model, then it is detected and the related soft evidence is reported back to the ASAM repository for further analysis by the BN web service.

The fourth step is the BN web service, that is analogous to a higher-level decision maker. It provides a global measure of the threat.

The final step in the ASAM process is to report both the real-time and what-if scenario analysis from the HMM and BN web services.

V. Example: Development of a Nuclear Weapons Program (DNWP)

There are many reasons a country may seek to develop nuclear weapons, but whatever the reasons, the development of the nuclear capability by a country has vast implications for the US and its allies. The intelligence community's ability to detect, analyze, and monitor the development of these programs is essential. The purpose of this model is to describe the evolution of a nuclear weapons program by a hostile country. The model developed herein describes the progress of a nuclear weapons program as a pattern of events grouped into three HMMs*: research and design HMM; production of weapons grade material HMM; and fabrication, test, and integration (FTI) HMM*. This model does not attempt to enumerate every possible step or observation, but rather to capture key observable events in the process of developing nuclear weapons. The model is gleaned using the open sources [7], [8], [9], [10], and [11].

The *research and design HMM* involves research and design of the processes and equipment used to enrich nuclear material, planning for integration of the weapons into the military portfolio, as well as the design of weapons themselves. The activities of key scientists within a country would reveal that it is developing nuclear weapons. We consider information requests and studies related to nuclear engineering as key indicators. Also, computer simulations are a substantial part of the initial design process of both enrichment and weapons technologies. In addition, a country must gain proficiency with development and detonation of chemically pure high explosives. The research, experimentation, and testing of these high explosives are observable. Experimentation requires the acquisition of many pieces of specialized test equipment, which, we assume might be detected. Finally, the unsafeguarded experimentation with refinement of nuclear material would be a strong indicator that a country was developing a nuclear weapons program.

In the *production of weapons grade material HMM*, we assume that in order to remain clandestine and have enough material to create even a meager arsenal, the country chooses to mine, mill, and refine its own uranium. However, the ultimate refinement to weapons grade is allowed to follow the uranium or plutonium enrichment technologies. The enrichment of uranium is assumed to be by means of gas diffusion or centrifuge. A gas diffusion facility would likely be collocated with a large power plant. Meanwhile, a centrifuge enrichment facility would be very large and its construction as well as heat signature would likely be observable. The enrichment of plutonium from uranium would require a nuclear reactor and a processing plant. The reactor would have no output power when it was being used to create plutonium and this would likely be observable. Throughout the progress of this group of events, we assume that the acquisition of specialized equipment and resources are observable. Finally, if a country has its own nuclear energy program, its conduct (e.g., lack of cooperation) with International Atomic Energy Agency (IAEA) regulations and inspections is also considered as indicators of an active nuclear weapons program.

Once the nuclear material has been refined to weapons grade, the nuclear material must be assembled together with the non-nuclear components into the final nuclear weapon. The weapons grade material must be formed into a shape according to the particular design. This requires lathes, furnaces, an inert gas environment, and other special equipment. A mature nuclear weapons program will have tested and will be developing significant quantities of high explosives. It is also assumed that country X will be experimenting with boost technology to increase their weapon's yield. Deployment of a nuclear weapon once it has been developed requires a delivery system. Therefore, we assume signs of the development of certain delivery systems are indicators of a nuclear weapons program. At some point before the weapon is actually assembled, a political decision must be made to do so. This event is likely to coincide with the implementation of policy, strategic, and military integration of the nuclear weapon program. The test of a nuclear weapon is the final state of *fabrication, test, and integration HMM*. Due to space limitations, only the Markov chain depicting the *FTI HMM* is shown here (Fig. 3).

