Assessing the Uncertainty of Communication Patterns in Distributed Intrusion Detection System*

Krzysztof Juszczyszyn and Grzegorz Kołaczek

Institute of Information Science and Engineering
Wroclaw University of Technology, Wroclaw, Poland
krzysztof@pwr.wroc.pl, grzesiek@pwr.wroc.pl

Abstract. A paper proposes a formal framework for communication patterns' uncertainty assessment within a distributed multiagent IDS architecture. The role of the detection of communication anomalies in IDS is discussed then it is shown how sequences of detectable patterns like fan-in, fan-out values for given network node and clustering coefficients can be used to detect network anomalies caused by security incidents (worm attack, virus spreading). It is defined how to use the proposed techniques in distributed IDS and backtrack the incidents.

1 Introduction

In order to process intrinsically distributed information, most of modern IDS systems are organized in a hierarchical architecture [4], consisting of low level nodes which collect information and management nodes which aim to detect large-scale phenomena. The task of management nodes is to reduce the amount of the data processed, identify attack situations as well as make decisions about responses [10].

In our approach it is assumed that the network system consists of the set of nodes. There are also two types of agents in our multiagent system: monitoring agents (MoA) and managing agents (MA). Monitoring agents observe the nodes, process captured information and draw conclusions that are necessary to evaluate the current state of system security within their areas of responsibility. Managing agents are responsible for gathering information from MoA agents and generating reports about global threats and ongoing attacks. Each agent MoA monitors its own area of responsibility consisting of the set of network nodes.

It is commonly known that in the case of worm attack there occur at least two kinds of anomalies: in observed traffic characteristics and in communication scheme which tends to be constant under normal conditions (see the next section). In this context the system properties observed by the agent MoA in the proposed architecture will fall into two basic (and physically different) categories: 1. Traffic measurement. 2. Communication pattern measurement. The decision about current situation is being made on the basis of them.

* This work was supported by the Polish State Committee for Scientific Research under Grant No. 3 T11C 029 29 (2005-2007).

B. Gabrys, R.J. Howlett, and L.C. Jain (Eds.): KES 2006, Part II, LNAI 4252, pp. 243 – 250, 2006.

The MoA agent's algorithm for decision making process is invoked periodically and uses observed values as input data. MoA also stores acquired values thus creating the history of system behaviour. The algorithm itself consists of the following steps (and was discussed in detail in [7]):

BEGIN
1. Detect traffic anomalies (using chosen technique).
2. Create a list of traffic anomalies.
3. Compute the communication patterns.
4. Create a list of communication anomalies.
5. If any of the anomalies' lists is not empty, perform an attack backtracking analysis which will return result in the form of attack graph.

END.

As mentioned, the managing agent MA successively obtains data which are related to particular moments of time from monitoring. Then the managing agent MA uses an algorithm for determining the global tree representing the attack propagation [7,8].

In this paper we deal with the 3rd and 4th steps of the above algorithm and show how to estimate the uncertainty of communication anomalies assessment and how to construct local attack graph on the basis of them. The method may be used independently but in the proposed architecture its results will be used together with other techniques (currently under development) in order to provide more accuracy in tracking attacks.

2 Communication Patterns

Network traffic show some quantitative and topological features that appear to be invariant and characteristic for given network [3,9]. Moreover, general rules underlying that features are the same for almost any network of remarkable size. These distinct features concern topology of network communication, considered as origin-destination flows graph, the distribution of data volumes sent between destinations and the in/out ratio of data sent between nodes/subnets and outside world.

With respect to these properties, wide range of network attacks can be detected by observation of communication patterns and comparison existing under normal state of the network to new ones which occur under attack. For example, in case of Internet worm attacks, within a network there could be scanning and attack flows which differ substantially from normal network activity [11]. Moreover, total scanning rate into the sub-network (or given set of nodes) is a function of the number of all infected nodes in the network.

