IDEA GROUP PUBLISHING

701 E. Chocolate Avenue, Suite 200, Hershey PA 17033, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com

ITP4754

Agent Based Intrusion Detection with Soft Evidence

V. Gowadia, C. Farkas, and M. Valtorta
Information Security Laboratory
Department of Computer Science and Engineering
University of South Carolina
Columbia, SC 29208
{gowadia, farkas, mgv}@cse.sc.edu

ABSTRACT

In this paper we propose a new framework for intrusion detection, called Probabilistic Agent-Based Intrusion Detection (PAID), using agent encapsulated Bayesian networks. *It allows agents to* share *their* beliefs, *i.e., the calculated probability distribution of event occurrence. A unique feature of our model is that the agents use the* soft evidential update *method to process beliefs. This provides a continuous scale for intrusion detection, supports merging of signature based and anomaly based systems, and reduces the communication overhead in a distributed intrusion detection scenario. We have developed a FIPA compliant agent communication architecture that provides a prototype implementation.*

1. INTRODUCTION

Even in the presence of sophisticated security safeguards, it is unrealistic to assume that a computer system is fully protected. As malicious attacks become more and more sophisticated, the need to provide effective, high-assurance intrusion detection methods increases [CERT, AFV95, LS98, Axel00]. Network-based, distributed attacks are especially difficult to detect and require coordination among different intrusion detection components or systems [SB91, Cann98, MST98, NP99]. The development of models and protocols for information sharing becomes critical for intrusion detection systems (IDS). Recent research [BFIS98, JMKM99, CHSP00, HWHM00] shows that agent-based technology seems to be a promising direction for developing collaborative intrusion detection systems.

Agent-based and cooperative architectures require that each IDS component is able to process information and requests that they receive from other components. Bayesian inference based models support this requirement and have been considered for intrusion detection [BV99, DM99, VS00, BWJ01]. However, they use traditional probability update methods for Bayesian networks [Jens01, Pearl88] that are limited because they cannot handle soft evidence. Furthermore, it is necessary that IDS components may share decision, data or partial data in a flexible way and provide quantitative representation of the confidence in the decisions.

In this paper we address the shortcomings of current models by proposing a new intrusion detection framework and develop underlying technologies. More specifically, we propose an agent-based, cooperative architecture, called *Probabilistic Agent-Based Intrusion Detection (PAID)*, to analyze system information and estimate intrusion probabilities. PAID uses a multiagent system, called Agent Encapsulated Bayesian Network (AEBN) [BMV02], in which autonomous agents share their beliefs. From the security perspective, we classify agents into two types: *system-monitoring agents* and *intrusion-monitoring agents*. System-monitoring agents are responsible for collecting, transforming, and distributing intrusion specific data upon request and evoke information collecting procedures. Each intrusion-monitoring agent encapsulates a Bayesian network and performs belief update as described in [VKV02] using both facts (observed values) and beliefs (generated values). Intrusion-monitoring agents generate probability distributions (beliefs), over intrusion variables that may be shared with other agents. Each belief is called a *soft finding*. Soft findings can indicate abnormal states of a system, which affect the probability of an intrusion, even in the absence of certain hard findings. A probabilistic representation of hard and soft findings makes our model capable of identifying variations of known intrusions.

The organization of the paper is as follows. Section 2 gives a brief introduction to background information on Bayesian network and agent technology. Section 3 contains the design considerations of our model. Section 4 describes the proposed framework (PAID) and its implementation. Section 5 contains a detailed description of Bayesian network models. Finally, we conclude and recommend future research in Section 6.

2. BACKGROUND

2.1 Bayesian Networks

Bayesian networks are probabilistic models that exploit the conditional independence properties present in a task domain to reduce both the space required to store the model and the time needed to compute posterior probabilities upon receipt of evidence. A Bayesian network is composed of a probability distribution over *n* random variables in the set $V = \{V_1, \ldots, V_n\}$, and a directed acyclic graph (DAG) whose nodes are in one-to-one correspondence with $V_1,\ldots,V_n$. The defining property of a Bayesian network is that the conditional probability of any node given any subset of non-descendants is equal to the conditional probability of that same node given the parents alone.

