



## Data Consistency and Time Competence of System for Controlling Intranet through Mobile Device Using Cellular Networks

Anand Khatri\*, Prof. Ranjana Badre

Computer Engineering Department  
University of Pune, India

---

**Abstract** — Many companies/organizations are trying to move towards automation and provide their workers with the internet facility on their mobile in order to carry out their routine tasks to save time and resources. The system is based on GPRS technology aims to provide a solution to problem faced in carryout routine tasks considering mobility. In the world of increasing mobility, mobile service is one of the emerging services due to the explosive increase in the number of mobility device and control the status of the PC. With this system, a network administrator or user will have an effective remote control over the intranet network. Data reliability and security required for the data transfer over network media. However, available cellular networks with protocols like 3G, GPRS, EDGE or UMTS are highly unreliable due to frequent connection interruptions and high bandwidth variations for data traffic. System improved data reliability and transmission done fast over available cellular networks.

**Keywords**— Remote Administration, GPRS (General Packet Radio Service), 3G, block cipher (AES algorithm), stream cipher (RC4 algorithm)

---

### I. INTRODUCTION

Wireless communication is one of the biggest research areas among recent technologies providing various facilities to consumers of mobile and small computing devices made them to expect high performance from mobile devices. They demand quick response time, compatibility with companion services and full-featured applications in a small device. Consumers expect the same software and capabilities found on their desktop and laptop computers to be available on their cell phones and personal digital assistants. To meet these expectations, developers have to rethink the way they build a mobile device and need to harness the power of existing front-end and back-end software found on business computers and transfer this power onto small, mobile and wireless computing devices.

Today there is need of monitoring the network remotely because, it has been observed that most of the employee in an organization or students in institutes having access to the computer are goofing off on the internet or playing games etc. reducing productivity and the overall development. Thus it has become essential to monitor the remote machines in LAN so that the company or institutes can redirect the work force and get the best out of the institute members. This requires the organization to keep a track of the user activities in remote machine so as to get full benefit of their talent and time. If we see today's LAN controlling and monitoring system, administrator has to sit in front of his/her server in the premises of their organization and see the activities performed by users. Suppose administrator wants to go somewhere at this time, he cannot force all clients to shut down the systems, hence there is a need for control and monitor all clients even though administrator is physically not present at server. At most administrator stores all information about activities done by clients when he is not present at server and see clients work afterwards.

Our system helps administrator who will receive data remotely from different locations in network, like some textual information about current work of clients, accounting information of each clients depending on requests of administrator and accordingly take action to control client work and to provide maximum details about the network through a mobile device remotely by managing computer network through mobile by functioning as the eyes and ears of the network. The system is designed for mainly monitoring and controlling the Intranet or Local Area Network only from the place where it is installed or from where the network node extends and exists from a remote location using mobile device enabled with GPRS.

### II. RELETED WORK

Mobile communications are rapidly becoming more and more necessary for everyday activities. With so many more users to accommodate, more efficient use of bandwidth is a priority among cellular phone system operators. Mobile banking is one of the emerging services in telecommunications due to the explosive increase in the number of mobile customers around the world. Solutions for mobile banking are varied, ranging from the use of Wireless Transport Layer Security, Security Socket Layer, or application-layer based options [1]. In real time health monitoring system, the performance of several cryptographic protocols for different data sizes applied on the system in different network condition and a security protocol adoption scheme allowing to automatically to change the encryption algorithm to use, depending on the size of the input data and some other network parameters. Don't have one security protocol which suits all conditions [3][4][5].

The motivation behind design the system is to facilitate the user to automate their homes with a low cost system. Data Transfer Over GPRS: Palm OS., Transfer of files from a device to a pc (server) can be done in different way: like HTTP, FTP and TCP/IP. In these entire cases one thing that remains same is the channel that is the “Cellular Network”. Things are bit different while sending data files across to the server, when we are using the cellular network. Software architecture should be considered very important when designing application depending on the GPRS. Growth in the cellular telephony has increased demand for the wireless data services. There are many standards like 3G (3<sup>rd</sup> generation) UMTS (universal Mobile Telecommunications System) mobile networks but these are still away from the wide-scale development. In the meantime, the extension of GPRS (General Packet Radio Services) to current 2G GSM networks provides a widely deployed solution for data access. In the wired internet TCP is the dominant protocol and is very important for the mobile users too.

