**Agent Based Network Surveillance System**

**Chandrashekar TR**

[24cstr@gmail.com](mailto:24cstr@gmail.com)

Computer Engineering Department, Silver oak college of Engineering & Technological Gujarat Technological University, India

**Abstract: -**

In a world which is moving forward at a great pace, Information sharing and communication with others is very vital to sustain the development of the human kind. Networking provided us a great platform for this and has since become an irreplaceable tool of communication whose need is only going to increase as we move forward. Increase in networking also means increase of burden on a network admin. So to cope with this growing burden a network admin will need all the tools which can make his work a little simpler. Agent Based Network Surveillance System is one such tool. It has been implemented using raspberry pi [7] as gateway though which we aim to provide an affordable system to small Startup Companies and home users. We are trying to provide a network admin a single application which will monitor, analyze and control network traffic exactly as he wants.

**Keywords:** Network Monitoring, Access control, Raspberry pi as gateway.

1. **Introduction**

Agent Based Network Surveillance System is a centralized application to monitor and manage networked systems using Java-based packet capturing and manipulating over LAN & WAN both. The GUI of any system is very important and so we are using JavaFX 8 with N-tier architecture for a dynamic and responsive UI. JavaFX is natively disabled in raspberry pi since Java 8 [3] but we used JavaFX Port created by gluon in this project [4]. The increasing use of communication networks has raised the demand for advanced network management. A network management system handles problems related to the reliability, efficiency, security and accountability of networked systems.

This application is concerned with monitoring, analysis, security, file sharing and control of network performance to ensure effortless network operations. Accurate and effective monitoring is vital for network management, and is the main focus of our work. The program captures all the packets moving inside and outside around the network to extract useful information from it and represent it all. This information obtained from the packets will be helpful for controlling the network with more precision. Also one can analyze and manage bandwidth utilization, keep track of all activities occurring in the network and be sure that the network performance is maintained at optimal levels. The security of the resources and data available on our network is of paramount importance. File and message transferring will also be provided through our software. This application will contain a server side and a client side program [6]. The Server program is installed on the Raspberry Pi and is operated by the network admin. It provides all the above mentioned functionalities to the network admin. The client program is installed on the all PCs in the network. The clients are differentiated on the basis of Privilege level set by the admin during account creation. The client side can also be used to monitor all the activities done by that particular client himself. The main purpose of this project is to provide a wide array of functionalities at as low a cost as possible. To make this possible we chose raspberry pi a low cost mini-PC to act as our Server agent which controls the whole network. The project also provides a network administrator all the tools needed to manage the network efficiently in one software. This makes collecting and managing the data much more easy and effective. This application hence tries to cover a lot of ground when it comes to easing the work of a network administrator and so acts as a complete solution to for most of his/her problems.

1. **Study of current system**

There are many network monitor systems today which gives a host of functionalities but not any one offer what can be considered as a complete solution. Most functionality found in these softwares are complex and hence special care has to be taken in UI to make the system understandable.

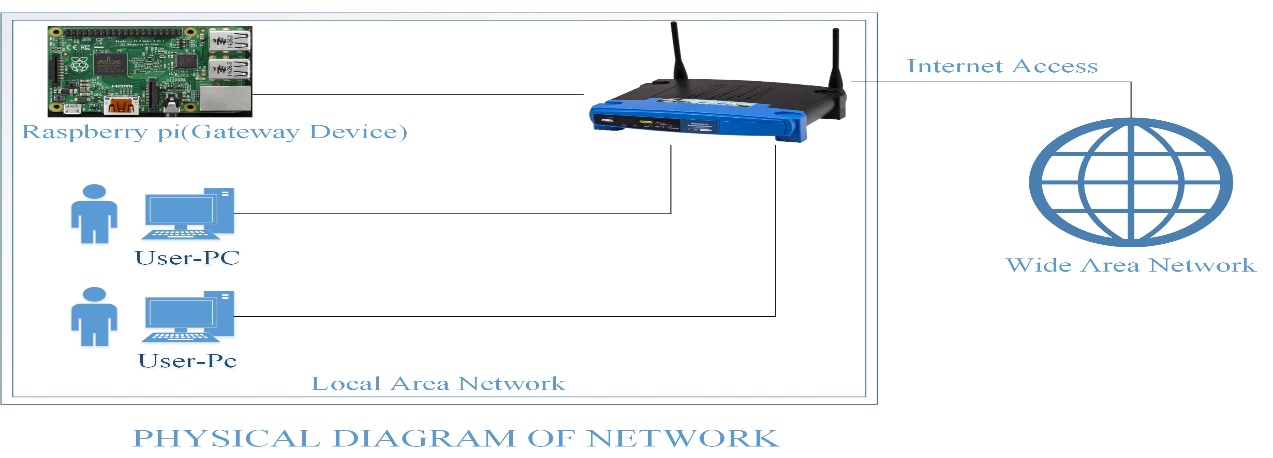
* 1. **Problems in existing systems**

1. The current systems found in the market are either too costly or don’t have even the basic required functionalities.
2. The open source softwares like wireshark have a complex and non-user friendly User interface or are very basic and don’t give more functionalities.
3. The paid software like PRTG, even though provide a lot of functionalities, are too costly to be bought by small startups.
4. The need is to find the right balance between both functionalities and cost.
5. **Network Setup Used**

