Implementation of Customized Monitoring Tool for Adapative Distributed Systems

Manjunath Kotari
Research Scholar
NMAMIT, Nitte

Dr. Niranjan N Chiplunkar
Principal
NMAMIT, Nitte

Dr. Nagesh H R
Prof & Head
MITE, Moodbidri

ABSTRACT

In the direction of cram the monitoring systems and identifying parameters that can be monitored with or without encrypting the data in an Adaptive Distributed System (ADS) which changes dynamically in the real time environment. By knowing the parameters the system can work more effectively by doing the necessary changes. The two problems that are addressed here are monitoring a system and collecting data necessary for adaptation, may cause security problems. In this paper we are addressing customized monitoring tool with the help of two modules. One of the module is System Under Study(SUS), a node in a distributed system; which sets the security level of its parameters like IP Address, Host-ID etc. and in turn it gives the permissions for monitoring same with or without encryption. Other module is Network Monitoring Tool(NMT), a monitoring node in a distributed system; gets the different parameters of SUS in encrypted format or unencrypted format depending on the security level set by SUS and decrypt its values for the purpose of adaptation in the distributed systems.

Keywords

Adaptive Distributed System (ADS), Network Monitoring Tool (NMT) ,System Under Study(SUS)

1. INTRODUCTION

Monitoring provides the necessary information in order to allow the construction of the required model of the observed system and its presentation. It is the purpose of monitoring which dictates what should be observed and also how the information is to be obtained. The purpose of monitoring is carried out in order to obtain information about a system, and in general, monitoring is part of the process of management. Among the many activities which involve monitoring we find: debugging, testing, accounting performance evaluation, resource utilization analysis, security fault detection, teaching aid.

There are critical differences between the internal monitoring and external network monitoring service. Internal monitoring[1] checks if the server and/or certain processes are up. Can check that if the web server is up, but would not check if application is really functioning. Another difference is that internal monitoring is watching the servers from within the data center.

An ADS[2] is a system that dynamically adjusts its behaviour based on changes in the environment. These changes could be network congestion, heavy load on the some systems, process or link failures, changes in communication patterns or frequency, changes in failure rates, or changed user requirements. Adaptation technique allows software or the system to modify its own functions and configuration in response to changes in its environment. Hence, adaptive distributed systems better know what is happening in their environment by detecting and evaluating the changes in the environment and adjusting their actions to the changes than the non-adaptive ones. Adaptation[3] can be achieved by allowing the system to collect detailed information by its monitoring subsystem. Allowing the monitoring system to gather information for the purpose of adaptation allows the adaptive distributed system to know more about changes in its environment and as a result the system can have best adaptive[4] capability to take proper action for the changes. But allowing the monitoring system to gather more detailed information can cause considerable security problem if the monitoring system is overtaken by intruders and as a result the information is available for the intruders. In this regard we are implemented a secured customized monitoring tool to gather information with the help of two different modules.

One of the module is System Under Study(SUS), a node in a distributed system; which sets the security level[4] of its parameters like IP Address, Host-ID etc. and in turn it gives the permissions for monitoring same with or without encryption. If the security level of parameter is high then encrypt the parameter. Other module is Network Monitoring Tool(NMT), a monitoring node in a distributed system; gets the different parameters of SUS in encrypted format or unencrypted format depending on the security level set by SUS and decrypt its values for the purpose of adaptation in the distributed systems. During the monitoring, if the intruder comes in between then intruder gets a encrypted format of the parameters.

2. LITERATURE REVIW

2.1 Security Issues in Adaptive Distributed Systems

Demissie B. Aredo et al.[3] presents monitoring of adaptive distributed systems and security metrics for the adaptive distributed systems by using security metric function. The basic components of ADSs include monitoring, change detection and reconfiguration in response to the changes in the environment. A monitoring component is employed for collecting information on parameters that can later be analyzed to detect changes in the environment of the target distributed system. The parameters that can be monitored may include the time it takes for a message to arrive at its destination, failure rates, and failures themselves. Demissie B. Aredo et al. [3] does not address about how to achieve an adaptation through the minimal impact on its security mechanism. Also the authors do not discuss about, what kind of data that can be monitored and how to monitor without affecting the performance of the distributed monitoring architecture. In our proposed framework we are going to address these issues.

