Proceedings of the Third International Conference on Machine Learning and Cybernetics, Shanghai, 26-29 August 2004

# THE NETWORK MANAGEMENT DESIGN INTEGRATED WITH THE INTRUSION DETECTION SYSTEM

XIN-YOU ZHANG, CHENG-ZHONG LI, QING-GUI HU

The School of Computer and Communication Engineering, Southwest Jiaotong University, Chengdu 610031, China
E-MAIL: xyzdog@21cn.com, lichengzhong@tsinghua.org.cn

**Abstract:**

**In order to improve the network management ability, The integration of network management with intrusion detection is an effective solution. The conception of network management and intrusion detection are introduced firstly. Then, SIDS, an integrated design, is analyzed, and the shortcomings of SIDS are also pointed out. Finally, NM-IDS, a new integrated design, in which the intrusion detection and the network management are integrated into a whole in the high layer, is put forward. NM-IDS not only can overcome the shortcomings of the SIDS, but also improves the ability of the network management and intrusion detection greatly.**

**Keywords:**

**Network management; intrusion detection; system architecture; SNMP; data collection**

## 1. Preface

The network management and the intrusion detection are the important two study areas of the computer network. The network management includes five areas: Performance management , Fault management, Configuration management, Accounting management, and Security management respectively. As for the network management on the basis of the Simple Network Management Protocol (SNMP), the former four areas could be achieved perfectly with the interrelated technology, and only the Security management could not be applied very well in the computer network system. Because the Intrusion Detection System (IDS) could not be integrated in the Network management system, then, besides buying the network management software, users had to buy the extra security devices such as the Firewall, IDS etc, which would place the heavy burden on the users and make the resources wasted.

The author first analyzes a network management design integrated with the distributed intrusion detection system, which is called SIDS [1] (Simple Intrusion Detection System), and then, points out the shortcomings of it. Finally, the author will put forward a new design model NM-IDS, in which the Intrusion Detection System is integrated in the Network Management System perfectly.

## 2. The Network Management and the Intrusion Detection System

### 2.1. The Network Management

To ensure the validity and the reliability of the network is the main purpose of the network management. And the network management must have the function to supervise the network resource, control the network resource and harmonize the network resource. For instance, the network management must have the function to configure the network equipments availably, to supervise the network malfunctions and revise them, to analyze the network's capability and adjust them, and to supervise the network's security and enforce the network's security etc.

The main two protocols about the network management are the SNMP designed by IETF and the CMIP designed by ISO. The first protocol is on the basis of TCP/IP, and it is simple and easy to apply. The second protocol is on the basis of the ISO's seven-layered model: OSI/RM, the function of CMIP is rather strong, but it is too complex. Though, most interrelated products based on the first protocol, at the same time, the second protocol is adopted widely due to its strong function in the telecom field.

The RFC3411 has defined the new management

0-7803-8403-2/04/$20.00 ©2004 IEEE

architecture: SNMPv3, which adopt modularized design idea to strengthen its security and make itself possessing the stronger ability to adapt the development in the future. The SNMP entity is an application of this architecture. Each SNMP entity includes a SNMP engine, one or several applications.

The main functions of the SNMP engine[②] are to send out signals, receive signals, authenticate information, encrypt information, and control the right accessing to managed object etc, which are corresponding to the SNMP entity. Each SNMP engine has only one identifier: SnmpEngineID. The SNMP engine consists of four components: a scheduler, a message process system, a security system and an access control system, respectively.

### 2.2. The Distributed Intrusion Detection System

The Distributed Intrusion Detection System[③⑤] is constructed by the combination of the intrusion detection system based on the host with the other one based on the network. A common Distributed Intrusion Detection System includes five components, which are data collection component, correspondence transport component, data analysis component, urgency process component and management component, respectively. Of course, those components are not independent completely, they could be combined mutually according to the design or concentrated into the same module. This system can distribute the data collecting task to every detection point existing in the network, which makes the detection efficiency and accuracy improving.