Another invariant for a long time periods and different scales (subnet sizes) or traffic types (protocols) is proportion between a number of internal (Fan-in) and external (Fan-out) data flows [1]. Experiments showed that both Fan-in and Fan-out for given node and their distribution for all nodes tend to be constant under normal conditions. It was also shown that the IP graph has heavy-tailed degree distribution showing scale-free structure according to power law [3]. Under worm attack the structure of communication is heavily affected and the distribution changes. There is

also a detectible dependence between worm propagation algorithm, and communication pattern disturbance [9].

Similar relationships occur also on the level of given communication protocol, for example the topology of e-mail corporate networks exhibits a scale-free link distribution and small-world behaviour, as for known social networks. This result was recently used to propose an anti-spam tool [2].

2.1 Detectable Communication Patterns

Monitoring agents of proposed IDS system will gather information about communication within the network under state that is assumed to be secure. Then the existing communication patterns will be discovered. The system will be viewed as a graph consisting of nodes (each monitoring agent will have a set of nodes under control) and edges which appear if there exists data flow between given pair of nodes. In our approach we are interested in tracking the following communication patterns:

1. Clustering coefficient for a given node.

The *clustering coefficient* c is the probability that two nearest neighbours of vertex i are also neighbours of each other. The value of c provides a quantitative measure for cliques in communication graph. For node i clustering c_i is given by:

$$c_i = \frac{2k_i}{n_i(n_i - 1)} \tag{1}$$

where n_i is the number of its neighbours and k_i – the number of connections between them. High (close to one) c means that a node belongs to a clique in considered graph.

2. Fan-in and Fan-out ratios.

Fan-in is the number of nodes that originate data exchange with node i, while Fan-out is the number of hosts to which i initiates conversations.

According to results listed in previous section the above patterns are invariant during most time of normal system activity or change in a predictive way. But while attack appears they will change leading to alert and taking chosen countermeasures.

Each MoA agent stores data about communication in the form of M_c matrix. The values of M_c are set according to the following rules:

$$M_c(i, j) = \begin{cases} 1\text{: node } i \text{ communicates with node } j \\ \varepsilon\text{: lack of knowledge about communication between } i \text{ and } j \\ 0\text{: there is no communication between nodes } i \text{ and } j \end{cases}$$

Value ε reflects that accurate value of some fields in M_c matrix may be unknown (their actual values were for some reason not observed by MoA). This results in some uncertainty in attack investigation analysis. The level of this uncertainty will be also a part of the algorithm's result. As suggested in sec.1 the M_c entries are updated periodically in discrete time moments t. The history is stored by the MoA and forms a basis for anomalies' detection. Let's denote the state of M_c in t as M_c^t.

Before dealing with communication patterns' uncertainty we briefly introduce Subjective Logic, an useful and strong formalism for reasoning and expressing opinions about uncertain observations.

3 Subjective Logic

Subjective logic was proposed by A.Josang as a model for reasoning about trust propagation in secure information systems. It is compatible with Dempster-Shafer's theory of evidence and binary logic [5]. Subjective logic includes standard logic operators and additionally two special operators for combining beliefs – consensus and recommendation. The basic definitions of subjective logic given in this section come from [5,6].

Subjective logic can be used to express so-called opinions (see below) about facts with assumption that we do not require the knowledge of how these facts were grounded or inferred. We may also have an opinion about some subject (source of information). When expressing belief about a statement (predicate) it is assumed that it is either true or false, but we're not necessarily certain about it. Let's denote *belief*, *disbelief* and *uncertainty* as b, d and u respectively. A tuple $\omega = \langle b,d,u \rangle$ where $\langle b,d,u \rangle \in [0,1]^3$ and $b + d + u = 1$ is called an *opinion*.

Opinions have always assigned membership (are expressed by certain agents) and are not inherent qualities of objects but *judgments* about them. For any opinions $\omega_p = \langle b_p, d_p, u_p \rangle$ and $\omega_q = \langle b_q, d_q, u_q \rangle$ about predicates p and q the following operators may be defined (definitions, proofs and in-depth discussion are to be found in [6]): Conjunction (result of the conjunction of opinions is also an opinion and is denoted by $\omega_{p \wedge q}$), Disjunction ($\omega_{p \vee q}$), Negation ($\omega_{\neg p}$).