2.2 Security Metrics for Adaptive Distributed Systems

Sule Yildirim et al. [4] proposed a security metric for quantifying the impact of monitoring on the effectiveness of security mechanism of the target systems. The metrics is a function of set of attributes of data to be collected by monitoring the system, which are relevant to the security implementation. Sule Yildirim et. al [3] [4] identified the following attributes as relevant to the security issues and the metrics are defined in terms of these attributes: level of Criticality, Detail, Size, and support for Inferences.

- Criticality of data is an attribute that indicates the importance of the data with respect to security.
- The detail attribute of data indicates the level of abstraction/concreteness of monitored data.
- The size attribute measures the amount of data collected during monitoring.
- By the support for inference attribute we mean the possibility to derive security relevant information about other data objects from given data.

The security metrics can be defined by the equation: $M = \alpha.C + \beta D + \lambda S + \eta I$ for some nonnegative coefficients α ,β ,λ and η . The values of these coefficients and their relationships can be determined using some analytical techniques.

Sule Yildirim et al. [4] does not address about detailed definition of security metrics. The parameters of the security metrics needs to be redefined, because detail of data is directly related to support for inference. In our proposed work, we are going to discuss these issues in detail.

2.3 An Adaptive Online Load-Balancing Algorithm for Distributed Range-Query Specialized Systems

In this work, Ioannis Konstantinou et al. presents PASSION[5], an on-line, adaptive load balancing algorithm that operates on distributed range-partitioned data structures. The algorithm operates in a completely decentralized manner and requires no kind of global coordination. Its goal is, through key exchange between neighboring nodes according to their current load and individual thresholds, to counterbalance the inequality in load that affects performance. Each peer, upon sensing an overload situation relative to its individual threshold, requests help and proactively sheds a suitable part of its load to its neighbors. Load moves in a "wave-like" fashion from more to less loaded regions of the structure adaptively.

The main idea behind *PASSION* is the following: When the current load of a node exceeds its self-imposed threshold *threshi*, the node sends a HelpRequest message containing its current load to one of its neighbours. The recipient node takes over a portion of the overloaded node's key range. This procedure is performed online, that is, nodes continue to serve requests during the key transfer. The recipient then estimates his new load and if this is above its local threshold, it initiates a new HelpRequest towards another neighbouring node. The procedure continues until all nodes have successfully shed their load below their thresholds.

But author has not addressed about how to monitor this threshold level securely with the help of monitoring node and how to use monitored data for the purpose of adaptive load balancing system.

2.4 On Fully Distributed Adaptive Load Balancing

Monitoring is an inherent part of the management loop. This paper studies the problem of quantifying utility of monitoring in a fully distributed load balancing setting. David Breitgand et al.[6] consider a system where job requests arrive to a collection of *n* identical servers. The goal is to provide the service with the lowest possible average waiting time in a fully distributed manner (to increase scalability and robustness). They present a novel adaptive load balancing heuristic that maximizes utility of information sharing between the servers. The main idea is to forward the job request to a randomly chosen server and to collect load information on the request packet as it moves on. Each server decides, based on that information, whether to forward the job request packet to another server, or to execute it locally.

But the authors not addressed about how to balance the load without forwarding the packets to its neighboring server.

3. PROPOSED SYETM

3.1 Problem Statement

It is obvious that a monitoring component aims at becoming more knowledgeable about the environment it is functioning in so that the changes in the distributed environment can be detected and corresponding actions can be taken in order to compensate for the changes in the environment for the purposes of providing acceptable quality of service. There are few main problems in Adaptive Distributed Systems. One of the problem is, monitoring a system[3] and collecting data necessary for adaptation may cause security problems.
For this reason we have identified the following parameters and for these parameters we need to find the level of security required are ,IP Address ,User Name, Host ID, Network ID, Port Number ,File Name, File Content, Network Connectivity, Processor Response Time, Processor Utilization or CPU Utilization , Memory and Disk. The above said parameters are required in secured adaptation.

