Design and Development of Network Monitoring and Controlling Tool for Department of Computer Studies CSIBER

Mr. M. B. Patil
Department of Computer Studies
Chatrapati Shahu Institute of Business Education and Research
Kolhapur, India
mbpatil@siberindia.edu.in

Dr. R.S.Kamath
Department of Computer Studies
Chatrapati Shahu Institute of Business Education and Research
Kolhapur, India
rs_kamath@rediffmail.com

Dr. P.G. Naik
Department of Computer Studies
Chatrapati Shahu Institute of Business Education and Research
Kolhapur, India
luckysankalp@yahoo.com

Abstract— In most of the organizations it is highly desirable to perform different tasks on different machines based on their configuration and permissions assigned to the machines for execution of different tasks. This can be achieved by performing a user-machine mapping by stating clearing the list of tasks that can be performed by a particular user on a particular machine. This kind of discipline further enables traffic control, prevents internal DOS (Denial Of Service) attacks for legitimate users and helps in fair resource sharing. The intent of this research is to enable the end user performing only the tasks permissible to him/her. In this paper we have developed a network monitor and control tool for monitoring the tasks on a medium sized local area network. To facilitate this, task permissions are assigned to different machines which are stored in XML configuration file which is then parsed using JDOM (Java Document Object Model) Parser. The configuration file contains the details such as machine name, and the list of tasks not permitted on that machine. The list of machines and the list of tasks denied on that machine are configurable by an end user. A background thread will continuously monitor the execution of illegal task on a machine and will abort and report the same in a database. This also facilitates the control of network traffic thereby improving the network performance by aborting illegal tasks. Network monitoring tool is tested for local area network of department of computer studies at SIBER by setting up specific monitors to check status and to carry out specific operations. The tool developed by us requires a small amount of system resources, and it is an open source tool. Presently, the tool generates a report comprising of a list of illegal tasks in a specified time period, which enables network administrator to take corrective measures for the smooth operation of the network.

Keywords*- Illegal Tasks; JDOM; Network Management; Workgroup; XML Parser*

*****

I. INTRODUCTION

Network management is a process of monitoring and controlling the network to ensure that it is operational, works and provides value to the network administrator and its users. As organizations have become increasingly dependent on their networked computing environments, the importance of effective network management has become a key element in the success of those networks. A smooth working of the network should identify network bottlenecks and guarantee fair allocation of resources to all users of the network. Network management is a broad topic which involves software management, hardware management, file management, security management and user management. In this paper we emphasize on user management alone by ensuring a fair share of the available network resources to each user of the network.

Network management is a combination of technical skills that a technician can offer mixed with a product/application that can be used to aid in both monitoring infrastructure and further controlling it. The products typically work by providing a management console that can contain multiple items to manage, or by grouping many functions into one executable function. In sum, it makes network functioning smooth and makes it more manageable. Network management is the operation, administration and maintenance, and provisioning (OAMP) of networked systems. Network management is essential to command and control practices.

- Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- Administration deals with keeping track of resources in the network and how they are assigned.
- Maintenance is concerned with performing repairs and upgrades.
- Provisioning is concerned with configuring resources in the network to support a given service.

II. LITERATURE REVIEW AND PRIOR ART

In literature, there exist variety of tools for monitoring and controlling network traffic for both wired and wireless networks and most of them aim at controlling of network traffic. NetBalancer [1] is one such Traffic Control and Monitoring Tool designed for Microsoft Windows XP, 2003, Vista, 7, 8 with native x64 support. This tool is used to set for any process a download and/or upload network priority or limit, manage priorities and limits for each network adapter separately, define detailed network traffic rules, group local network computers and balance their traffic synchronized, set global traffic limits, show network traffic in system tray. NetLimiter [2] is yet another internet traffic control and monitoring tool designed for Windows. This tool can be used for full internet bandwidth control over applications and computers, powerful connection blocker, long-term internet traffic statistics, fully customizable behavior using user-defined Rules and Filters.

Network Access Control (NAC) [3] is a complete standards-based, multi-vendor interoperable solution for wired and wireless LAN and VPN users. It can deploy a leading-edge NAC solution to ensure only the right users have access to the right information from the right place at the right time including time of day, location, authentication types, device and OS type, and end system and user groups. Infoblox [4] delivers a Control Plane that sits between and integrates with the network infrastructure device layer and the applications, virtual machines and end-points. Infoblox delivers the discovery, compliance, and real-time configuration and change management needed for all network infrastructure devices, as well as the essential network control functions like DNS, DHCP and IP address management (IPAM). As network requirements have evolved, Infoblox has stayed ahead of the curve by developing and integrating solutions to solve common enterprise challenges and, more importantly, maximize return on investments in Infoblox deployments.