Now assume two agents, A and B, where A has opinion about B. Opinion about other agent is interpreted as opinion about proposition "*B's opinion is reliable*". We'll denote opinion expressed by agent B about given predicate p and agent's A opinion about B as ω_p^B and ω_B^A respectively. Then the opinion of agent A about p is given by *discounting operator* (a.k.a *reputation* operator, denoted by $\otimes$): $\omega_p^A = \omega_B^A \otimes \omega_p^B$. From the other hand, the joint opinion of two agents A and B about given predicate is computed by *consensus* operator $\oplus$ (ω_p^A and ω_p^B are opinions of A about B and B's about p): $\omega_p^{AB} = \omega_p^A \oplus \omega_p^B$.

Consensus operator is commutative and associative thus allowing to combine more opinions. Opinions about binary events can be projected onto a 1-dimensional probability space resulting in *probability expectation* $E(\omega_p)$ value for a given opinion:

$$E(\omega_p) = E(\langle b, d, u \rangle) = b + \frac{u}{2} \tag{2}$$

When ordering opinions the following rules (listed by priority) hold:

1. The opinion with the greatest probability expectation E is the greatest.
2. The opinion with the smallest uncertainty is the greatest.

Thus, for instance, $\langle 0.5, 0, 0.5 \rangle > \langle 0.4, 0.2, 0.4 \rangle > \langle 0.2, 0, 0.8 \rangle$.

4 Assessment of the Communication Patterns

We assume tracking three communication patterns: Fan-in (from here on denoted as $f^t_{in,i}$ for node *i* at time moment *t*), Fan-out ($f^t_{out,i}$) and clustering coefficient (c^t_i).

There are two main sources of uncertainty, when analyzing communication patterns. The first is lack of knowledge about existing communication (ε-edges in communication graph stored in communication matrix M_c). The second is that we actually need to know which communication pattern may be considered *normal* and which may be referred to as *anomaly*. This implies referring to the history (we assume that the attack is preceded by some period of normal system functioning) - the clear sign of the ongoing attack is rapid change of communication patterns being observed.

4.1 Fan-In, Fan-Out, Clustering Coefficient

As stated above our observations of communication patterns variables ($f^t_{in,i}$, $f^t_{out,i}$, c^t_i) are uncertain due to ε-values in M_c. As each of them may be in fact of the value 0 or 1 as well, we'll use the following formula to evaluate current values of the variables:

$$x = \frac{x_{(\varepsilon=0)} + x_{(\varepsilon=1)}}{2} \tag{3}$$

Where *x* stands for any of ($f^t_{in,i}, f^t_{out,i}, c^t_i$) and $x_{\varepsilon=0}$, $x_{\varepsilon=1}$ are their values under assumption that all ε values in M_c equal 0 or 1 respectively.

Now we should investigate which values of the parameter are *normal* (safe). Assume that the MoA's history consists of a number of observations of Fan-in values from some starting point up to current time *t*. So we have $f^1_{in,i}, f^2_{in,i}, \ldots f^t_{in,i}$. Let us now consider the Fan-in as a random variable $F_{in,i}$. Thus, ($f^1_{in,i}, f^2_{in,i}, \ldots f^t_{in,i}$) is a sample of size *t* of $F_{in,i}$. We also assume all of the $f_{in,i}$ to be independent. It is commonly known that the mean value and the variance of $F_{in,i}$ can be estimated by the following formulae:

$$\overline{\mathrm{F}}_{in,i} = \frac{1}{m}\sum_{k=1}^{t} f^k_{in,i} \tag{4}$$

$$\mathrm{S}_{\mathrm{in,i}} = \frac{1}{t-1}\sum_{k=1}^{t}(f^k_{in,i} - \overline{F}_{in,i})^2 \tag{5}$$

$\overline{\mathrm{F}}_{in,i}$ and $\mathrm{S}_{\mathrm{in,i}}$ are thus the estimations (based on the data being at our disposal) of mean value and the variance of $F_{in,i}$. Obviously the bigger our sample is, the better

they approximate $E(F_{in,i})$ and $Var(F_{in,i})$ respectively - from this point we assume that the observations' number is big enough to state that $E(F_{in,i})$ and $Var(F_{in,i})$ are known.