There are two intrusion detection methods[④]: anomaly intrusion detection and misuse intrusion detection. To the anomaly intrusion detection, it checks action of the user or the system, according to the computer resource used abnormally or not, to detect the intrusion action, but only on the condition that the intrusion action set be included in the anomaly action set could this method do its work. It forecasts intrusion action by detecting the deviation degree from the normal behavior.

The misuse intrusion detection, on the other hand, works by comparing the attack information collected with the message which have been stored in the system database. Obviously, if there are no proper system database, the misuse intrusion detection can not work well.

The misuse intrusion detection could directly detect out the adverse or non-accepted action, but the anomaly intrusion detection could detect out the actions violated to the normal actions.

According to user's needs, the data analysis could employ either the centralized model or the distributed model. The SIDS model employs the distributed model.

## 3. SIDS System Model

### 3.1. The Structure of the SIDS System Model

In order to detect out the intrusion action effectively in the large-scale network, and in order to embed the SIDS System Model into the current enterprise network management system smoothly, The SIDS model adopts the distributed model. The SIDS includes two types of agent, the one is the host agent and the other is network agent. The host agent is used to scan the host's log to discover the intrusion action, and the network agent is used to detect the network traffic or the doubtful action to discover the intrusion action. Each agent is located in its autonomous fields, and it could correspond with the common network management agents, what's more, it could control common network management agents and change their configuration. SIDS integrates the anomaly intrusion detection with the misuse intrusion detection.

The SIDS System can be divided three components, which are detector, controller and analyzer. The detector collects and audits the data, and sends the data to the MIB database included in controller. The controller has the primary analysis ability, after being analyzed, the data is send to the analyzer for further analysis. The architecture of the SIDS is figured as Figure 1.

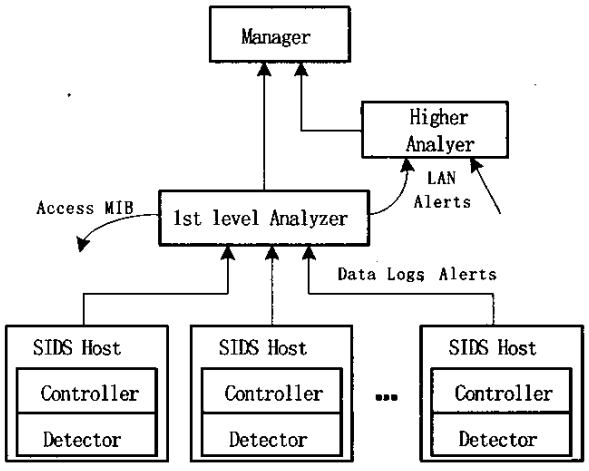

Figure 1. SIDS Architecture

#### 3.1.1. Detector

The detector is a data collection program or an SNMP agent, which is responsible for the data collection. Each detector is located in a particular autonomy field, and it is a light-weight process. All the detectors can be started and stopped by the controller, they can be configured again and upgraded. The running and configuration information of every agent's can be found out in the MIB. This design can let the manager get the dynamic information of the detector at any time, and can let the manager adjust appropriately the configuration of the detectors through the SNMP message to make the detectors running well.

#### 3.1.2. Controller

According to the size and the actual demand of the network, a controller can control several detectors. A controller consists of a first level analyzer, a local MIB and a SNMP agent.

The first level analyzer is responsible to analyze and filtrate the data collected by detector in order to find out the messages which have the obvious invading characteristic, then, the first level analyzer will put tag on those messages so that the higher level analyzer would audit those messages again. Some urgent messages could be reported up to the higher level analyzer by the Trap message through SNMP.

The MIB saves not only the related data collected, but also the related parameters that control the agent running and the thresholds to trigger alert etc. The SNMP agent is an interface for the analyzer to collect the data into the database. The performance of the controller would influence directly the running efficiency of the whole network.

#### 3.1.3. The Analyzer

A analyzer includes two SNMP correspondence modules, a database, a rule database, a network topology database, an analysis engine, and a graphical interface module.

