Volume 5, Issue 2, February 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Android Based Security Spyder for MANETs

Prof. P. B. Kumbharkar[1], Suraj Kalokhe[2], Atish Tamhane[3], Lokesh Kiwale[4], Ankita Bhatkande[5]

Head of the Computer Engineering Department, Siddhant College of Engineering[1]
Department of Computer Engineering, Siddhant College of Engineering,
Savitribai Phule Pune University, Pune, Maharashtra, India

Abstract- The use of android devices in daily life has been increased tremendously in last five years. The performance of android devices made it possible in many applications. MANET is a self-configuring network of computers which allows every node to work as sender as well as receiver. So we can say that, every computer laboratory is a kind of MANET where every computer work as both sender as well as receiver. This paper proposes an android application which can be work on any android device. Using this application administrator of the network (computer laboratory) can monitor, control and manage the activities of network or workstation. We have maintained security through EAACK mechanism which is specially designed for MANETs. Compared to contemporary approaches, EAACK demonstrates higher malicious –behavior-detection rates in certain circumstances while does not greatly affect the network performance. For authentication purpose, we used RC6 (Rivest Cipher 6) and SPEKE (Simple Password Key Exchange) algorithms techniques.

Keywords- Android, Wireless media, Remote Monitoring & Controlling.

I. INTRODUCTION

In today's electronic world, we all human beings are surrounded by the computer networks. Every organizations has a small workstation or computer laboratory which is called as Local Area Network (LAN). In every LAN various activities are happen daily on client machines as well as server machines. In such a network we can access and control these activities through server. We can build a program which is run on server and then send a messages or requests to a particular machine to do changes. All these activities are maintained in the log registry on server machine. But sometimes it is hard to maintain log for long time. For making changes in the network or privileges a personal interaction with the machine is required. Nowadays, there are some applications which can be helpful to do such changes very easily. But all these require a personal computer or laptop with specific configuration and features.

In computer laboratory every computer is able to send and receive messages or requests. So, we can say that is one kind of the MANET [1]. In the era of internet services & mobile phones, email & mobile applications are widely used and it has penetrated every part of our life, but remote monitoring of networks through email and android mobile applications which are GPRS or Wi-Fi enabled is still a mirage [3]. In this application the central server is further connected to the android device through wired or wireless media. After installing this applications on the android device and server we can connect server with the android device. Then, android device becomes an administrator of the network and the computers connected to the server becomes clients [2] [3] [4]. The whole network is connected via any wired or wireless media like WIFI. Before running the application android device has to establish connection with the server through internet. After connecting to the server, whenever admin wants to interact with the network he/she has to just login to the application and can use the given features of the application as needed.

II. LITERATURE SURVEY

In the year 2013, the authors Elhadi M., Shakshuki,Nan Kang, and Tarek R. Sheltami, presented **"EAACK- a Secure Intrusion-Detection System for MANETs"** [1]**.** Using the concepts of ACK (Acknowledgement), S-ACK(Secure ACK) and MRA(Misbehaviour Report Authentication) given in this paper we have maintain security in our application. Through this paper we have implemented an intrusion detection system for our application. We can find any unauthorised user in our network. EAACK mechanism helps us to avoid the loss of data and secure delivery of the packets.

In the year 2013, the authors Prof. P.S. Dhotre, Anuradha Kadam, Pooja Satav & Vishakha Salunkhe, presented **"Mobile Based LAN Monitoring And Control"**[2], in which they mainly focus on LAN controlling by using various techniques which enables user to remotely operate some functionalities for report generation. Proposed system providing the following feature:

- Offers valuable wireless connection.
- There is no need of GSM modem in our application so it is cost affective.
- The area of covered services is more than current system.
- It requires lesser time to establish data connection than current system. The main drawback of system was it uses SQLite database for storage.

In the year 2013, the authors Prof. C. S. Nimodia, Prof. S. S. Asole, Khurana Sawant, presented **"A Survey on Network Monitoring and Administration Using Email & Android Phone"** [3]. Using the concepts of this paper we can provide the maximum details about the network to the administrator on email and android device. There can be number of protocols are used to monitor and control the network using android phone; it can be android protocol and network management protocols or combination of them. The main drawback was the includation of GSM system. Due to which the processing and hardware dependencies make system dependent. Failure in such hardware modules can lead system error prone.