Let also $E(F_{out,i})$ and $Var(F_{out,i})$ for the Fan-in, as well as $E(C_i)$ and $Var(C_i)$ for clustering coefficient be defined in the same way.

4.2 Detecting Anomalies

As the MoA detects anomalies by formulating opinions about the node *i*'s state using Subjective Logic, appropriate values of a tuple $\omega^{MoA}_{i,abnormal\_x} = < b,d,u >$ (MoA's opinion that the value of parameter *x* at node *i* is abnormal) must be defined with respect to the current mean values and the variances of $F_{in,i}$, $F_{out,i}$ and $F_{c,i}$. The same as in equation (3) we assume that *x* stands for any of ($f^t_{in,i}, f^t_{out,i}, c^t_i$). Let us define *uncertainty, disbelief* and *belief* of MoA's opinion in the following way:

$$u = \frac{\sum_x \varepsilon}{\sum_x 1 + \sum_x \varepsilon} \tag{6}$$

Where $\sum_x \varepsilon$, $\sum_x 1$ is a total number of ε or 1 values in M^t_c for a particular *x*. From the Chebyshev's inequality we can estimate the upper bound of the probability that $\left|\overline{F} - x\right|$ is greater than *kS*. Where $\overline{F}$ and *S* are mean value and the variance of *X*, while *X* denotes the random variable related to *x* (in this case one of the following: $F^t_{in,i}, F^t_{out,i}, C^t_i$). According to this estimation the MoA's disbelief about the statement that *x* value is normal can be defined as follows:

$$d = \min(1-u, 1-\frac{1}{\alpha k^2}) \tag{7}$$

Where α is a coefficient which value should be set during a process of IDS tuning to the real network conditions and parameter *k* is:

$$k = \begin{cases} 1 & if \left|\frac{\overline{F}-x}{\sqrt{S}}\right| < 1 \\ \left|\frac{\overline{F}-x}{\sqrt{S}}\right| & if \left|\frac{\overline{F}-x}{\sqrt{S}}\right| \geq 1 \end{cases} \tag{8}$$

Finally the MoA's belief about the statement that *x* value is normal is evaluated using the subsequent formula:

$$b = 1 - u - d \tag{9}$$

5 The Backtracking Analysis – Building a Local Attack Graph

In the preceding section we show how the monitoring agents establish opinions about anomalies in given discrete moments of time. Let us define a communication anomaly occurring in time moment t and site s as a tuple $An_s^t = \langle s, \varpi_s, t \rangle$ where ϖ_s is the Subjective Logic's opinion associated with the anomaly ($Ex(\varpi_s)$, computed as given by (2) must exceed some required threshold to be positively recognised as an anomaly. The precise value of this threshold will be set during simulations and tuning of the IDS). As mentioned in sec.1 the task is (if only at least one anomaly was detected) to perform the backtracking analysis and produce the attack graph as defined in [7] and [8]. The generic algorithm for generating the attack graph is as follows: denote by $\boldsymbol{A}$ the set of agents; $\boldsymbol{S}$ – the set of sites of monitored system and $\boldsymbol{T}$ – the set of discrete ordered moments of time. A monitoring agent A_i observes the nodes and analyses gathered information in order to determine in given time moment t a graph $G_i^{(t)} = (S_i, R_i^{(t)})$, where $S_i \subset \boldsymbol{S}$ (the set of sites monitored by given A_i) and $R_i^{(t)}$ is a binary relation on S_i such that pair $\langle s,s' \rangle \in R_i^{(t)}$ for $s,s' \in S_i$ if and only if according to knowledge of agent A_i the attack has come directly from site s to s'. Let's define L_i^t as a list of all anomalies detected in time moment t within S_i by the agent A_i. The local attack graph building algorithm invoked by A_i when L_i^t is not empty has the form:

Given: M_c^t, L_i lists for all time moments up to current moment $t \in \boldsymbol{T}$.
Result: The graph $G_i^{(t)} = (S_i, R_i^{(t)})$.
BEGIN

1. Set $R_i^{(t)} = \varnothing$ (no attack relations at the beginning).
2. Pick an element An_s^t from L_i^t.
3. For An_s^t select $s' \in S_i$ such that: $M_c^t(s',s)=1$, there exists $An_{s'}^{t'}$ at moment $t'<t$, and $Ex(\varpi_{s'})$ at time t' is maximal (in case that there are more $An_{s'}^{t'}$). If there's no appropriate $s' \in S_i$ – go to step 2. Add $\langle s',s \rangle$ to $R_i^{(t)}$. Remove An_s^t from L_i^t. Recursively perform step 3 for $An_{s'}^{t'}$. Goto step 2.