We define *evidence* as defined as a collection of findings, a (*hard) finding* on variable *v* as a specification of the value of *v*, and a *soft finding* on variable *v* as a distribution on the values of *v*. These definitions of finding and of evidence may be generalized [CDLS99; VKV02], for example, by allowing specifications of impossible configurations of pairs of variables. The most common operation on a Bayesian network is the computation of marginal probabilities both unconditional and conditioned upon evidence. Marginal probabilities are also referred as *beliefs* in the literature [Pearl88]. This operation is called probability updating, belief updating, or belief assignment.

2.2 Agent Encapsulated Bayesian Networks

In Agent-Encapsulated Bayesian Network (AEBN) [BMV02] each agent uses a single Bayesian network (which is also called an AEBN) as its model of the world. The agents communicate via passing messages that are distributions on variables shared between the individual networks.

The mechanism for integrating the view of the other agents on a shared variable is to replace the agent's current belief (probability distribution) in that variable with that of the communicating agent. The

update of a probability distribution represented by a Bayesian network upon receipt of a belief is called *soft evidential update* [VKV02]. We use the big clique algorithm for soft evidential update, implemented in the BC-Hugin system [KVV02].

The graph of agent communication (*agent graph)* is a directed acyclic graph. It is assumed that equilibrium is reached and a global consistency is achieved if the belief in each shared variable is the same in every agent. When an agent makes a new observation it publishes its new belief. In turn, the subscribers may adjust their internal view of the world and send their published values to their subscribers. However, it is permissible to have multiple views of a common variable.

2.3 Agent Based Intrusion Detection Systems

Agent-based systems require a communication infrastructure. Agent communications can be divided into two categories, communication among agents at same host and communication among agents on different hosts. Balsubramaniyam et al. [BFIS98] examine these methods in the context of intrusion detection. Agent communication in our implementation follows the Foundation for Intelligent Physical Agent (FIPA) specifications [FIPAOS, BPR98].

Agent-based intrusion detection has been considered previously. In [BFIS98] Balasubramaniyan et al. present a framework, where autonomous agents report their findings to per host entities called transceivers. They also perform data reduction and send data to monitors that oversee operation of several transceivers. Monitors have the capability to detect events that may be unnoticed by the transceivers. In mobile agent based systems, like the ones presented in [HWHM00] and [ATG99], mobile agents collect, integrate, and analyze data from different components of a distributed system. Findings of the agents are recorded in a database and/or reported to the users.

3. SYSTEM DESIGN GOALS

Our model can be used either as a stand-alone system or to support an existing IDS. The following objectives guided our system design:

1. *Continuous intrusion classification*
2. *Scalability:* The architecture of distributed IDS must allow local analysis and sharing of results, minimizing the communication costs.
3. *Flexibility*: A site security officer (SSO) must be able to customize IDS sensitivity and selectivity according to the requirements of the site.
4. *Automated analysis and intrusion response*.
5. *Maintainability*: It should be easy to modify intrusion monitoring agents and network configurations.
6. *Reliability*: IDS should perform at an acceptable level even in the presence of intrusions.

4. PROBABILISTIC AGENT-BASED INTRUSION DETECTION

In our model, we use agent graphs to represent intrusion scenario. The agent at each node of the graph encapsulates a Bayesian network. Each Bayesian network contains a particular intrusion scenario, error modeling and a method to incorporate multiple beliefs on input variables. Nodes of the Bayesian network represent beliefs on suspicious events, intrusions, or system and network parameter values. Each agent is associated with a set of input variables, a set of output variables or beliefs, and a set of local variables. A belief (node variable) can have any number of states. This calculation incorporates the uncertainties and measurement errors.