Rao [5] in his paper has reviewed the various tools and solutions available for network management, challenges involved in implementing network management solutions and also a simple solution for a pro-active network management solution is proposed. This solution was tested by implementing in a large enterprise. With the implementation, the stakeholders were able to achieve higher efficiency and able to do proactive network management. This paper discusses the challenges involved in implementing the network management solution using commercially available NMS tools and possible solution to implement the same. The solution was implemented in more than one enterprise with strength of more than 1000 full time employees and geographically spread across, with at least three branch offices. All the branch offices were connected through WAN.

Authors of paper [6] have reported the tools that users currently rely on for their home network management, the usability problems with those tools, and some desirable features for a tool for householders. The data was collected from 25 home network users in Atlanta, USA. The study depicts that householders currently rely mainly on the tools built into the OS and the router to perform management tasks in their home, despite the widely perceived usability problems of these tools, not least of which is the relatively sophisticated level of technical knowledge required in order to use them effectively. The results of this study provide initial clues on the practices of home network management of householders, as well as design implications for future kinds of home network management tools.

Vaarandi [7] has developed a lightweight platform independent tool for rule-based event correlation called sec (Simple Event Correlator). The primary design goal of sec was to create an open source tool that could be used for both central and local event correlation, regardless of the underlying operating system, and that could be integrated into an arbitrary network management system. Sec is a rule-based event correlation tool that receives its input events from a file stream, and produces output events by executing user-specified shell commands.

Yang et.al. [8] have presented Eden, an interactive, direct manipulation home network management system aimed at end users. Eden supports a range of common tasks, and provides a simple conceptual model that can help users understand key aspects of networking better. It provides a range of mechanisms for supporting end user management of home networks while retaining compatibility with existing IP based applications and devices. The system leverages a novel home network router that acts as a “dropin” replacement for users’ current router. Authors demonstrated that Eden not only improves the user experience of networking, but also aids users in forming workable conceptual models of how the network works.

In this paper we present a generic network management automation tool for monitoring the illegal tasks executed on different machines of the network. Machine-task mapping information is stored in an XML file which is well formed and valid. The Document Type Definition (DTD) for the XML document is presented. The Graphical User Interface (GUI) is designed in VB and other functions such as listing all machines in the current network, identifying active processes on each machine in the network, validating these processing against data stored in XML file by parsing XML file using DOM parser etc. are carried out in Java. The communication between VB and Java is established using intermediate RDBMS system designed in MS-Access.

III. DESIGN FRAMEWORK

The application architecture for implementation of the tool and the interaction between various modules in the application is depicted in the following Figure 1 (a) and the corresponding control flow logic is shown in figure 1 (b).

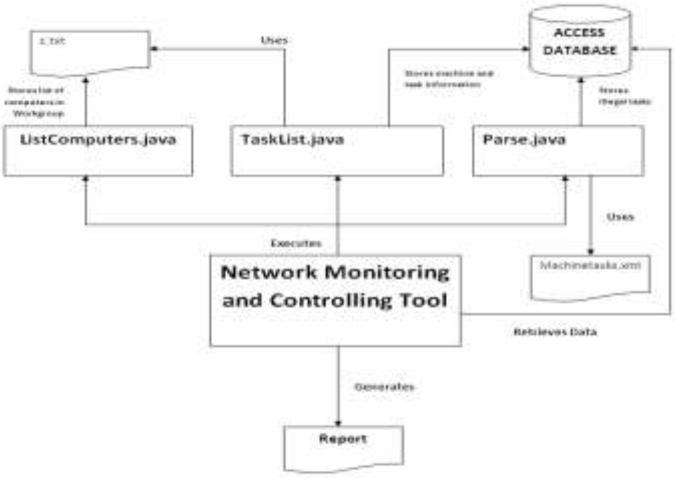


Figure 1 (a). Application Architecture

IV. Assumptions in Tool Development

1. The correctness of the tool depends on the accuracy of the output generated by the net view, tasklist and taskkill commands.
2. The tool is intended only for medium sized network running windows nodes.