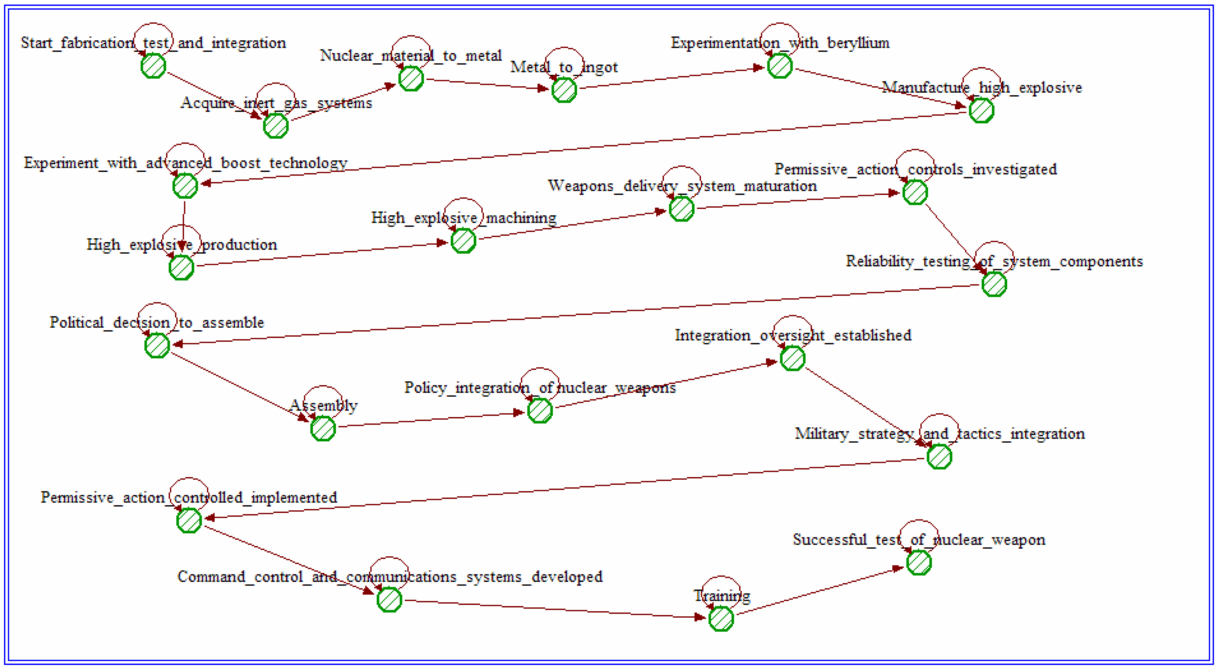

Start_fabrication_test_and_integration
Acquire_inert_gas_systems
Nuclear_material_to_metal
Metal_to_ingot
Experimentation_with_beryllium
Manufacture_high_explosive
Experiment_with_advanced_boost_technology
High_explosive_production
High_explosive_machining
Weapons_delivery_system_maturation
Permissive_action_controls_investigated
Reliability_testing_of_system_components
Political_decision_to_assemble
Assembly
Policy_integration_of_nuclear_weapons
Integration_oversight_established
Military_strategy_and_tactics_integration
Permissive_action_controlled_implemented
Command_control_and_communications_systems_developed
Training
Successful_test_of_nuclear_weapon