A description of this method with example of Mitnick attack [Nort99] scenario, including a discussion of how to build the Bayesian networks, is given in [GFV01].

The following types of agents are supported in PAID architecture:

1. *System-monitoring agents*: The system-monitoring agents perform either online or offline processing of log data and communicate with the operating system and monitor system resources. These agents publish their output variables, which can be utilized by other agents.
2. *Intrusion-monitoring agents*: Each intrusion-monitoring agent computes the probability for a specific intrusion type. These agents subscribe to variables and/or beliefs published by the system-monitoring agents and other intrusion-monitoring agents. Information about the required input variables for an agent is obtained from the corresponding Bayesian network. The probability values are computed again on modification in the values of input variables or beliefs.
3. *Registry agent*: For each registered agent, our registry agent maintains information about the published variables and monitored intrusions. The registry agent also maintains the location and current status of all the registered agents. Registry agents are used to find information (e.g., name and location) about agents who may supply required data.

4.1 Agent Communication

Agents in our system communicate with each other by sending messages in Agent Communication Language [FACL02] specified by FIPA. Figure 1 shows the interactions within PAID.

The content of the messages is in eXtensible Markup Language [XML]. The important messages exchanged among the agents are:

1. Registration of agent with registry agent
2. Request to registry agent for finding other agents
3. Search results
4. Belief subscription requests
5. Belief update messages.

4.2 Communication Security

Our system provides reliable and secure communication by incorporating the following features:

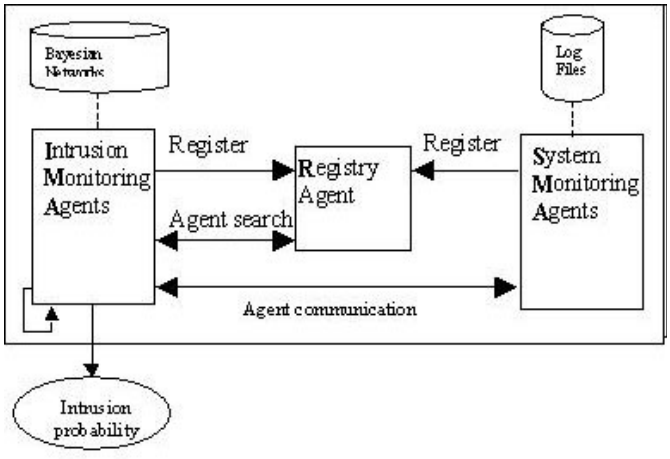
1. *Status maintenance of registered agents and network links*: Registry agent monitor the status of the registered agents. This monitoring is performed by periodically probing system-monitoring agents. Responses to the probing messages carry information about the state of the system-monitoring agents. The status of a communication link between any two agents is determined by attempting to achieve a reliable UDP communication between them.
2. *Authentication*: Our model uses public key cryptography to provide authentication of messages and agents. Each message is signed by the sending agent. In addition, we require that agents authenticate themselves to the registry by their digital certificates.
3. *Encryption and Decryption*: Encrypted messages are sent among agents using secret key encryption method.

4.3 Performance Analysis

The factors affecting scalability are:

1. *Data transfer*: Agent needs to share mainly their beliefs, thus PAID has low bandwidth requirements. Actual data sharing is required only to analyze suspicious events.

Figure 1. Probabilistic Agent-based Intrusion Detection (PAID)



2. *Performance of the belief update:* Pearl [Pearl88] has shown that belief update can be performed in linear time in trees and (more generally) singly connected networks. Unfortunately, belief update in general Bayesian networks is NP-hard [Cooper90]. This negative result holds even for some notions of approximation and for many restrictions on the structure of the Bayesian network. Despite these negative theoretical results, update in most Bayesian network using the junction tree algorithm [LS88] is very fast, because most practical Bayesian networks compile into a junction tree where the largest clique is small [Neap90].
3. *Agent registry*: PAID can provide scalability by supporting multiple registries. Each subnet may have its own agent-registry. The agent-registries can forward requests and replies to neighboring registries based on the IP address of the receiving agent. Therefore, dynamic routing algorithms for IP networks [OSPF97, Perl92] are also applicable for this purpose.