IP address[7] personally identifiable information. IP address provides an identification and location system for computers on networks and Routes traffic across the internet. Network activity of each device can be tracked. The host address[7], or the host ID portion of an IP address, used to identify hosts on the network. The host-id is used by licensing software to "lock" a license to a machine so that they can be used on only that computer. CPU time[7] and CPU usage have two main uses. When the CPU usage is above 70%, the user may experience lag. A high CPU usage may be useful in the adaptive load balancing. The network ID[7], is the portion of the IP address that refers to the network itself. If the Network ID & Permissions attacked by Malware, it causes a mess without tripping any alarms. Concluding that Network Id is extremely critical, less size and less detailed parameter. Sensitive information are stored in files[7] these days. Servers, workstations, backup tapes, USB drives, laptops etc, they all contain sensitive and mission critical information. Primary memory[7], secondary Memory , additional Hard disks and other storage devices are considered. Based on the importance or level of confidentiality of the data stored its concluded for its criticality, detail and sizes.

3.2 General Objective

The main objective of this study is to identify the type of parameters that can be monitored with and without encryption and implementing secured customized monitoring tool.

- To implement customized monitoring tool by providing necessary security for parameters while gathering information.

3.3 Specific Objective

In particular, the proposed secured customized monitoring tool contains two different modules. One of the modules is SUS, a node in a distributed system to be monitored by monitoring system; sets the security level of its parameters like IP Address, Host-ID etc. for making parameter more secure.

The security level of the each parameter is defined in following manner. The criticality level of each parameter out of 100 weight can defined as ; 0-25 means Not Critical, 26-50 means Less Critical, 51-75 means Medium Critical, 76-80 means Critical and 81-100 means Extremely Critical. Also the level of detail of each parameter out of 100 weight can be defined as; 0-25 means Not Detailed, 26-50 means Less Detailed, 51-75 means Moderate Detailed and 76-100 means Full Detailed. Similarly the level of size of each parameter out of weight 100 can be defined as; 0-25 means less size, 26-50 means Moderated Size and 51-100 means fully sized. The security metrics(SM)[4], can be defined, as in

$$SM = a.C + b.D. + c.S \qquad Eq\text{-}1$$

- C is the level of security criticality attribute of the data

- D is the level of the detail of the data

- S is the size of the data

- a, b, c are non-negative coefficients whose values and relationships can be determined using some analytical techniques.

After calculating SM value for each parameter the SUS node can decide whether to monitor that parameter with or without encryption. The SUS node will sets the security level and in turn it gives the permissions for monitoring same with or without encryption. If the SM value of parameter is high then encrypt the parameter by using Rijndael Algorithm[8].

The second module in the proposal is NMT, a monitoring node in a distributed system; gets the different parameters of SUS in encrypted format or unencrypted format depending on the security level set by SUS. If the parameter of SUS is encrypted then NMT applies decryption function. During this monitoring, if the intruder attacks in between the NMT and SUS then intruder gets a encrypted format of the parameters only.

4. IMPLEMENTATION & RESULTS

4.1 Parameter Collection

A simple client-server application that establishes remoting communication in two directions while using infrastructure components that extract the common remoting related tasks from the application as shown in Fig. 1.

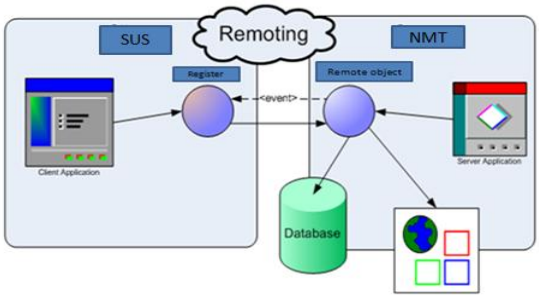

Figure.1. Remoting

4.2 Results of System under Study and Network Monitoring Tool

In this secured customized Monitoring Tool, systems are connected over a LAN/WAN, where one system acts as a Monitoring System known as Network Monitoring Tool (NMT) and other systems which are monitored by NMT are called as System Under Study (SUS).