Fig. 3. Markov chain of *fabrication, test and integration* HMM

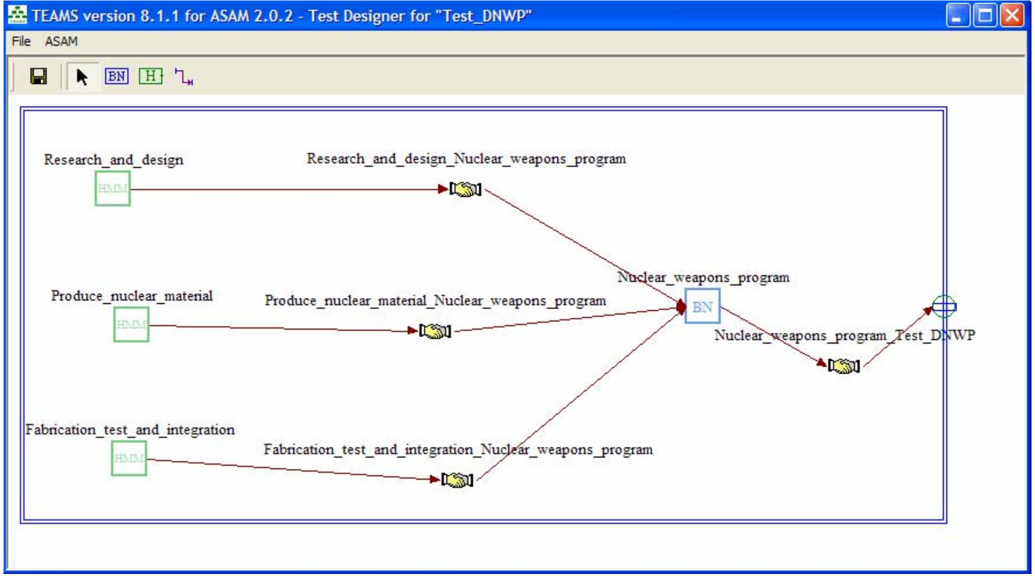
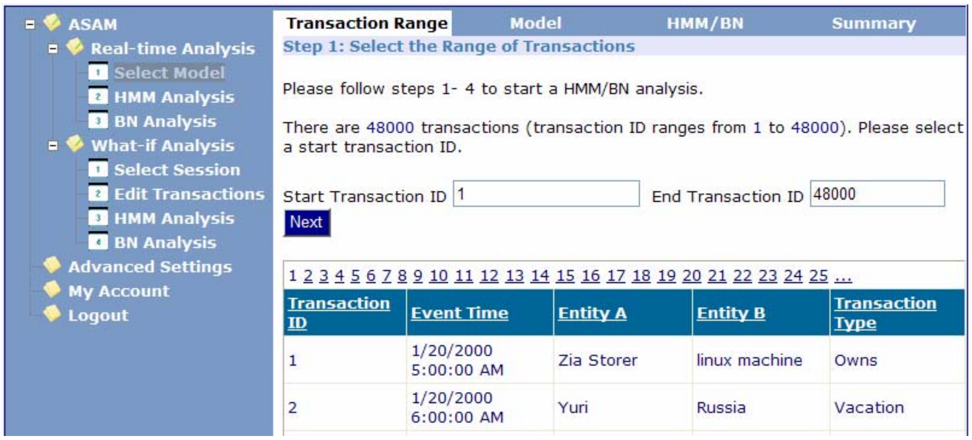

TEAMS version 8.1.1 for ASAM 2.0.2 - Test Designer for "Test_DNWP"
File
ASAM
BN
H
Research_and_design
HMM
Research_and_design_Nuclear_weapons_program
Produce_nuclear_material
HMM
Produce_nuclear_material_Nuclear_weapons_program
Fabrication_test_and_integration
HMM
Fabrication_test_and_integration_Nuclear_weapons_program
Nuclear_weapons_program
BN
Nuclear_weapons_program_Test_DNWP