“Implementation of Telecontrol Applications over GPRS Networks”, depicts how GPRS technology has reached sufficient levels of development and reliability. GPRS can be applied in technological applications, either as a backup for private communications channels or as a main communications technology. It also tells how GPRS Applications work over network.

### III. OVERVIEW OF SYSTEM

The system provides the facility to remotely monitor and control of all the nodes of an intranet using mobile device through GPRS/3G. With this system a network administrator will have effective remote control over the network connection framework which makes use of J2ME, sockets and RMI technologies and security for the messages and energy required for the transferring data. Authentication of users for the system is ensured by initial authentication which verifies the user is intended one. When the administrator starts the application, username, password and IP address are to be entered by him/her which is required for logging into the system and further activities as required will get start functioning. Some of the services provided are reading, executing and killing services, chat, broadcast, compile, word pad, broadcast client and shut down etc. and provide maximum details about the network through a mobile device remotely.

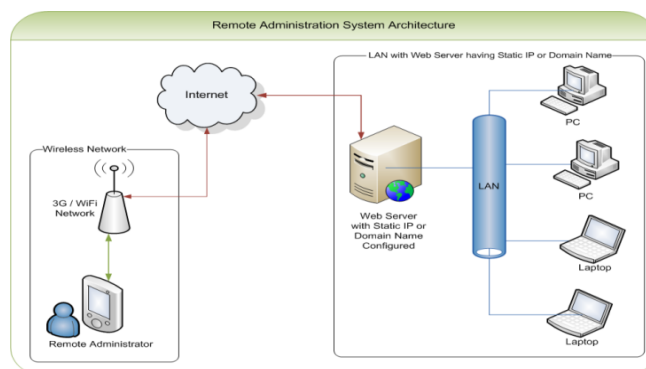


Fig. 1 Frame work

The frame work of system model given in fig. 1 is as follows: The system protocol provides the facility to remotely monitor and control of all the nodes of an intranet using mobile device through GPRS/3G. With this system a network administrator will have effective remote control over the network connection framework which makes use of J2ME, sockets and RMI technologies and security for the messages and energy required for the transferring data. Authentication of users for the system is ensured by initial authentication. When the administrator starts the application, username, password and IP address are to be entered by him/her.

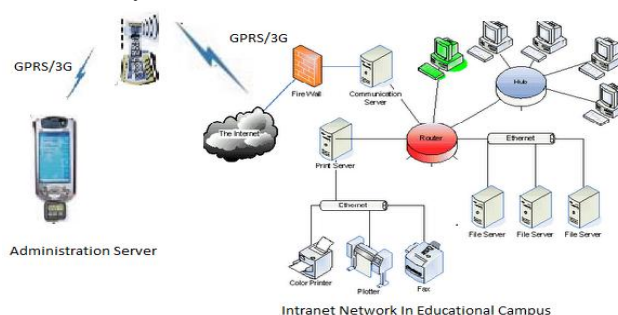


Fig. 2 Architecture of System Model

Android mobile device or PDA plays the role of as an Administrator Server and control all the activities of the intranet network remotely. Here we have system to monitor process of the node such as start, reading, executing, kill the process services. Our system is implemented by developing application for a mobile device using J2ME, designing the interface between a mobile device and sever using connection framework, GPRS/3G/WI-FI and Tomcat Web server, establishing

connection between a mobile device and clients on the intranet using RMI and Sockets server. The architecture of model is as illustrated in fig. 2.