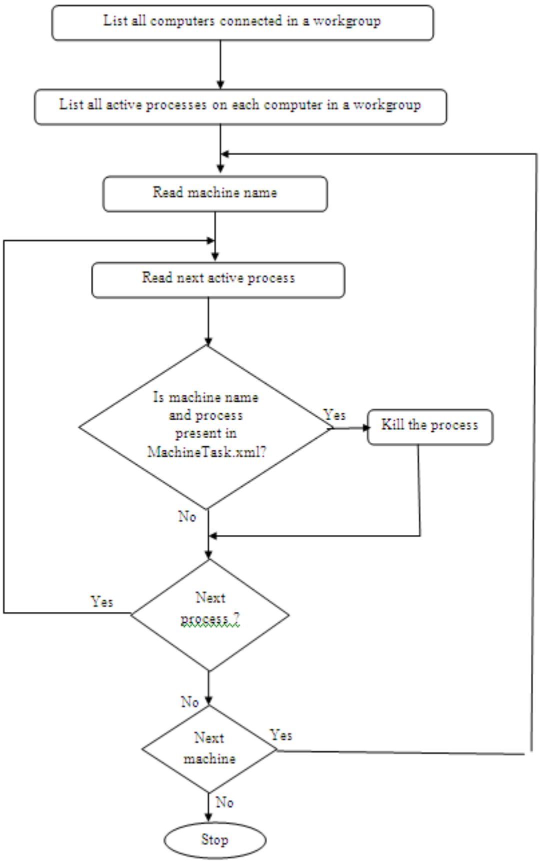
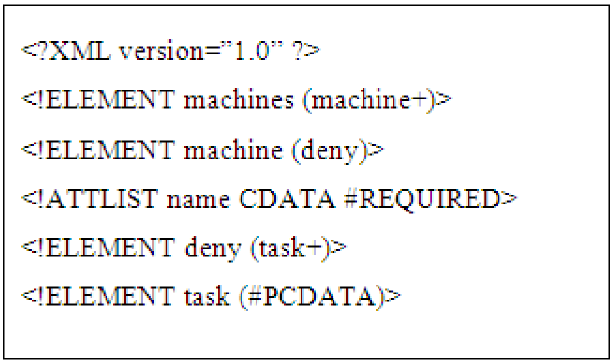

List all computers connected in a workgroup
List all active processes on each computer in a workgroup
Read machine name
Read next active process
Is machine name and process present in MachineTask.xml?
Yes
Kill the process
No
Next process ?
Yes
No
Next machine
Yes
No
Stop

Figure 1 (b). Application Architecture

V. Application Modules

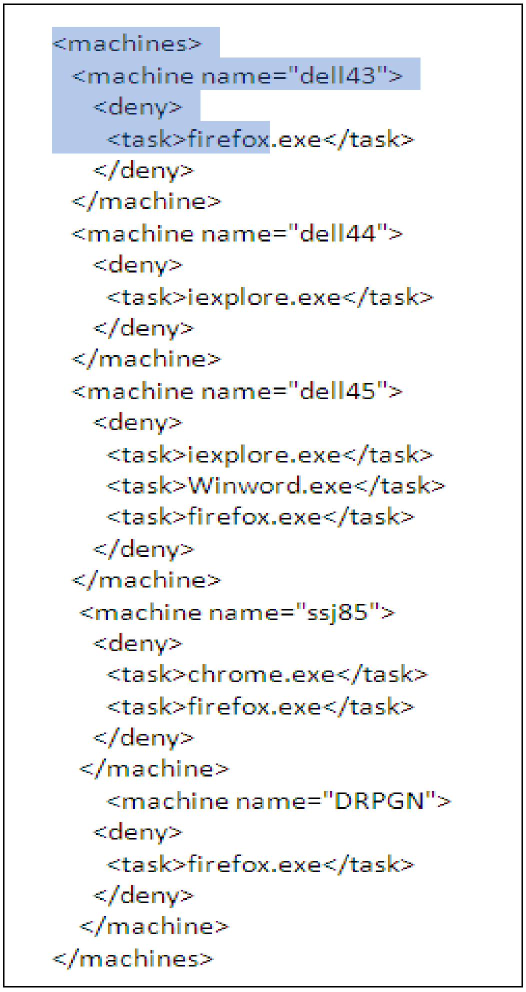
A. *Storing task permissions on various machines in XML configuration file.*

For the smooth operation of the network and controlling the execution of certain tasks only on certain machines and only for certain users based on their position in the organization/institution, the list of tasks which are not permissible on certain machines is documented in an XML file with the structure shown in Figure 2 and the corresponding DTD is shown in Figure 3.



```
<?XML version="1.0" ?>
<!ELEMENT machines (machine+)>
<!ELEMENT machine (deny)>
<!ATTLIST name CDATA #REQUIRED>
<!ELEMENT deny (task+)>
<!ELEMENT task (#PCDATA)>
```

Figure 3. DTD Specification for XML Document



```
<machines>
  <machine name="dell43">
    <deny>
      <task>firefox.exe</task>
    </deny>
  </machine>
  <machine name="dell44">
    <deny>
      <task>iexplore.exe</task>
    </deny>
  </machine>
  <machine name="dell45">
    <deny>
      <task>iexplore.exe</task>
      <task>Winword.exe</task>
      <task>firefox.exe</task>
    </deny>
  </machine>
   <machine name="ssj85">
    <deny>
      <task>chrome.exe</task>
      <task>firefox.exe</task>
    </deny>
   </machine>
      <machine name="DRPGN">
    <deny>
      <task>firefox.exe</task>
    </deny>
   </machine>
</machines>
```

Figure 2. Structure of XML Configuration File

B. To list the computers connected in the Network Workgroup

We have employed the well documented NET VIEW command to view a list of computers or network resources. The NET VIEW command displays a list of computers in the specified workgroup, or shared resources available on the specified computer.