In order for the program work properly it is mandatory for the network to be setup properly. The Raspberry Pi on which the server program is implemented has to be set as the gateway for all the PCs in the network so that all the packets pass through it. To enable that Feature in Raspberry pi it is mandatory to Follow a bunch of procedure [1] and that are: -

* IPV4 Forwarding Must be enabled.
* In all the Client pc the gateway must be set to the ip address of Raspberry Pi.
* Network Address Translation is must be enabled.
  1. **Physical Setup of the network**

The below image shows the physical setup of the network. This is how all the components are connected with each other.

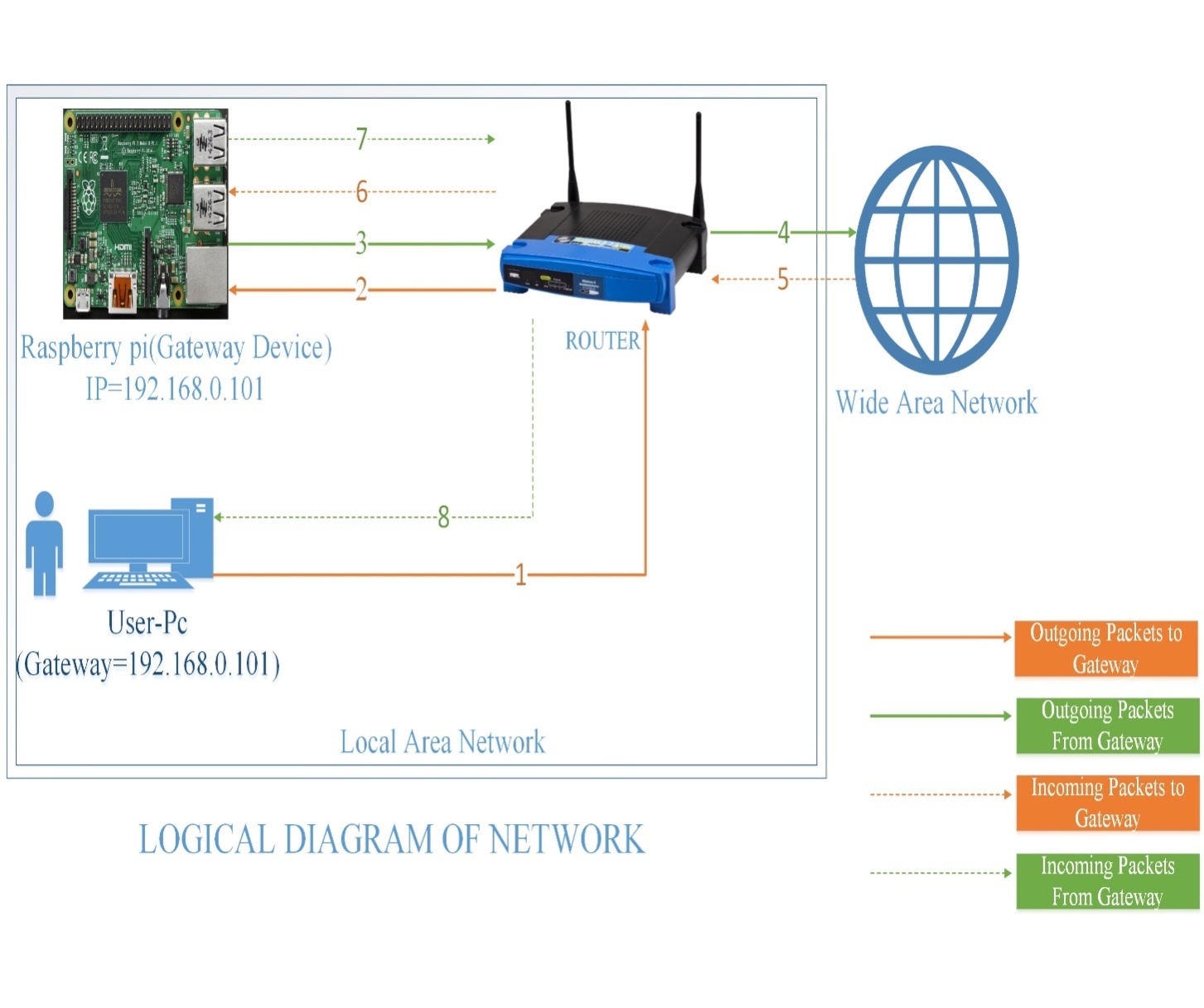


**Fig 3.1 physical setup of network**

In, fig 3.1 the user pc and the raspberry pi is connected through the router and the router is connected to the internet. Here all the clients get their internet through the raspberry pi [1]. The role of router is only to switching the packets from internetwork to wide Area network.