The application is running in the SUS system and the values of each parameter are specified by the user or SUS node for the calculation of the level of criticality, detail and size of the parameters of the system. The SUS system needs to enter IP Address of NMT for giving permission to monitor SUS by NMT. This scenario can be viewed as shown in the Fig.2.

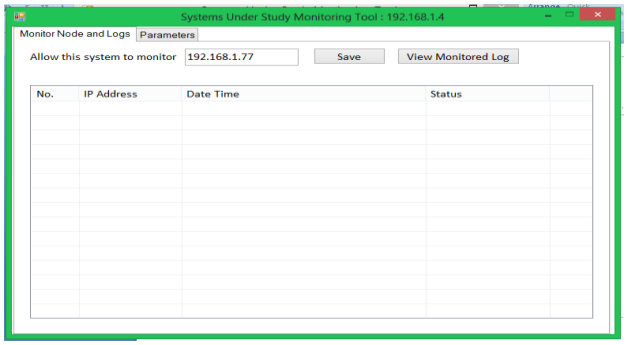

Figure. 2 SUS Monitoring Tool allows NMT to Monitor

The SUS system can set its security levels by setting three values C,D and S for each parameters. Also it calculates the SM value as shown in the Fig. 3 for the purpose of monitoring these parameters confidentially by NMT.

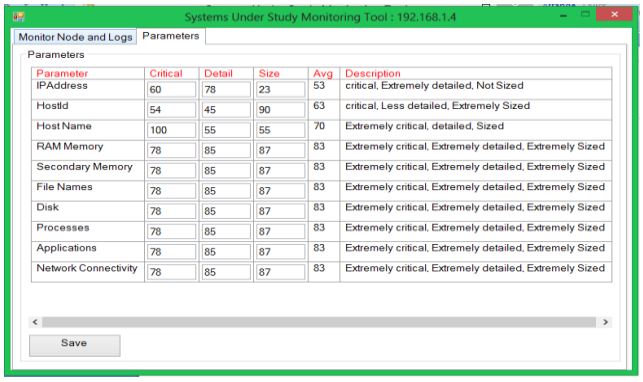

Figure. 3 SUS sets C,D & S values and saves

The IP-address of the SUS to be monitored is selected and viewed by NMT is as shown in Fig. 3. Here NMT system will select the IP address of different SUS system one at a time and presses view button to gather the information about SUS. NMT node selects the SUS IP address over the network, alongside number of other systems are also exists.

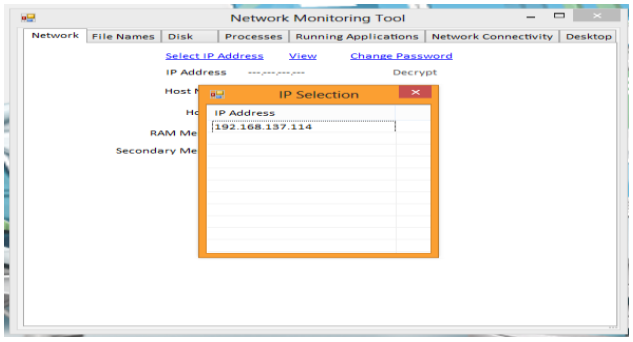

Figure. 4: NMT Selects IP Address of SUS

Based on the SM value of each parameter, the NMT node will gather information about SUS in the encrypted manner only as shown in Fig.4. The NMT node then clicks on decrypt button and supply the key for getting the information about parameters of SUS.