#### IV. EXPERIMENTAL DESIGN

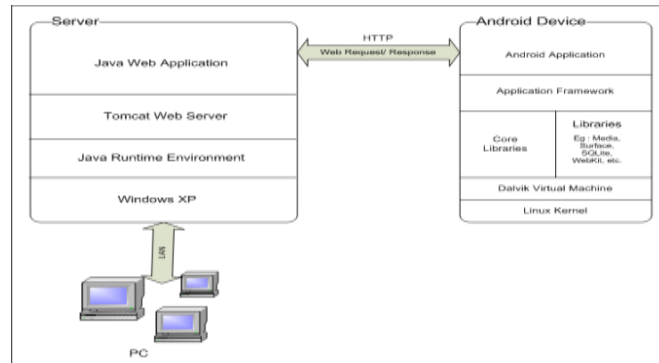


Fig. 3 Implementation details

As shown in fig. 3 shows the implementation as follows,

1. Using Android device through web request (HTTP protocol) get connected to Server.
2. Get Authenticate and get list of PC's in N/W on Device.
3. Execute/Run/Stop Services / processes remotely Using Mobile.

To start with administrator has to do the initial authentication by filling the information through secure web access. Once the initial authentication done, administrator start the application in the MID, Welcome screen display on his MID for few second and then login screen appears on the MID as shown in fig. 4.

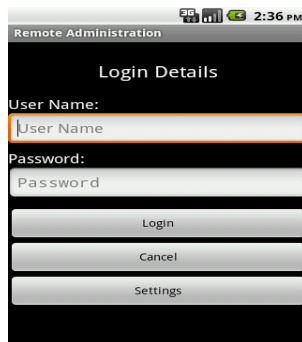


Fig.4 Login Screen

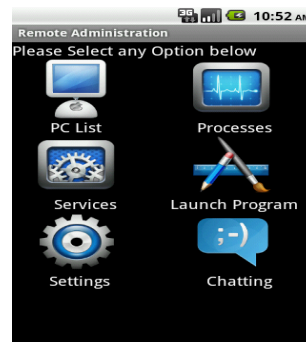


Fig.5 Menu list On MID

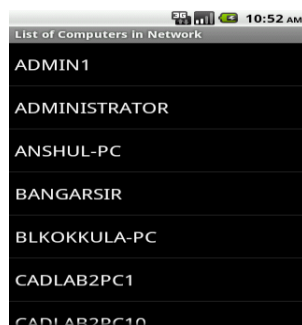


Fig. 6 Running Nodes in the Network



Fig. 7 List Of Processes

Firstly in setting option set the IP address of server where application of remote administrator is present. After giving user-id and password, an administrator gets connected to the server which is present in the network as “Administrator server”.

After logged to the server, menu list appears on the MID screen is as shown in fig 5.

All the nodes which are running are displayed on MID as shown in fig. 6 when administrator click on the “1 Nodes in network”.

When administrator selects the ANSHUL-PC, should get list of processes running on that node and accordingly he/she can start, execute or kill the process. Similarly other service functionalities like chat, broadcast, client messaging,

compile and shutdown will be provided. The communication between the device and the server of such a system needs to encrypt/decrypt the data all the time for protecting user privacy.

## V. SECURITY

In our system, we used block cipher (AES) algorithm and stream cipher (RC4) algorithm. Based on the analysis and result, we will conclude that comparison technique used in RC4 algorithm is better to use based on different performance metrics.

1. Block cipher (AES 128 bit) used in at the time of authentication, while connecting to server and client in intranet network.
2. Stream cipher (RC4 256 bit) used while transmission of data from node machine to mobile and mobile to node machine.

In this work, for stream cipher we used compression/decompression technique before encryption and after decryption of data. The fig. 8 shows how we included new technique.

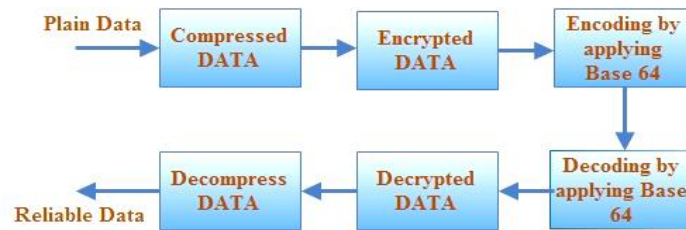


Fig. 8 Flow of data in system over cellular network

Stream cipher Encryption Algorithm

Encryption Technique:

- Step 1: Firstly receiving data from source is compressed.
- Step 2: Get the compressed data to be encrypted
- Step 3: Provide key for data encryption
- Step 4: Convert the key into byte array
- Step 5: Copy the bit into key result (using binary AND operator)
- Step 6: Apply the byte swapping on key bytes
- Step 7: Convert Data into byte array
- Step 8: Copy the bit into data result (using binary AND operator)
- Step 9: Apply the byte swapping on Data bytes
- Step 10: XOR the final key stream with the data to be encrypted to give cipher text.