Fig. 4. Bayesian network of the DNWP model

VI. MODELING VIA TEAMS®

The modeling interface of the ASAM system is currently developed based on TEAMS® version 8.1.1 [6]. The TEAMS® software provides a platform to build the network structures for both BN and HMMs. The BN model is on the top level of the hierarchy and multiple HMMs are on the second level. Each HMM is associated with a BN node (which has binary states, the HMM results are reported to one of the states and the other state is essentially the null hypothesis, e.g., the modeled threat activity doesn't exist or isn't activated). The ASAM system has the capability for fusing information via messages passed from a lower level HMMs to the higher level BN (fusion center). This functionality is achieved by specification of the relationships between BN and HMMs. Fig. 4 shows three HMMs connected with a BN model. The connection is displayed as a "Hand-shaking" icon. The left side icons represent the input from the HMMs and the right side icons represent the output of the BN and the input to the monitoring point. By default, all the BN nodes are binary with states "Yes" and "No," with specified initial probabilities (at the leaves). Fig. 3 shows the *FTI HMM*. The states and the transitions between states (shown as the links between states) can be added in the HMM designer. Analyst must specify the transition probabilities, prior probabilities, and the nodes associated with the HMM. The nodes are the transaction sources or destinations. They can be persons, places, or things. Different attributes are available for each type of node. For example, a person type node may have attributes such as citizenship, age, education level etc. Each attribute must be given a confidence, which represents the confidence



Step 1: Select the Range of Transactions

Please follow steps 1- 4 to start a HMM/BN analysis.

There are 48000 transactions (transaction ID ranges from 1 to 48000). Please select a start transaction ID.

Start Transaction ID: 1 End Transaction ID: 48000

Transaction ID	Event Time	Entity A	Entity B	Transaction Type
1	1/20/2000 5:00:00 AM	Zia Storer	linux machine	Owns
2	1/20/2000 6:00:00 AM	Yuri	Russia	Vacation

Fig. 5. The ASAM website

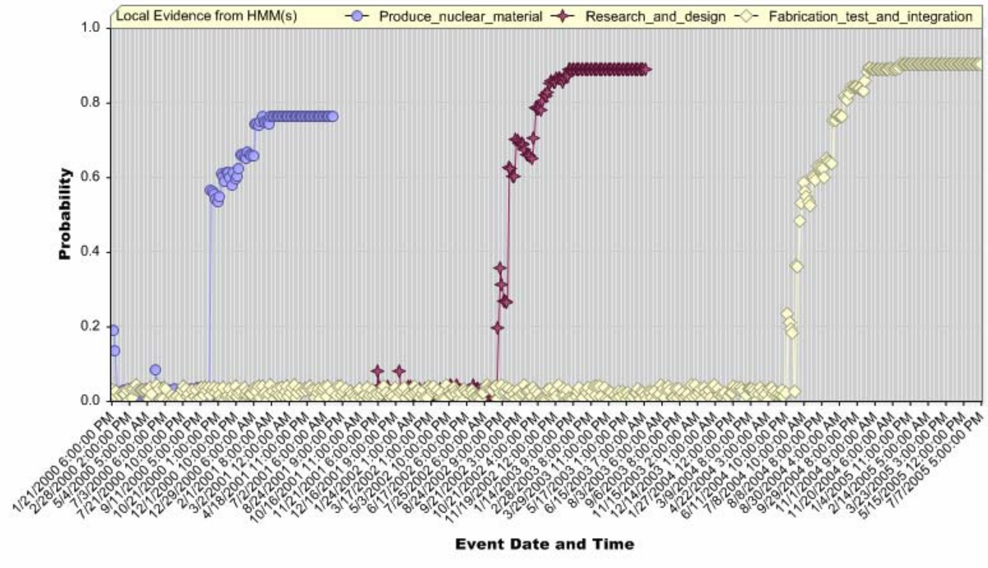


Fig. 6. Local evidence plot of 3 HMMs of the DNWP model

that the node of the observation will contain this attribute. The confidence is a number between 0 and 1, which represents the weight by which the attribute is available in the observation. After inputting all the nodes, the analyst can add transactions associated with each state of the HMM model. Finally, all the model information is exported to the repository for further analysis.