The SNMP correspondence module is responsible to correspond between the controllers and the analyzers in the different layers. The database is used to save the historical data which is collected by detector or produced by lower analyzer. Compared the rules in the rule database with the data which needs to examine, analyzer could decide that the data suffers from invasion or not. The network topology database includes the information that is provided by the interrelated network manage modules and is used to describe the topology configuration of the whole network. analyzer engine is responsible to match the rule database with the data that needs check. The graphical interface module provides the manager with the friendly interface, which can let the manager get the information about the current security state of the network easily.

For the large enterprise, a network could include several subnets, we could configure it on several levels, in that case, the low level analyzer would provide data for the high analyzer.

#### 3.1.4. MIB database

The management information database of the SIDS system (SIDS MIB) contains the information collected by the detector, the configuration information of the detector itself and the control information. The design of the MIB should follow the data structure defined by SMIv2.

In order to make the data format used by different detectors accordant, the design of the MIB should be universal.

The management object designed in the network could be divided into the following object groups: SystemGroup, AgentGroup, ConfigGroup, LogGroup, TrapGroup, and RuleGroup.

How to realize this object groups? In fact, we could apply for a sub-node below the management object 1.3.6.1.4.1 , then, put the object groups under the node.

### 3.2. The Characters of the SIDS

Because the SIDS employs the loose-coupled distributed structure, then, one detector's malfunction could not influence the running of other detectors, which makes the system having high stability and reliability. The components employ SNMPv3 for corresponding with each other, and both the detection rules and the detector's parameters are saved in the MIB database, so, the manager could enlarge the rules database and/or add the detectors to make the intrusion detection and the network management system scalable and integrated closely.

At the same time, the SIDS has the following disadvantage:

Commonly, the SNMP agent works in the network equipments, if it must detect the intrusion actions meanwhile, large quantities of the network equipment's CPU time would be token, which would influence the

running efficiency of the network equipment greatly.

For some intrusion features difficult to be gotten, such as port scan, SYS Flooding etc. so we can't use the method based on the rule matching to detect it, it is difficult for us to detect it insides in SIDS.

Because both the structure and the level used by rule database in the MIB of the controller are different from that used by rule database in the analyzer, then, it will make the task's arrangement, the database's maintenance and upgrade difficult.

So, in this paper, the author puts forward a new design in which the intrusion detection and the network management would be integrated into a whole in the high layer, which is called Network Management Intrusion Detection System (NM-IDS).

## 4. The Model of NM-IDS

The task and processing mode of the IDS and network management are different. NM-IDS implements the integration of IDS and network management in higher level. So this design can reduce the workload of modifying the SNMP agent which is running now, so that each part of the system can exert its ability best. NM-IDS will work efficiently and expediently.

### 4.1. NM-IDS Architecture

An overview is given in Figure 2 and elaborated as below:

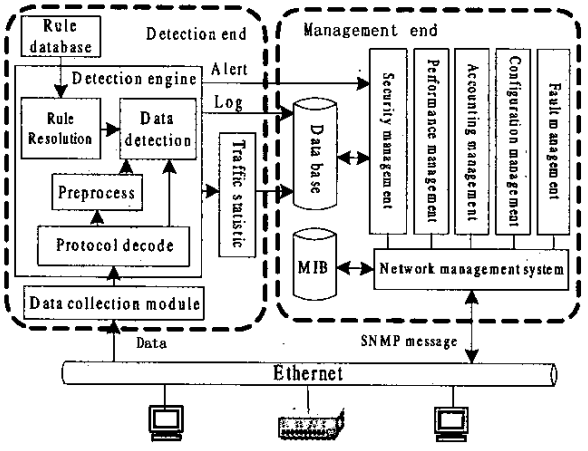


Figure 2. General Architecture

NM-IDS includes two parts: Detection end and Management end. Detection end includes Data collection module, Detection engine module, Rule database and Traffic statistic module. Management end includes system database and network management system based SNMP. Data collection module is responsible for collecting data packets from the network connected, and sending the data packets to the detection engine module, where the data packet is compared with the information stored in the rule database, then, the detection engine module decides if there are intrusion actions in the network or not. When there exists the intrusion, it will alert to the management end and write the log into system database, at the same time, management end processes and displays the alert it received. According to the protocol type, traffic statistic module counts the number of data packets, and writes the statistical information to the database.