After getting cipher text, encoding it by applying Base-64 and then transmit data over internet. Data reached to destination, administrator got reliable data on smart phone by applying decryption technique.

```

// encrypt
public String encrypt(String text) {

String encText = "";
String key = "@A1n2a3n4d_:K0h9a8t7r6i@";

byte[] dataByte = null;
dataByte = compress(text.getBytes());
byte[] dataOut = new byte[dataByte.length];

StreamEncryptor engine = new StreamEncryptor();
KeyParameter keyParameter = new KeyParameter(key.getBytes());
engine.init(true, keyParameter);
engine.processBytes(dataByte, 0, dataByte.length, dataOut, 0);

encText = new String(Base64.encodeBase64(dataOut));
return encText;
}
  
```

First, apply Base64 technique to decode data arrived at destination.

Decryption Technique:

- Step 1: Get the encrypted data to decrypt
- Step 2: Convert the Data into byte array
- Step 3: Provide key for data decryption
- Step 4: Convert the key into byte array.
- Step 5: Copy the bit into key result (using binary AND operator)
- Step 6: Apply the byte swapping on key bytes.
- Step 7: Convert Data into byte array
- Step 8: Copy the bit into data result (using binary AND operator)
- Step 9: Apply the byte swapping on Data bytes
- Step 10: XOR the key stream & data stream to get original compressed data
- Step 11: decompress the data get plain text.

// decrypt

```
public String decrypt(String ciphertext) {
String decText = "";
String key = "@A1n2a3n4d_:K0h9a8t7r6i@";

byte[] dataByte = Base64.decodeBase64(ciphertext.getBytes());

byte[] dataDec = new byte[dataByte.length];

StreamEncryptor engine = new StreamEncryptor();
KeyParameter keyParameter = new KeyParameter(key.getBytes());

engine.init(false, keyParameter);
engine.processBytes(dataByte, 0, dataByte.length, dataDec, 0);
decText = new String(decompress(dataDec));

return decText;
}
```

## VI. APPLICATIONS

Wireless communication is one of the fastest growing research areas where handheld devices such as a mobile phone, require certain applications and services for efficient utilization of the device. Since mobile phones, as the name indicates are mobile in nature, services related to monitoring and remote controlling of local area network will be more useful. Some of the applications where our system can be used are described as below. Personal area networks (PAN): It is useful in controlling all nodes which are present in the personal area network, which gives mobility to the owner of the network administrator due to our system and also gives the security to intranet network in PAN.

Military operation: In the military operations, it is obvious that the data sensed or disseminated is of a private nature and is required to remain the same. Enemy tracking and targeting are among the most useful applications of wireless or networks in military. Agriculture field: In agriculture, it is useful for getting information about the temperature, humidity and plant condition so as to get better crops in the field.

## VII. TEST RESULT OF SYSTEM

The test result for sending request of some data in Bytes to the single node in the intranet from mobile across the internet through media WI-FI and 3G are as follows:

Test case: Consider Intranet Local Area Network from one of the Lab of Computer Engineering Department in which one server machine with internet connection and almost 19 machines in the Intranet Local Area Network. Out of these machine we consider four machine for analysis of data from which "Administrator" machine are two years old and having number of application software installed on it, "Admin1" having less application compared to "Administrator", "Anshul-PC" is a server machine which contains many system software and application software as well as security software installed on it and "CADLAB2PC1" is only new machine installed only operating system.

System is tested is as follows:

1. Firstly, tested without compression of data using stream cipher algorithm.
2. Secondly, tested with compression of data using stream cipher algorithm.

Table 1 shows that Data analysis with and without compression.