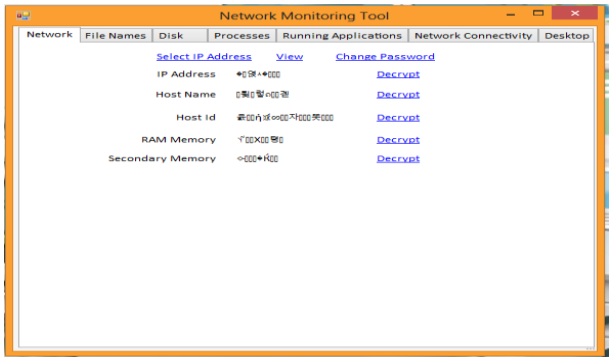

Figure. 5 Encrypted details of SUS viewed by NMT

The NMT system supplies valid key for decryption process and decrypted values of Host-ID of SUS system displays on NMT nodes screen is as shown in Fig. 5.

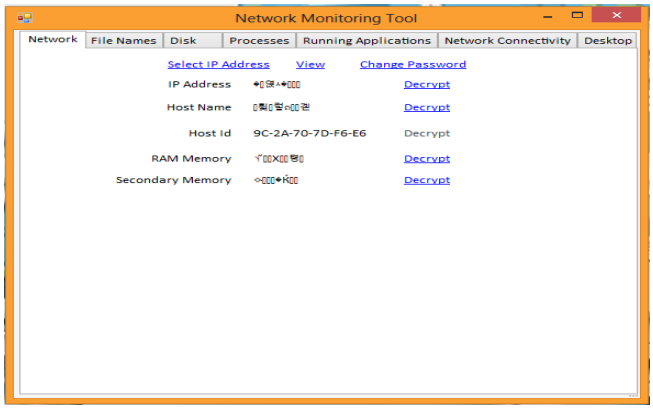

Figure. 6 Decrypted Host ID of SUS

Suppose SUS system is not giving its permissions to NMT system then NMT system can view the details of SUS in encrypted format only without any decryption option as shown in Fig. 6. Even if intruder node tries to gather the information about SUS, then intruder node will get a encrypted format of data.

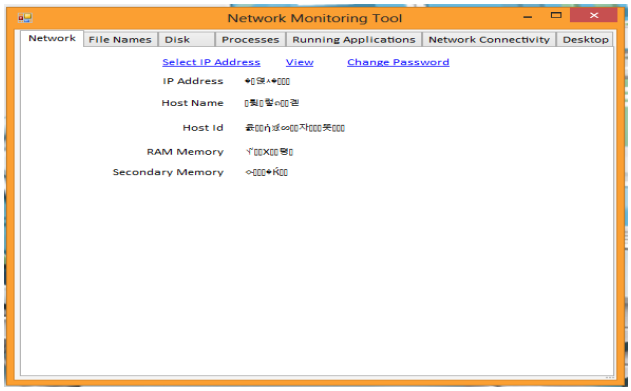

Figure. 7 SUS not allowed to Monitor by NMT

Likewise monitoring of IP Address, Host ID, Memory and HostName, the NMT can also monitor File Names present in the SUS system, Number of Disk and Disk spaces, Processes, number of running applications and Network Connectivity of various SUS. The Fig. 8 shows the different Network Interfaces of SUS systems.

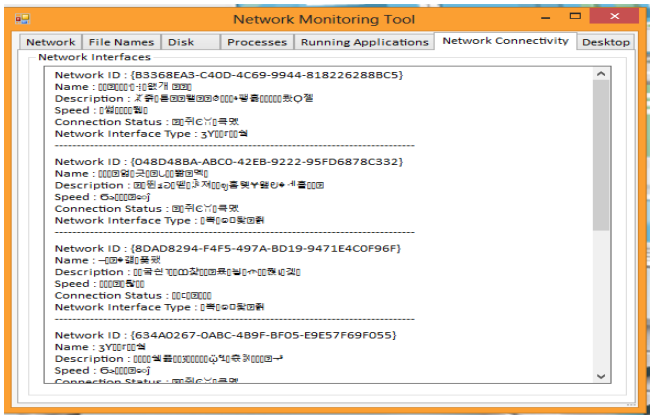

Fig. 8 Network Connectivity of SUS monitored by NMT

4.3 Analysis of Results over existing monitoirng tool

The Secure customized network monitoring tool is better than the existing network monitoring tool in the following manner.