In the year 2014, the authors Dhanke D.T., Bodkhe S.S., Hambarde S.M., and Vaidya R.P. presented "LAN Monitoring and Controlling Using Android" [4]. In this paper, researchers have also proposed Silent Unattended Installation Package Manager (SUIPM) that automates the process of silent unattended installations and requires the minimal possible level of interaction with the user. Silent Unattended Installation Package Manager (SUIPM) generalizes the process of silent and unattended installation. The process is fully autonomous and does not require any user interaction.

III. PROPOSED SYSTEM

Our paper proposes an android application which can be installed on any android device like mobile or tablet. Using this application we can control and access the network. We can make changes in the network, permissions required to access application. That means we can access central sever which is responsible for all the activities on the network. For security purpose we can give username and password to a single administrator. For secure data transmission between client and server a s well as android device we have introduces security mechanism named EAACK which helps in detection of an unauthorized user of intrusion[1]. Our application have a facility to set number of administrators for LAN monitoring. So, if it is only one, then it can be accessible to a single administrator. If we try it for more, then one network will not allow.

A. System Architecture

The application is designed with a GUI which provides administrator a list of features. Administrator has to select the option for the desired action. When he/she selects the option a request is sent to the server. The particular client machine is recognized by the server for action like shut down process, shut down or kill process, create, delete, modify file. The feature which is selected by the admin on phone, a HTTP request is sent from the phone in URL form and received by the server. This same HTTP request is read and encoded and sent further to the client. The client reads this URL message and extracts the command name and other required parameters. The command is executed on the particular machine to which the server sent the URL to. The URL from phone contains the IP address of central server and its port number. Using the internet service provider or WIFI the communication between android device and server and server communicates with the clients though LAN. So, administrator can control the LAN using his/her android device even he/she is at remote location. The administrator also checks the load on the LAN. If server fails in this model then Client can communicate to admin through mobile phones [2].

B. System Workflow

Whenever the application is opened, the administrator is asked for username and password. If he/she entered a valid one then it proceed further. If there are more than eight or ten attempts then he/she has to authenticate from the network. After the successful login user can control LAN network using menu driven commands. A drop-down menu is shown which contains the list of features [2] [3].

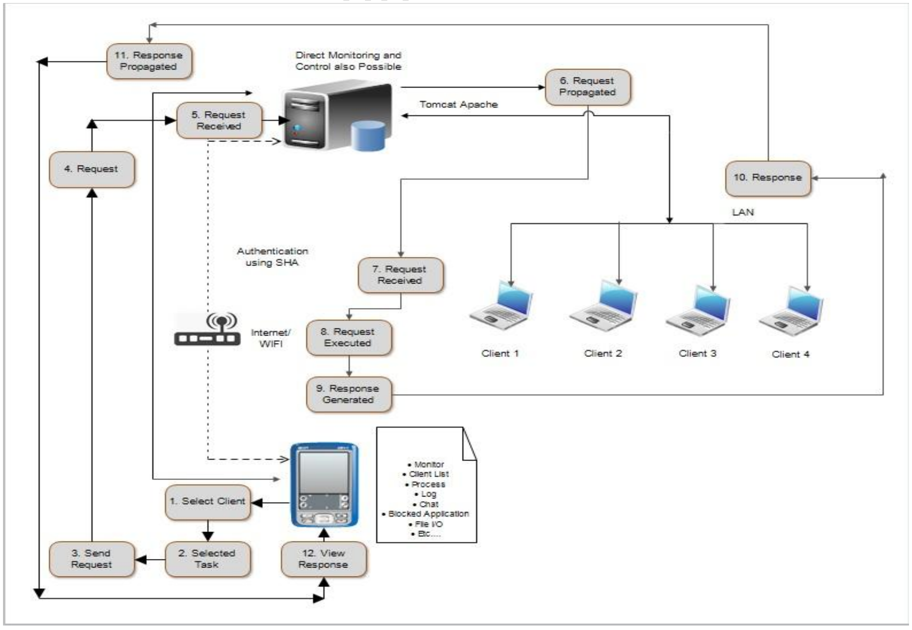

Fig. 1. System Architecture

Let us consider a silent software installation function. In this client wants any software from the server then he/she sends request to the administrator. Then admin will check for that requested software and allows server to send and install that software. Then server will send that software setup file to the respective client and installation can be began.