VII. RESULTS VIA THE ASAM WEBSITE

The ASAM website provides the capability to view and analyze the results [12]. It is designed to execute the HMM and BN web services, and visualize the results generated by the HMM and BN engines. Fig. 5 shows a screen shot of the website. The website has a navigation menu on the left side, which provides the flexibility to operate both real-time and what-if-scenario analysis from the HMM and BN web services. The website also provides the capability to change simulation parameters, ability to create random datasets for simulations, and data management using advanced settings. As the real intelligence data is not publicly available, we used synthetically generated data to simulate a development of nuclear weapons program activity. The simulated data is a combination of the underlying hidden states of three HMMs of the DNWP model embedded in background noise from a benign source. Probability of detection of 80%, and probability of gated false alarm of 5% was used for generating the observations. The dataset contained 48000 observations, which consist of 58 true transactions and 47942 clutter transactions. Following are typical results obtained using the simulations:

1. Likelihood of observations: The likelihood of the observations is a quantitative measure of the confidence of the match between the observed events and the template models. The HMM determines whether the monitored activity exists. If the activity is consistent with the models derived in the first step, then it is detected and the related soft evidence is reported back to the BNs for further analysis. Fig. 6 shows the HMM local evidence associated with *Fabrication* phase of the DNWP model. Probability of detection of 90%, Page's test threshold value of 4.0 and probability of gated false alarm of 1% was used for computing the inference. The starting point of each HMM detection curve is associated with the first time this HMM is detected; thus, we believe with certain probability that the modeled suspicious activity is in progress. A peak probability usually results when this pattern evolves into the

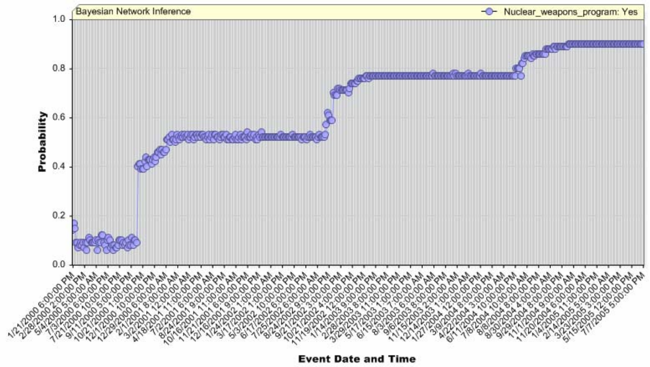


Fig. 7. BN inference associated with *Nuclear weapons program* BN node

TABLE 1

Clutter suppression capability of the ASAM system

S. No.	Probability of detection for algorithm (%)	Probability of gated false alarm for algorithm (%)	Clutter suppression capability (%)
1	90	1	98.2
2	90	5	97.8
3	80	3	97.9
4	70	1	98.2
5	70	5	97.6

absorbing state of the HMM, and we obtain maximum number of signal transactions for this HMM.

2. Evidence from the observations: The evidence is a description of actors, transaction type, transaction description, transaction time, etc.

3. Probability of an asymmetric threat: The BN software uses the soft evidence from the HMMs to produce a belief about the global threat level. Note that the HMM software detects the local activity and measures local threat levels, whereas the BN inference is a culmination of all reported activities. Fig. 7 shows the BN inference plot associated with the *Nuclear weapons program*, the central BN node.

We performed several simulations to measure the performance of the ASAM system under different noise levels. The performance is measured using clutter suppression capability (CSC), which is defined below:

$$\text{Clutter suppression capability (\%)} = \frac{\text{No. of true false transactions- No. of detected \& true false transactions}}{\text{No. of true false transactions}} \times 100$$

As shown in Table 1, the ASAM system achieves high performance (high CSC) under high *clutter*.

Next, we perform what-if analysis on the *FTI* HMM. In this experiment, we assume that the intelligence data contains transactions corresponding to only first 10 states of the HMM and the rest of the pattern is missing. We simulate this scenario using what-if analysis mode of the website. Fig. 8 shows the local evidence plot for this scenario. The local evidence plot is changed from the plot under real time mode (a yellow lined curve in Fig. 6) in which the dataset had the entire pattern. However, the HMM still detects the pattern associated with fabrication activity. The fall in the local evidence plot occurs due to an increase in the number of gated false alarms. This scenario demonstrates that the ASAM system is robust, and that it can detect the pattern even if the only half of the pattern was embedded in the noisy intelligence data.