* 1. **Logical Setup of the network**

The below image shows how a packet travels logically in the network.



**Fig 3.2 Logical setup of network**

In, Fig 3.2 the arrow 1 shows the packet leaving from a PC to the router. The router then sends the packet to raspberry pi in 2. The Pi then check if the packet has to be forwarded or blocked and if it has to be forwarded it send it back to the router in 3. The arrow 4 indicates the packet moving from the router to the Internet service or website. In arrow 5 the incoming traffic is shown using dotted line and it arrives at the router. The router then forwards the packets to the Pi at 6 and the pi route the packets to the Pc though the router at 7 and 8 arrows.

1. **Module Wise Description**
   1. **User Login / Register**: Login module is used to check whether the user is an authorized person or not. Also the privileges allocated to that particular user can be determined from this. We also get current IP of the user while login only for file transfer or messaging. For this the user should give the correct username and password. User must have to register an account and the admin has to validate his account before using functionalities within the application.
   2. **Access Control**: Through this module we control the network access provided to a particular user. We can block any Website or Service for a particular user or privilege level or for the whole network through this module. Also we can specify an upper limit on the amount of data usage for a user of a particular privilege level. We can also block a particular user if we want so that he/she can’t use any internet services or website. We can also revert or change all the above mentioned functionalities as per our wish. There is also an option to implement any iptables rule though our project for advanced users.
   3. **Packet Monitoring**: This module is implemented using a third-party API called Jnetpcap [2] which is a java wrapper for libpcap [5]. Though this module an admin can monitor each and every packet moving around the system. This is an advanced option provided to an admin if he wants to use. The admin also can apply filter for seeing packets from a particular source or destination IP or port or for a particular protocol. Though this module a raw pcap file is also stored which can be used for deep packet inspection in other dedicated packet monitoring software’s like Wireshark.
   4. **Mail Notification**: Through this module an admin can select to get mail updates of all the ongoing activities periodically. He can add multiple email Id of different members to send them all the periodic updates. He can set the time interval between mails and also select what all the contents that has to be mailed.
   5. **File Transfer and Messaging**: Through this module the users can do file transferring and messaging inside the network among themselves. The Client can do file transfer or unicast messaging while the Server can do multicast and broadcast messages too. As the Server Side of the application will be running on a raspberry pi dedicated only for this software keeping File transfer module in the server side seemed redundant and hence it will not be available on the server side of the project.
   6. **Manage User Account**: The admin can change all the details of a client except his username and password through this module he can also upgrade the user’s privilege level or block or unblock him using this module.
   7. **Bandwidth Usage and System (Pi) Temperature Monitoring**: Through this module live updates of Bandwidth Usage and Pi’s Temperature is displayed on the home tab of the server side.
2. **Results and discussion**

Though the raspberry pi is a very capable device it can only be used for a small scale networks only without any lag. The following results were obtained when the memory was split 30-70 % between GPU and RAM

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| State of PI | RAM used(MB) | GPU memory used(MB) | Network utilization | Threads | CPU usage (%) |
| Before program starts | 150-200 | <50 | Depends on Internet Speed | 20-30 | 10 |
| When program is idle | 250-270 | =<150 | Same as Above | 50-60 | 70-75 |
| When program is in Usage | 300-350 | 150-200 | 54 Mbps | 65-80 | 76-99 |

**Table 4.1 Raspberry Pi Statistics**

In, table 4.1 it is seen that when program is in full usage the CPU usage can reach up to 99%. Hence in large Scale Systems the pi has to be used in cluster Architecture to work lag free.

1. **Conclusion**

The growth in the previous 4-5 decades is mainly due to the networks (internet) which has enabled sharing of information at never before speed and ease. This makes networks indispensable tool and a network admin a very essential person and he would require all help he gets to manage the flow of information at a desirable level. With the growing responsibilities and burden on a network admin, our project will surely play a constructive role in easing his burden and better manage his responsibilities thereby increasing the efficiency of the network and of the organization too.

1. **References**
2. <http://qcktech.blogspot.in/2012/08/raspberry-pi-as-router.html> on how to setup raspberry pi as router
3. <https://code.google.com/archive/p/iotsys/wikis/groupCommunication.wiki>
4. <http://www.rpiblog.com/2014/03/installing-oracle-jdk-8-on-raspberry-pi.html>
5. <http://docs.gluonhq.com/javafxports/#_setting_up>
6. <https://www.raspberrypi.org/forums/viewtopic.php?f=63&t=35826>
7. <http://www.developer.com/java/ent/article.php/1356891/A-PatternFramework-for-ClientServer-Programming-in-Java.htm>
8. <https://en.wikipedia.org/wiki/Raspberry_Pi>