5. INTRUSION DETECTION WITH AGENT ENCAPSULATED BAYESIAN NETWORKS

The calculation of a belief depends on factors such as accuracy of measurement and conflicts among beliefs reported by various agents. In this section, we briefly describe how Bayesian networks model errors and resolve conflicts.

5.1 Modeling errors in measurement

In our model, if an agent is not able to accurately determine the state of a published variable, the agent publishes a probability distribution (belief) over the possible states of the variable. The publishing agent determines this distribution by incorporating the measurement errors. Errors in the measurement of a variable state are modeled within an agent with help of Bayesian network shown in Figure 2. This is achieved by representing the state of variable with a belief or soft finding. The parent node S represents the actual value of interest. The prior distribution of the actual values is P(S). The measured value is represented by variable S_{obs}. The measurement error is modeled by the conditional probability $P(S_{obs}|S)$. In the absence of error, this is a diagonal matrix. The magnitude of non-diagonal entries is directly proportional to the measurement errors. In the special case of a 2x2 matrix, the two diagonal entries quantify the specificity and sensitivity of the measurement, and the other entries quantify the false positive and false negative ratios. When the actual value is propagated to parent node S, we get a probability distribution over different states of the variable. The agent can publish this distribution as its belief on the state of the measured variable.

5.2 Conflict resolution

Conflicts among beliefs on a state of variable due to information provided by multiple agents on the same underlying quantity can be resolved using soft evidential update. For example, let A_1 and A_2 be two agents that measure a variable *v*. The values measured by them are B_1 and B_2 respectively. The belief computed after incorporating the views of both agents is B. We design a Bayesian network as shown in Figure 3. The computed posterior probability of v effectively fuses the information provided by the two agents in the context specified by variable CR.

This approach requires estimating the prior probabilities of B and CR. In most practical uses of the Bayesian network, the value of CR is known, so the assessment of the prior probability of CR does not need to be accurate. The prior probability of B needs to be more accurate, and it is normally possible to estimate B by using counts of the values of B in past cases. A similar technique (based on counts) can be used for the conditional probability tables $P(B_1|v,CR)$ and $P(B_2|v,CR)$. See [Jens01, CDLS99] for a discussion of the technique in general and [VS00] for an application of the technique in an intrusion detection scenario.

In special cases B_1 and B_2 are statements that *v* is in a particular value. In general, they are probability distributions representing each agent's belief that the variable *v* has a particular value. The unique feature of AEBN approach is to allow such general situations, whereas other approaches require the beliefs of the two agents to be hard findings. The process of updating *v* in the presence of the probability distributions on B_1 and B_2 is called soft evidential update. We implemented a program (called BC Hugin) for soft evidential update that is described in [KVV02].

6. CONCLUSION

In this paper, we demonstrated the feasibility of probabilistic intrusion detection technique using soft evidential updates. We developed and implemented an intrusion detection architecture called Probabilistic Agent-Based Intrusion Detection (PAID). The advantages of our framework are that PAID:

1. needs low volume of data that must be sent over network in a distributed intrusion detection scenario.
2. provides a continuous scale to represent the probabilities of events. This feature allows easy exploration of the trade-off between sensitivity and selectivity that affects the rate of false positive and false negative decisions.
3. can support both misuse-detection based and anomaly-based intrusion detection.
4. processes intrusion detection efficiently due to its distributed nature and the fact that each agent is an autonomous entity. In addition, there is no single point of failure.

A proof-of-concept prototype of our model has been developed using Java, C, JADE and the soft evidential update program BC-Hugin. We are planning to further improve and fine-tune our current model to address agent trust management and dynamic agent-activation protocols.