C. To list the active processes on each computer in the Workgroup

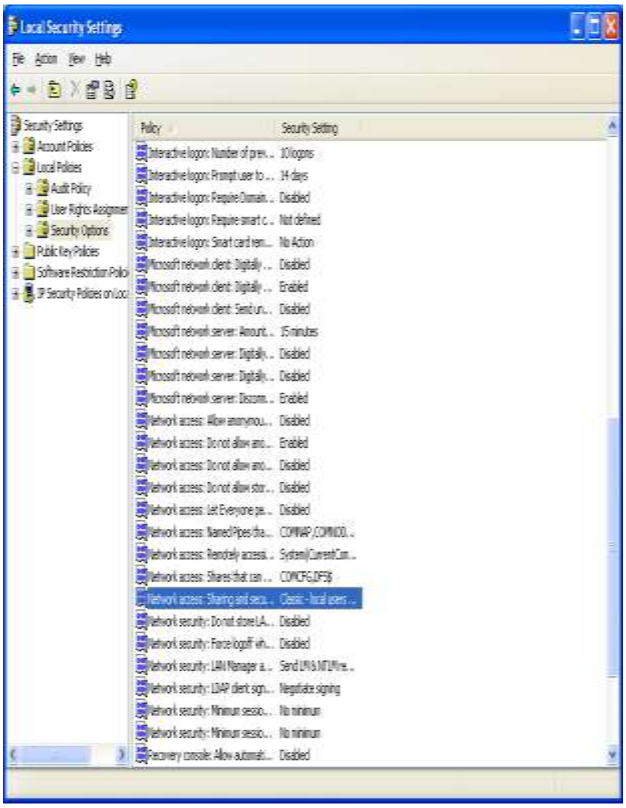
TaskList command is used for listing all the active processes running on each computer.

For the correct execution of this command it is required to disable firewall service running on the machine. After the task is complete the machine should be restored to the original state by enabling the firewall service again. The following command is used for remotely disabling the firewall temporarily on each machine.

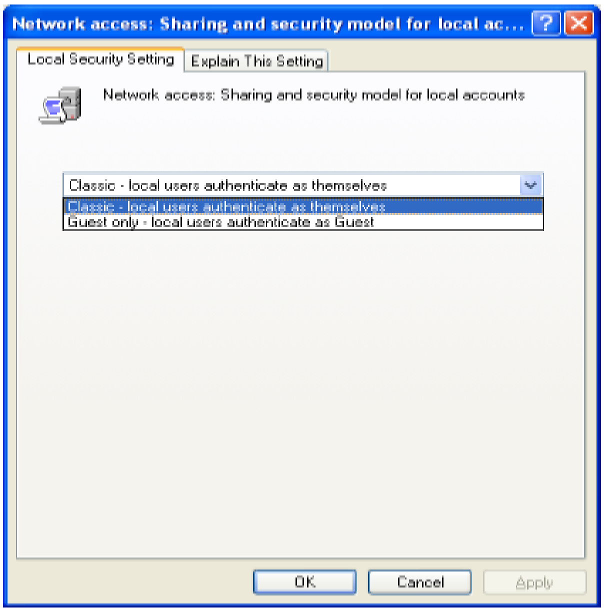
```
C:\>psexec \\dell43 -u administrator -p rebis01 cmd.exe.
Netsh firewall set opmode disable
```

The second requirement is to set the local security setting to classic (local users) for enabling the access to local users (default is for guests). This option can be accessed using Local Security Policy applet of Administrative tool in Windows Control Panel. Follow the steps shown below to set the required policy for local accounts.

1. Select Local Policies in Local Security Settings window
2. Double-click on "security options" listing in right-pane.
3. Double-click on Network Access : Sharing and Security Model for Local Accounts as shown in 4 (a) and
4. Select Classic – local users authenticate as themselves option as shown in Figure 4 (b).



Policy	Security Setting
Interactive logon: Number of prev...	10 logons
Interactive logon: Prompt user to ...	14 days
Interactive logon: Require Domain...	Disabled
Interactive logon: Require smart c...	Not defined
Interactive logon: Smart card rem...	No Action
Microsoft network client: Digitally ...	Disabled
Microsoft network client: Digitally ...	Enabled
Microsoft network client: Send un...	Disabled
Microsoft network server: Amount...	15 minutes
Microsoft network server: Digitally...	Disabled
Microsoft network server: Digitally...	Disabled
Microsoft network server: Discon...	Enabled
Network access: Allow anonymou...	Disabled
Network access: Do not allow ano...	Enabled
Network access: Do not allow ano...	Disabled
Network access: Do not allow stor...	Disabled
Network access: Let Everyone pe...	Disabled
Network access: Named Pipes tha...	COMNAP,COMNOD...
Network access: Remotely access...	System\CurrentCon...
Network access: Shares that can ...	COMCFG,DFS$
Network access: Sharing and secu...	Classic - local users ...
Network security: Do not store LA...	Disabled
Network security: Force logoff wh...	Disabled
Network security: LAN Manager a...	Send LM & NTLM re...
Network security: LDAP client sign...	Negotiate signing
Network security: Minimum sessio...	No minimum
Network security: Minimum sessio...	No minimum
Recovery console: Allow automati...	Disabled