END.

The partial attack graphs deduced by the monitoring agents are successively sent to the managing agent MA. The task of MA is to integrate their decisions in order to determine the global attack tree representing the propagation of the attack in the whole system. Owing to this global tree one should get to know the source of the attack as well as reason about its propagation plan.

6 Conclusions and Further Work

The proposed framework for communication anomalies detection is also compatible with the other elements of multiagent IDS architecture, as presented in sec.1. The use

of Subjective Logic's operators allow us to formally join (by means of Consensus operator) opinions about the same nodes on the level of MA. The MA may compute opinions about the credibility of monitoring agents (based on their former results) and apply them to their reports via Recommendation operator or use to take decisions about changing the MoA's areas of responsibility or delegating new ones. The above possibilities along with the algorithms for MA define important directions of forthcoming research. After testing and developing strategic algorithms for the managing agents we expect to create a full-fledged multiagent IDS environment.

The paper presented approach which will be the subject of further development and experiments under Polish State Committee for Scientific Research Grant no. 3 T11C 029 29 (2005-2007).

References

1. Allmanz M. et.al. A First Look at Modern Enterprise Traffic, In Proc. Internet Measurement Conference, October 2005, 217-231.
2. Boykin O., Roychowdhury V. Personal Email Networks: An Effective Anti-Spam Tool, IEEE Computer, **38(4)** (2005), 61-68.
3. Faloutsos M., Faloutsos P., Faloutsos C., On power-law relationships of the Internet topology. In Proc.ACM SIGCOMM '99 Conference on Applications, Technologies, Architectures, and Protocols for Computer Communication, August 1999, 251-262.
4. Gorodetski V., Karsaev O., Khabalov A., Kotenko I., Popyack L., Skormin V.: Agent-based model of Computer Network Security System: A Case Study. In: Proceedings of International Workshop Mathematical Methods, Models and Architectures for Computer Network Security, Lecture Notes in Computer Science, vol. 2052, Springer Verlag, Berlin Heidelberg New York (2001), 39-50.
5. Jøsang, A.: A Logic for Uncertain Probabilities. International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems, **9(3)** (2001) 279–311
6. Jøsang, A.: A Metric for Trusted Systems. In: Proceedings of the 21st National Security Conference, NSA (1998), 68-77
7. Juszczyszyn K, Nguyen N.T., Kolaczek G., Grzech A., Pieczynska A., Katarzyniak R. Agent-based Approach for Distributed Intrusion Detection System Design. International Conference on Computational Science 2006, Lecture Notes in Computer Science 3993 (2006) 224-231.
8. Kolaczek G., Kuchtiak-Pieczynska A., Juszczyszyn K., Grzech A., Katarzynak R., Nguyen N.T. (2005): A Mobile Agent Approach to Intrusion Detection in Network Systems. In: Proceedings of KES 2005, Lecture Notes in Artificial Intelligence 3682 (2005) 514-519.
9. Kohler E., Liy J., Paxson V., Shenker S., Observed Structure of Addresses in IP Traffic, In Proc. SIGCOMM Internet Measurement Workshop, November 2002, 253 - 266.
10. Kotenko I. et al.: Multi-Agent Modeling and Simulation of Distributed Denial-of-Service Attacks on Computer Networks, In: Proceedings of Third International Conference Navy and Shipbuilding Nowaday. St. Petersburg, (2003), 38-47.
11. Nicol D., Liljenstam M., Liu J., Multiscale Modeling and Simulation of Worm Effects on the Internet Routing Infrastructure, In Proc. Performance Tools Conference, 2003, 1- 10.