Figure 2. Incorporating error in measurement of variable

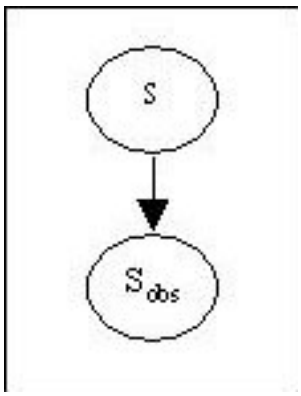
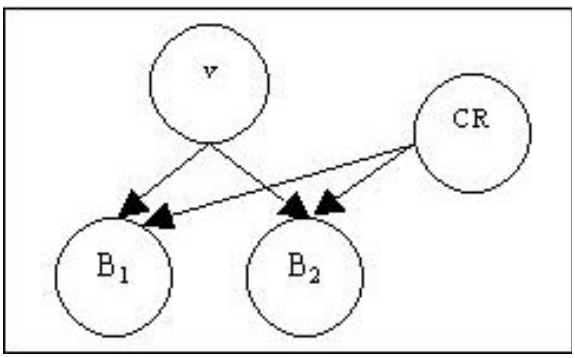


Figure 3. Conflict Resolution



ACKNOWLEDGEMENTS

This material is based upon work supported by the National Science Foundation under Grant No. 0112874

REFERENCES

[AFV95] D. Anderson, T. Frivold, and A. Valdes. "Next Generation Intrusion Detection Expert Systems (NIDES): A Summary." Technical Report SRI-CSL-95-07, SRI International, Menlo Park, CA, 1995

[ATG99] M.Asaka, A.Taguchi, and S.Goto. "The implementation of IDA: An Intrusion Detection Agent System", in Proceedings of the 11th FIRST Conference 1999, Brisbane, Australia, June 1999.

[Axel00] S. Axelsson. "Intrusion Detection Systems: A Taxonomy and Survey." Technical Report No 99-15, Dept of Computer Engineering, Chalmers University of Technology, Sweden, March 2000

[BFIS98] J. Balasubramaniyan, J.O. Garcia-Fernandez, D. Isacoff, E.H. Spafford, and D.M. Zamboni. "An Architecture for Intrusion Detection using Autonomous Agents." Technical Report, Dept. of Computer Science, Purdue Univ., West Lafayette, IN, 1998

[BMV02] Bloemeke, Mark and Marco Valtorta. "The Rumor Problem in Multiagent Systems." USC CSCE TR-2002-006, Department of Computer Science and Engineering, University of South Carolina, Columbia, 2002

[BPR99] F. Bellifemine, A. Poggi and G. Rimassa, "JADE – A FIPA compliant Agent Framework." *In Proc. of the 4th International Conference and Exhibition on The Practical Application of Intelligent Agents and Multi-Agents*, London, 1999

[BV99] D. Bulatovic and D. Velasevic, "A Distributed Intrusion Detection System Based on Bayesian Alarm Networks," *In Proc. of CQRE'99*, LNCS 1740, pp. 219–228, 1999.

[BWJ01] D. Barbara, N. Wu, and S. Jajodia. "Detecting Novel Network Intrusion using Bayes Estimator," *In Proc. of 1st SIAM Conference on Data Mining*, 2001

[Cann98] J. Cannady. "Artificial Neural Networks for Misuse Detection." *In Proc. of the 21st National Information Systems Security Conf.*, VA, 1998, pp. 441-454

[CERT] Center for Emergency Response Team, http://www.cert.org, 2002

[CHSP00] C.A. Carver, J.M. Hill, J.R. Surdu, and U.W. Pooch. "A Methodology for using Intelligent Agents to Provide Automated Intrusion Response." *In Proc. of the IEEE Systems, Man, and Cybernetics Information Assurance and Security Workshop*, West Point, NY, 2000

[CDLS99] Cowell, Robert G., A. Philip Dawid, Steffen L. Lauritzen, and David J. Spiegelhalter. *Probabilistic Networks and Expert Systems*. Springer-Verlag, 1999

[Coop90] Cooper, Gregory F. "The Computational Complexity of Probabilistic Inference Using Bayesian Networks." *Artificial Intelligence*, 42, 1990, pp.393-405.