Network access: Sharing and security model for local accounts

Classic - local users authenticate as themselves

Classic - local users authenticate as themselves
Guest only - local users authenticate as Guest

Figure 4 (a)-4 (b). Policy Setting for Local Accounts

D. To kill the illegal processes on each machine

To facilitate this the processes running on various computers of the network are compared against the information stored in machinetasks.xml configuration file and the information about the machine running illegal tasks, name of the task and Date and Time when the process is executed is documented in the database for future use.

VI. Results and Analysis

The results presented above are implemented in VB and Java with MS-Access as backend for storing machine and task information. The structure of the database employed for this purpose is shown in the following figure 5.

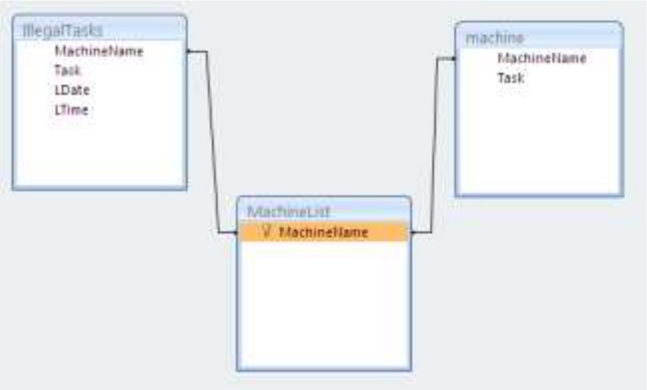


Figure 5. Structure of Database

A Graphical User Interface (GUI) presented to the end user for viewing machines in the workgroup is depicted in Figure 6. Further, the user can view the active processes and the illegal processes executing on any machine by clicking on the machine label and the machine, respectively as shown in Figure 7 a) and 7 b).

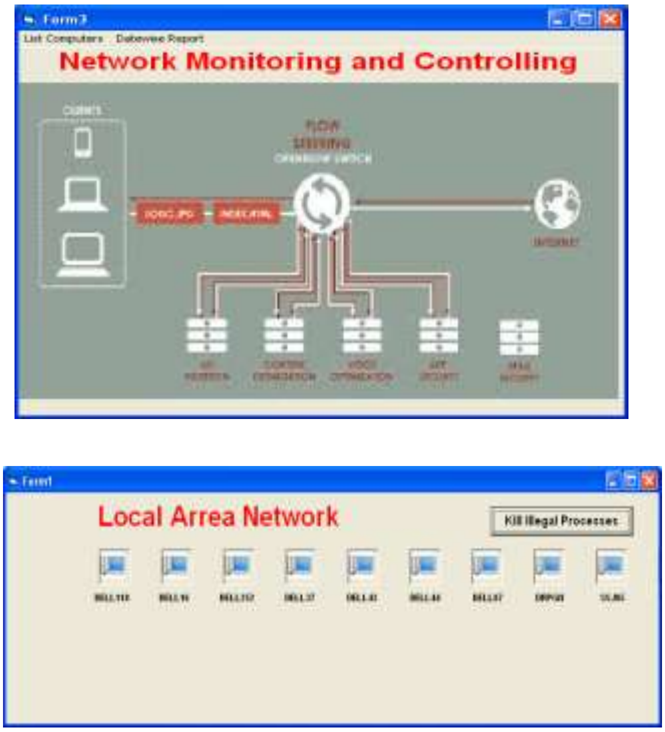
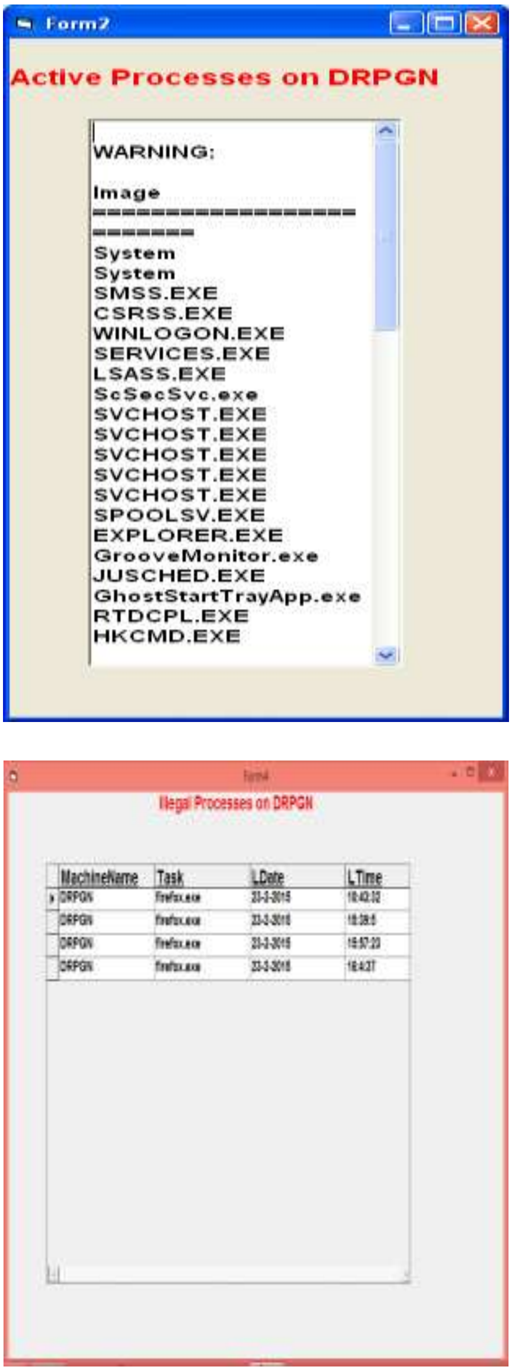