- Only essential data can be monitored with this customized monitoring tool. But where as in existing monitoring tool like Wireshark monitors all the parameters which present in the networked computers and user does not have any hold to controlling the monitoring.
- In case of secure customized monitoring tool the user can set the criticality level of each parameter and it provides a security to each confidential parameter.
- In case of using existing monitoring tool user can not able to encrypt each parameter separately; only users message can be encrypted.
- Security level of each parameter can be calculated with help of security metrics equation in case of customized monitoring tool.
- The performance of customized tool increases because of only essential data monitoring.

5. CONCLUSION AND FUTURE ENHANCEMENT

The Secured Customized Network Monitoring Tool is developed for adaptive distributed systems. The developed tool fetches the required information of the distributed systems that has to be monitored over the network once they are connected. The customized monitoring involves two phases. In the first phase System Under Study(SUS) sets the security level of its parameters like IP Address, Host-ID etc. and in turn it provides a security to its parameters in such a way that only NMT node is permitted to monitor this SUS. If the security metrics value of particular parameter is high then it encrypts the parameter. The second phase involves secure monitoring, the Network Monitoring Tool(NMT),monitors the different parameters of SUS in encrypted format or unencrypted format depending on the security level set by SUS. The monitoring node decrypts its values by using valid key. The intruders have no chance to gather this information; since all the confidential parameters are in encrypted format.

The future work involves the usage of gathered information in adaptive distributed systems functionalities like adaptive load balancing and adaptive network congestions.

6. ACKNOWLEDGMENTS

Our thanks to the M.Tech Student Sunil Dasharathi M for his contribution towards the implementation of the above proposed problem.

7. REFERENCES

[1] Manjunath Kotari , Niranjan N.Chiplunkar, Nagesh H R , Security Aspects of Adaptive Distributed Systems and proposed solutions by ANUSANDHANA-Journal of Science, Engineering and Management-Vol-01, Issue-01, March-2012.(pp 45-49)

[2] R. D. Schlichting (1998). Designing and Implementing Adaptive Distributed Systems, available at http://www.cs.arizona.edu/adaptiveds/overview.html.

[3] Demissie B. Aredo, METRICS FOR QUANTIFYING THE IMPACTS OF MONITORING ON SECURITY OF ADAPTIVE DISTRIBUTED SYSTEMS. MASTER THESIS PROPOSAL – II, http://www.ifi.uio.no/~demissie (December 2005.).

[4] Aredo D. and Yildirim S., Security Issues in Adaptive Distributed Systems. Proceedings of the Fourteenth European Conference on Information Systems (ECIS 2006), Goteborg, Sweden.

[5] Ioannis Konstantinou, Dimitrios Tsoumakos, and Nectarios Koziris, PASS It ON (PASSION): An Adaptive Online Load-Balancing Algorithm for Distributed Range-Query Specialized Systems, OTM 2008 Workshops, LNCS 5333, pp. 3–5, 2008, Springer-Verlag Berlin Heidelberg 2008.

[6] David Breitgand1, Rami Cohen2, Amir Nahir1, and Danny Raz2, On Fully Distributed Adaptive Load Balancing,DSOM 2007, LNCS 4785, pp. 74–85, 2007.,IFIP International Federation for Information Processing 2007.

[7] http://netsecurity.about.com/cs/generalsecurity

[8] Joan Daemen, Vincent Rijmen, Advanced Encryption Standard, publication of Federal Information Processing Standard (FIPS), May-2001

[9] David Breitgand, Rami Cohen, Amir Nahir, and Danny Raz, On Cost-Aware Monitoring for Self-Adaptive Load Sharing, IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 28, NO. 1, JANUARY 2010

[10] Chun-Chieh Yang1, Ssu-Hsuan Lu1, Hsiao-Hsi Wang1, and Kuan-Ching Li2, On Design and Implementation of Adaptive Data Classification Scheme for DSM Systems, ISPA 2006, LNCS 4330, pp. 794 – 805, 2006.Springer-Verlag Berlin Heidelberg 2006.