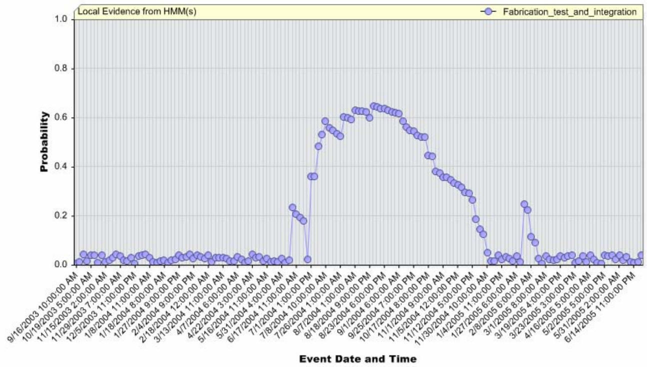


Fig. 8. Local evidence plot of *FTI* HMM for what-if scenario

VIII. CONCLUSIONS

In this paper, we introduced the ASAM system, an advanced information technology tool, for analyzing asymmetric threats. The ASAM system can detect, track, and predict the potential threat activities in real time. It can also work as a what-if analysis tool by allowing users to modify models (i.e., states in the HMMs, conditional probabilities in BNs) and/or transaction sequences. We utilized the ASAM system to detect and track a pattern consistent with the development of a nuclear weapons program. The concept of operations of the ASAM system along with its software architecture was discussed. The results associated with the DNWP model were presented using the ASAM website [12]. The simulation results demonstrate that the ASAM system is an advanced system to track asymmetric threats and that it has high clutter suppression capability.

REFERENCES

[1] R. E. Neapolitan, “Learning Bayesian Networks,” *Prentice Hall*, April 2003.

[2] L. Rabiner, “A tutorial on hidden Markov models and selected applications in speech recognition,” *Proc. IEEE*, vol 77, no. 2, pp 257-286, 1989.

[3] H. Tu, J. Allanach, S. Singh, P. Willett and K. Pattipati, “Information Integration via Hierarchical and Hybrid Bayesian Networks,” *IEEE Transactions on System, Man and Cybernetics, Part A: Systems and Humans, special issue on “Advances in Heterogeneous and Complex System Integration,”* January 2006.

[4] S. Singh, J. Allanach, H. Tu, K. Pattipati and P. Willett, “Stochastic Modeling of a Terrorist Event via the ASAM system,” *IEEE Conference on Systems, Man and Cybernetics,* Hague, Netherlands, October 2004.

[5] S. Singh, H. Tu, J. Allanach, K. Pattipati and P. Willett, “Modeling Threats,” *IEEE Potentials*, August-September 2004.

[6] QSI website, http://www.teamqsi.com.

[7] F. Barnaby, “How to Build a Nuclear Bomb and Other Weapons of Mass Destruction,” New York, *Nation Books*, 2004.

[8] R. Paternoster, “Nuclear Weapon Proliferation Indicators and Observables,” *Los Alamos National Laboratory*, December 1992.

[9] F. Settle, *“*Nuclear chemistry, nuclear proliferation,*”* http://www.chemcases.com/2003version/nuclear/nc-12.htm.

[10] L. Spector and J. Smith, “Nuclear Ambitions: The Spread of Nuclear Weapons 1989-1990,” Boulder, CO, *Westview Press*, 1990.

[11] U.S. Congress, Office of Technology Assessment, *“*Technologies Underlying Weapons of Mass Destruction*,”* OTA-BP-ISC-115, Washington, DC, *U.S. Printing Office*, December 1993.

[12] The ASAM website, System Optimization Lab, University of Connecticut, http://servery.engr.uconn.edu/asam_web/login.aspx.