Figure 6. GUI For Network Management



```
WARNING:

Image
==================
=======
System
System
SMSS.EXE
CSRSS.EXE
WINLOGON.EXE
SERVICES.EXE
LSASS.EXE
ScSecSvc.exe
SVCHOST.EXE
SVCHOST.EXE
SVCHOST.EXE
SVCHOST.EXE
SVCHOST.EXE
SPOOLSV.EXE
EXPLORER.EXE
GrooveMonitor.exe
JUSCHED.EXE
GhostStartTrayApp.exe
RTDCPL.EXE
HKCMD.EXE
```

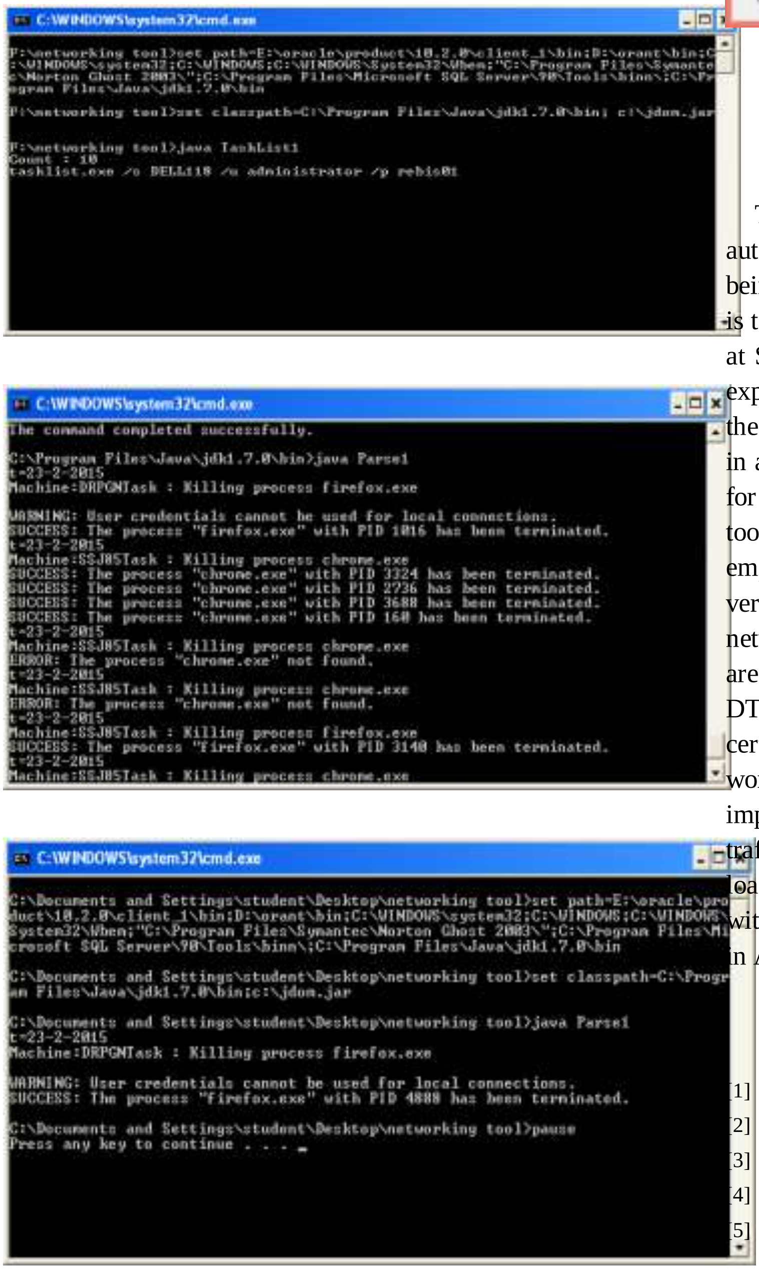
MachineName	Task	LDate	LTime
DRPGN	firefox.exe	23-3-2015	18:40:32
DRPGN	firefox.exe	23-3-2015	18:38:5
DRPGN	firefox.exe	23-3-2015	19:57:23
DRPGN	firefox.exe	23-3-2015	18:4:27