Management end analyzes the data stored in MIB or system database further, so as to judge if there are intrusion behaviors in the network detected. If there are, management end must take actions to prevent intrusion behaviors. Meanwhile, management end can realize the other function of network management.

### 4.2. The Function of Detection End

#### 4.2.1. Data Collection Module

Data collection model mainly fulfills the function of collecting and filtrating the data detected from the network, which is approximately same as that of collector in the SIDS. It is different that data collection module and SNMP agent is not implemented by the same objective.

Data collection model can be implemented by using libpcap or winpcap function library.

#### 4.2.2. Protocol Decode Module

Detection engine is kernel of the detection end. It includes four sub-modules, which are Protocol decode module, Preprocess module, Rule resolution module and Data detection module.

Data collection module sends the Ethernet frames captured to the detection engine. After being decoded, these frames are put into interrelated data structure according to their protocol types, and are ready for being called by upper module. Moreover, protocol decode module must check over these frames to ensure their correctness (for example check sum). If there exist error frames, these frames will be discard.

In order to describe all kinds of data distinctly, data

structure must be designed properly, it is used to note the important information. For example, integrated data structure notes header key words of each layer protocol, protocol data structures note basic information of each kind of protocols.

#### 4.2.3. Preprocess Module

The function of preprocess module is to process data before being detected, so as to make data analyzed conveniently. Moreover, preprocess module can find out some kinds of intrusion and alert to management end. Because these kinds of intrusion have not evident attack features, so they could not be detected by data detect module, such kind of intrusion include port scanning, SYS flooding, fragments attack and so on. Preprocess module is more complex than other modules comparatively.

Plugin can be used to implement the preprocess module, which can make it convenient to add other function into the module, and make the system scalable perfectly.

#### 4.2.4. Rule Resolution Module and Data Detection Module

**(1) The Rule's Format**

The description method and detection option provided by rule reflect detection ability of the IDS directly. It is a good way to adopt descriptive methods of the intrusion feature used by Snort system. The rule set includes many "*.rules" files classed by application layer protocol. For example, dos.rules file stores rules of Deny of Service attack, and ftp.rules file store rules of ftp service attack.

A rule is divided two parts, header and option. The header includes action, protocol type and a data group including four parameters: source IP, source port, destination IP, destination port. The option consists of one option or a group formed by several options. All options are separated by semicolons, each option includes a keyword and its value, keyword and value are separated by a colon.

**(2) Rule Resolution**

The function of rule resolution is to decode the rules in .rules files discussed above, and then store it into memory by layered rule tree, the layered process of rules is carry out as follow:

The first layer consists of the nodes with the same actions (alert, discard or ignore), these nodes are expressed by RuleListNode data structure. The second layer nodes have the same action as that of the first layer nodes, but are branch out by different protocol types (IP, ICMP, TCP, UDP). Moreover, each node of the second layer includes the same four parameters: source IP addresses, source ports, destination IP addresses and destination ports, and the node is expressed by RuleTreeNode data structure. The nodes in the following layers include the same four parameters as upper layer nodes, but the options of nodes are different (see Figure 3). This kind of data structure can simplify search process and improve detection speed.

**(3) Data Detection**

The task of data detection is to receive the data that was already processed by lower module, and match the data to rules along the rules tree. If the match is successful, which means that there exists an intrusion in the network, data detection module then alerts to management end, and writes the alert information to system database for analyzed later. The match algorithm usually used include KMP (Knuth-Morris -Pratt) and BM (Boyer-Moore).

A lot of detection ends can be placed in different segment of the same network, which forms a distributed network management and intrusion detection system.