If administrator notices that any user or client is doing unauthorized access to the network then he/she can to shut down that client's machine by shut down command. After receiving that command from administrator the client machine will be automatically get turn off. The system can do following tasks on request:

- On/off
- Process monitoring & controlling
- Desktop on, off, shut down
- Opening Browser with specific URL
- Files transfer
- Silent software installation
- Blocking a specific URL
- Blocking user
- Grant privileges

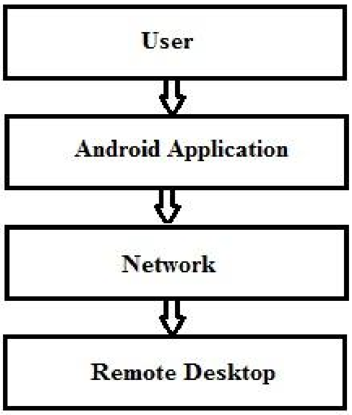

Fig.2 System Workflow

C. Security

As we mentioned above, we used an existing algorithms RC6 (Rivest Cipher 6) and SPEKE (Simple Password Key Exchange) for the authentication purpose. EAACK mechanism is used for the intrusion detection and secure transmission of data between administrator (android device) and server.

IV. ADVANTAGES

1. Low or no start-up cost.
2. No GSM module used so hardware dependency is not required.
3. Great flexibility in relation to fast up and down scaling of resource needs.
4. Easier access to new versions.
5. Encryption methodology for fast and secure communication.
6. Other common outsourcing advantages like security for uptime, availability, reliability, scalability, Contingency arrangements, reduced costs of investment in organization's infrastructure.

V. CONCLUSION AND FUTURE SCOPE

The LAN Monitoring Software will be able to identify different clients connected in a net- work and will be able to monitor them through a mobile phone irrespective of distance. This will reduce the workload on network administrator to great extent. This project makes it possible to support even the personal smart phones, laptops in the vicinity of LAN in use. Concurrent working on the same process, but one on the machine and the other through the android cell phone we are using. This paper contributes for IT Administrators to remotely control any computer present in the network, allowing them to remotely troubleshoot and solve problems faster. It can help the colleges to monitor the labs, to restrict the use of forbidden sites or applications. The application also helps one to monitor his own PC when he/she is away the workstation. We can conclude that android based is efficient and reliable from previously developed systems. In future, we can develop same application for the different operating systems like windows, mac, java, Symbian, blackberry, etc. We can also increase the capacity of the application to handle Wide Area Network.

REFERENCES

[1] Elhadi M. Shakshuki,Nan Kang, and Tarek R. Sheltami, EAACK- *A Secure Intrusion-Detection System for MANETs.* IEEE transactions on Industrial Electronics, vol. 60, no. 3, March 2013.

[2] P.S. Dhotre, A. Kadam, P. Satav & V. Salunkhe, *Mobile Based LAN Monitoring and Controlling*. International Conference on Computer Science& Engineering (ICCSE), 17th March-2013, Pune.

[3] C. S. Nimodia, S. S. Asole, *A survey on Network monitoring and administration using email and android phone*. International Journal of Emerging Technology and Advanced Engi- neering Volume 3, Issue 4, April 2013.

[4] D.T. Dhanke, S.S.Bodkhe, S.M. Hambarde, R.P. Vaidya, *LAN Monitoring and Controlling using Android*. International Journal of Ad- vanced Research in Computer Engineering & Technology (IJARCET) Vol- ume 3 Issue 3, March 2014.

[5] R. Bhardwaj, S. S. Jangam, P. N. Shinde, A. B.Raut, R. S. Trigune, *LAN Monitoring Using Android Phone.* In- ternational Journal of Innovative Research in Computer and Communication Engineering Vol. 2, Issue 2, February 2014.

[6] S. C. Sivakumar, William Robertson, Maen Artimy and Nauman Aslam, *a Web-Based Remote Interactive Laboratory for Internetworking Education*. IEEE transactions on education, vol. 48, no. 4, november 2005.

[7] R. Akbani, T. Korkmaz, and G. V. S. Raju, “Mobile Ad hoc Network Security,” in *Lecture Notes in Electrical Engineering*, vol. 127. New York: Springer-Verlag, 2012, pp. 659–666.