Figure 7 a) – b) List of Active Processes and Illegal Processes on a selected Machine

In future, we intend to develop the multi threaded version of the tool for improving the efficiency in case of large networks. Keeping this in mind, we have implemented the main functionality in Java and VB is used only for prototype design of GUI. To facilitate execution of Java code from within VB, we have designed two batch files, one for listing of machines in the network and the second for parsing and validating the data against that stored in an XML file. The structure of the batch files employed for this purpose are depicted in Figure 8 a) and b), respectively and the execution of the corresponding java programs in command mode are depicted in Figure 9 (a)-9(c).

run.bat	**run1.bat**
set path=%path%;C:\Program Files\Java\jdk1.7.0\bin set classpath=C:\Program Files\Java\jdk1.7.0\bin; c:\jdom.jar java ListComputers java TaskList1 pause	set path=%path%;C:\Program Files\Java\jdk1.7.0\bin set classpath=C:\Program Files\Java\jdk1.7.0\bin;c:\jdom.jar java Parse1 pause

Figure 8. Structure of Batch Files



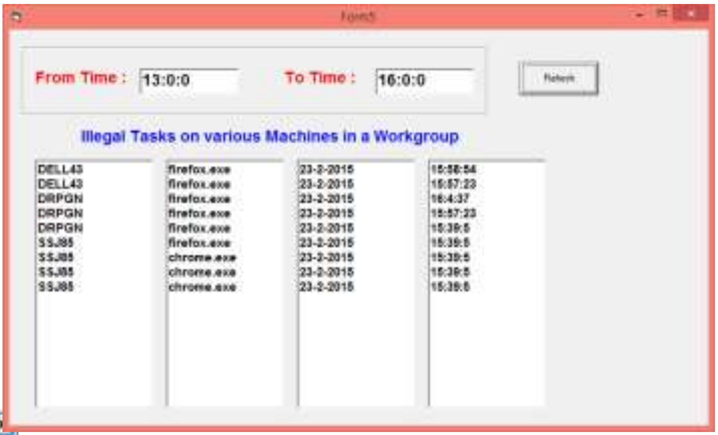
```
C:\WINDOWS\system32\cmd.exe
F:\networking tool>set path=E:\oracle\product\10.2.0\client_1\bin;D:\orant\bin;C
:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem;"C:\Program Files\Symante
c\Norton Ghost 2003\";C:\Program Files\Microsoft SQL Server\90\Tools\binn\;C:\Pr
ogram Files\Java\jdk1.7.0\bin

F:\networking tool>set classpath=C:\Program Files\Java\jdk1.7.0\bin; c:\jdom.jar

F:\networking tool>java TaskList1
Count : 10
tasklist.exe /s DELL118 /u administrator /p rebis@t
```

```
C:\WINDOWS\system32\cmd.exe
The command completed successfully.

C:\Program Files\Java\jdk1.7.0\bin>java Parse1
t=23-2-2015
Machine:DRPGNTask : Killing process firefox.exe

WARNING: User credentials cannot be used for local connections.
SUCCESS: The process "firefox.exe" with PID 1016 has been terminated.
t=23-2-2015
Machine:SSJ85Task : Killing process chrome.exe
SUCCESS: The process "chrome.exe" with PID 3324 has been terminated.
SUCCESS: The process "chrome.exe" with PID 2736 has been terminated.
SUCCESS: The process "chrome.exe" with PID 3688 has been terminated.
SUCCESS: The process "chrome.exe" with PID 160 has been terminated.
t=23-2-2015
Machine:SSJ85Task : Killing process chrome.exe
ERROR: The process "chrome.exe" not found.
t=23-2-2015
Machine:SSJ85Task : Killing process chrome.exe
ERROR: The process "chrome.exe" not found.
t=23-2-2015
Machine:SSJ85Task : Killing process firefox.exe
SUCCESS: The process "firefox.exe" with PID 3140 has been terminated.
t=23-2-2015
Machine:SSJ85Task : Killing process chrome.exe
```

```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\student\Desktop\networking tool>set path=E:\oracle\pro
duct\10.2.0\client_1\bin;D:\orant\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\
System32\Wbem;"C:\Program Files\Symantec\Norton Ghost 2003\";C:\Program Files\Mi
crosoft SQL Server\90\Tools\binn\;C:\Program Files\Java\jdk1.7.0\bin

C:\Documents and Settings\student\Desktop\networking tool>set classpath=C:\Progr
am Files\Java\jdk1.7.0\bin;c:\jdom.jar

C:\Documents and Settings\student\Desktop\networking tool>java Parse1
t=23-2-2015
Machine:DRPGNTask : Killing process firefox.exe

WARNING: User credentials cannot be used for local connections.
SUCCESS: The process "firefox.exe" with PID 4888 has been terminated.

C:\Documents and Settings\student\Desktop\networking tool>pause
Press any key to continue . . . _
```

Figure 9(a)-(c) Execution of Java Programs in Command Mode.