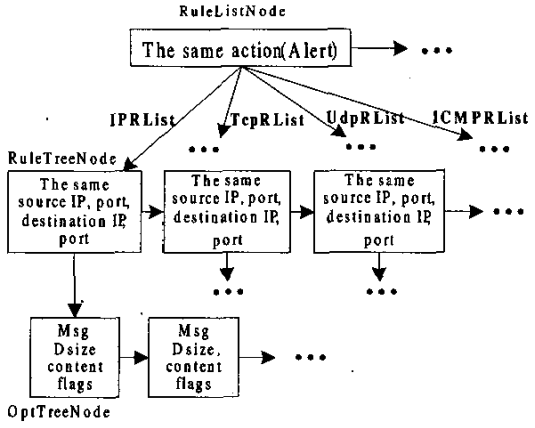


Figure 3. Structure of Rules Tree

#### 4.2.5. Data Statistic Module

The data produced by detection engine module, such as protocol type, protocol distribution, intrusion type, intrusion source, is stored in the table of the system database after being audited and classified. Depended on their different needs, user can decide which object would

be audited.

### 4.3. The Function of Management End

Management end includes a system database and all functions that SNMP manager should include.

It is these information including data statistic information, intrusion information, trap information come from SNMP agent and manager's operating information, that are stored in database. The system database cooperates with MIB, which can provide more information to manager for security analyzing and decision-making of the whole network. The tables in the database may include: intrusion information table, *protocol information table, traffic statistic table, trap log* table, manager operating log table, and so on. .

The function of management end include five areas that network management defined. There are two data sources in this design, the one comes from SNMP agent embedded in network device and is sent by SNMP message, the other comes from system database formed by the detection engine in detection end.

The two sources above mentioned have their features respectively. The network management based MIB can be implemented simply, and it's statistical data is more correct, device management is very convenient. But its shortcomings include: a little information about the protocol type, the lacking clues provided to manager to analyze the network condition, especially lacking for network security information. But the information that come from detection engine is plentiful, which helps the *manager to analyze network security, find out intrusion* action, and decide the method for preventing intrusion.

The ability of network management can be improved and network security can be enforced by integrating two kinds of data. Once an intrusion is detected, management end may modify the configuration of the firewall, router or switch to interrupt the intrusion action by sending SNMP message. If management end can not ensure that action is intrusion or not, it can analyze synthetically the information come from both MIB and system database. Moreover, management end can be more powerful and efficient by integrating with the techniques of artificial intelligence and expert system, which is next step for our to study.

## 5. Conclusions

This paper mainly discusses two designs that integrate IDS into network management system, the goal of those designs is to build a powerful network management system embedded with IDS. Firstly, Author introduces the SIDS architecture, describes function of each part of it, and analyzes the shortcomings of this design. Then, a new design, NM-IDS, is put forward, which not only keeps network management and IDS independent in lower layer and makes them integrated in management end, but also overcomes some shortcomings of the SIDS, reduces system's complexity, and improves management ability of the whole system.

## References

[1] Chris Christiansen, Roseann Day, John Daly, Brian Burke. Integrating Security Management Across Large Enterprises. http://www3.ca.com/Files/IndustryAnalystReports/Integrating_Security_Mgmt_Across_Lg_Ent.pdf.

[2] Panagiotis Astithas, Giorgos Koutepas, Athanassios Moralis, Basil Maglaris. Security Management in Large Enterprise Networks. Seventh Workshop of the HP OpenView University Association. 2000.

[3] Phil Porras, Dan Schnackenberg, Stuart Staniford-Chen, Maureen Stillman, and Felix Wu. The common intrusion detection framework architecture. http://www.gidos.org/drafts/architecture.txt. May 2001.

[4] Nicholas J. Puketza, Kui Zhang ,Mandy Chung, Biswanath Mukherjee, Member, IEEE, and Ronald A.OIsson. A methodology for testing intrusion detection systems. IEEE Transactions on software engineering. Vol 22, NO.10 October 1996.

[5] J.Pikoulas, W.Buchanan, M.Mannion, K.Triantafyllopoulos. An Intelligent Agent Security Intrusion System. Proceedings of the Ninth Annual IEEE International Conference and Workshop on the Engineering of Computer-Based System (ECB'02).