[DM99] William DuMouchel. "Computer Intrusion Detection Based on Bayes Factors for Comparing Command Transition Probabilities," Technical Report No. 91, Feb 99, National Institute of Statistical Sciences.

[FACL02] FIPA ACL Message Structure Specifications, http://www.fipa.org/specs/fipa00061, 2002

[FIPAOS] FIPA-OS Developers Guide,http:///fipa-os.sourceforge.net/docs/Developers_ Guide.pdf, 2002

[GFV01] Vaibhav Gowadia, Csilla Farkas, and Marco Valtorta. "Intrusion Analysis with Soft Evidential Updates," USC CSCE TR-2001-005, Department of Computer Science, University of South Carolina, Columbia, 2002.

[HWHM00] G. Helmer, J. Wong, V. Honavar, and L. Miller. "Lightweight Agents for Intrusion Detection." *Submitted to Journal of Systems and Software*,2000. http:// citeseer.nj.nec.com/helmer00lightweight.html

[Jens01] Finn V. Jensen. *Bayesian Networks and Decision Graphs*. Springer, 2001.

[JMKM99] W. Jansen, P. Mell, T. Karygiannis, and D. Marks. "Applying mobile agents to intrusion detection and response." NISTIR-6416, September 1999

[KVV02]. Young-Gyun Kim, M. Valtorta, and J. Vomlel. "A Prototypical System for Soft Evidential Update." USC CSCE TR2002-005, Department of Computer Science and Engineering, University of South Carolina, Columbia, 2002.

[LS88] Steffen L. Lauritzen and David J. Spiegelhalter. "Local Computations with Probabilities on Graphical Structures and their Application to Expert Systems." *Journal of the Royal Statistical Society*, Series B, 50 (1988), 2, pp.157-224.

[LS98] W. Lee and S.J. Stolfo. "Data Mining Approaches for Intrusion Detection." *In Proc. of the 7th USENIX Security Symp*, San Antonio, TX, 1998, pp.79-94

[MST98] M. Meneganti, F.S. Saviello, and R.Tagliaferri. "Fuzzy Neural Networks for Classification and Detection of Anomalies." *IEEE Trans. On Neural Networks*, 9/5, 1998, pp. 848-861

[Neap90] Richard E. Neapolitan. Probabilistic Reasoning in Expert Systems. Wiley, 1990.

[Nort99] S. Northcutt, *Network Intrusion Detection: An Analyst's Handbook*, New Riders, 1999

[NP99] P.G. Neumann and P.A. Porras. Experiences with EMERALD to Date. *In Proc. of the 1st USENIX Workshop on Intrusion Detection and Network Monitoring*, Santa Clara, CA, 1999

[OSPF97] J. Moy. OSPF version 2. Internet Draft, RFC-2178, July 1997

[Pearl88] Judea Pearl. *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*. Morgan-Kaufmann, 1988.

[Perl92] R. Perlman. *Interconnections: Bridges and Routers*. Addison-Wesley, 1992.

[SB91] S. Snapp, J. Brentano. "DIDS (Distributed Intrusion Detection System) - Motivation, Architecture, and an Early Prototype." *In Proc. of the 1991 National Computer Security Conference*, 1991

[VKV02] Marco Valtorta, Young-Gyun Kim, and Jirí Vomlel. "Soft Evidential Update for Probabilistic Multiagent Systems." *International Journal of Approximate Reasoning*, 29, 1 (January 2002), pp.71-106.

[VS00] A. Valdes and K. Skinner. "Adaptive, Model-Based Monitoring for Cyber Attack Detection." *In Proc. RAID*, 2000, pp. 80-92

[XML] Extensible Markup Language Language 1.0 specification, http://www.w3.org/TR/2000/REC-xml-20001006, W3C Recommendation, October 2000