Figure 10 depicts the list of illegal processes executing on a selected machine in a workgroup in a given time interval.



From Time : 13:0:0 To Time : 16:0:0

Illegal Tasks on various Machines in a Workgroup

```
DELL43   firefox.exe   23-2-2015   15:58:54
DELL43   firefox.exe   23-2-2015   15:57:23
DRPGN    firefox.exe   23-2-2015   16:4:37
DRPGN    firefox.exe   23-2-2015   15:57:23
DRPGN    firefox.exe   23-2-2015   15:39:5
SSJ85    firefox.exe   23-2-2015   15:39:5
SSJ85    chrome.exe    23-2-2015   15:39:5
SSJ85    chrome.exe    23-2-2015   15:39:5
SSJ85    chrome.exe    23-2-2015   15:39:5
```

Figure 10. List of illegal tasks in a specified time period

VII. Conclusion and Future Work

The authors have developed a generic network management automation tool for continuously monitoring the illegal tasks being executed on different machines of a workgroup. The tool is tested in the computer lab of department of computer studies at SIBER, Kolhapur and is found to work satisfactorily as per expectations and within the limits of defined scope. Currently, the tool is operable only for the windows nodes in a workgroup in a medium sized network. Theoretically, the tool is operable for the network of any size but practically the efficiency of the tool gets hampered due to the single threading model employed. In future, we intend to implement multithreading version of the tool for rendering it suitable for all sized hybrid networks. Also, the XML configuration file lists tasks which are prohibited on certain machines permanently. The XML DTD can be altered to prohibit execution of certain tasks on certain machines in a specified time period only. Our future work wil focus on modification of the tool for recording important information about every network adapter, real-time traffic statistics, transmission errors, and network connection load factors. The partial code for executing the process from within Java and parsing of XML configuration file is furnished in Appendix A.

References

[1] https://seriousbit.com/netbalancer/

[2] http://www.netlimiter.com/

[3] http://www.extremenetworks.com/product/network-access-control

[4] www.infoblox.com

[5] Umesh Hodeghatta Rao, Challenges of Implementing Network Management Solution, International Journal of Distributed and Parallel Systems (IJDPS) Vol.2, No.5, September 2011,

[6] Jeonghwa Yang, W. Keith Edwards, "A Study on Network Management Tools of Householders", HomeNets 2010, September 3, 2010, New Delhi

[7] Risto Vaarandi, “Platform Independent Event Correlation Tool for Network Management”, Proceedings of the 2002 IEEE/IFIP Network Operations and Management Symposium.

[8] Jeonghwa Yang, W. Keith Edwards, David Haslem, “Eden: Supporting Home Network Management Through Interactive Visual Tools”, UIST’10 October 3-6, 2010, New York.

Appendix A

Java code for executing the process.

```
FileReader fr=new java.io.FileReader("c.txt");
BufferedReader br=new BufferedReader(fr);
String line=br.readLine();
Whiel (line != null)
{
            String line1=line.substring(2,line.length()-4);
            String line2="tasklist.exe /s "+ line1.trim() + " /u
administrator /p rebis01";
            ProcessBuilder builder = new
ProcessBuilder("cmd.exe", "/c", line2);
            builder.redirectErrorStream(true);
            Process p = builder.start();
            BufferedReader r = new BufferedReader(new
InputStreamReader(p.getInputStream()));
            line=br.readLine();
            String line3="";
             while (line3 != null)
            {
                        line3 = r.readLine();
                        if (line3 == null) { break; }
            }
}
```

Parsing of XML configuration file using JDOM Parser

```
SAXBuilder builder = new SAXBuilder();
 Document doc=builder.build("machinetasks.xml");

List children = doc.getRootElement().getChildren();
 Iterator iter=children.iterator();
 while(iter.hasNext())
  {
      Element currentItem = (Element)iter.next();
      mname1=currentItem.getAttributeValue("name");
      List tasks=currentItem.getChildren();
      Iterator iter1=tasks.iterator();
      while(iter1.hasNext())
      {
        Element task=(Element) iter1.next();
        List t=task.getChildren();
        Iterator iter2=t.iterator();
        while(iter2.hasNext())
       {
          Element deny=(Element) iter2.next();
          .
          .
       }
     }

  }
```