TABLE I  
DATA VS COMPRESSED DATA  
( USING STREAM CIPHER SECURITY ALGORITHM( NEW COMPRESSION TECHNIQUE) )

	Administrator (byte)	Admin1 (byte)	Anshul-PC(byte)	CADLAB2PC1(byte)
Processes(wc)	9113.6	8840	12800	4320
Processes(c)	1740.8	1443.7	1842	780
Service(wc)	28058	22378	38576	17560
Service(c)	4505.6	3890	6540	2332
Launch(wc)	9	8	9	8
Launch(c)	68	56	54	58

(wc - without compression , c-compression)

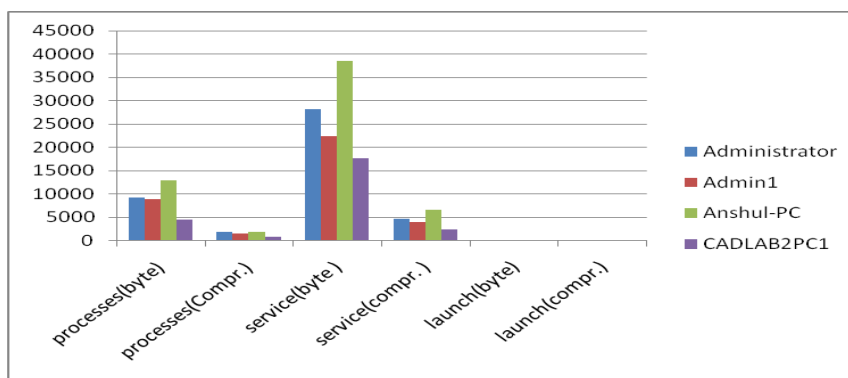


Fig. 9 Data Vs Compressed data (before and after using compression technique)

TABLE II  
TIME IN MILLISECOND FOR DATA TRANSMIT USING 3G AND WI-FI

	Administrator (ms)	Admin 1 (ms)	Anshul-PC (ms)	CADLAB2PC1 (ms)
processes(wifi-wc)	6110	5670	8750	2230
processes(wifi-c)	2450	1890	2531	1230
processes(3G-wc)	10220	9800	14530	5680
processes(3G-c)	2600	2100	2876	1300
service(wifi-wc)	15340	13250	21300	11230
service(wifi-c)	5600	4352	7654	2890
service(3G-wc)	23450	18760	29050	13758
service(3G-c)	9876	6754	10398	5489
launch(wifi-wc)	94	92	93	92
launch(wifi-c)	112	97	90	102
launch(3G-wc)	756	730	743	725
launch(3G-c)	889	804	712	826

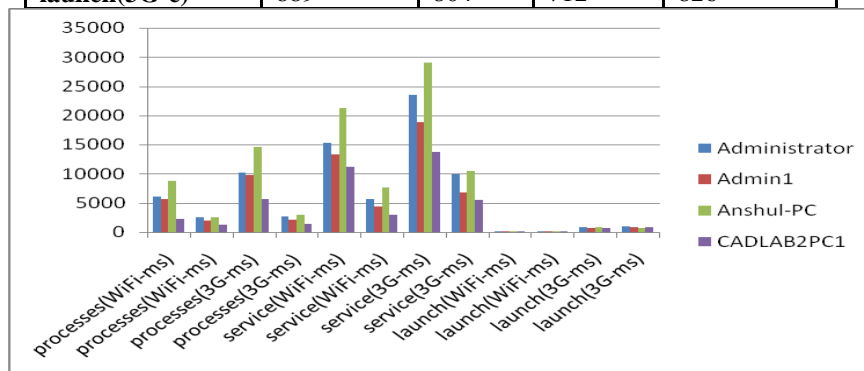


Fig. 10 Time in Millisecond ( without compressing of data/with compressing data )

### VIII. CONCLUSION

Monitoring and Controlling is an important aspect of any network. Lots of monitoring or controlling tools are available and to operate them, administrator has to sit in front of his server and do the monitoring and controlling, but still have to face challenges in developing software which will monitor, schedule the jobs, as well as control the computer network from any location in local area network or intranet. Initially, it was very difficult for administrator to control client activities remotely however our work enable the administrator not only to monitor the network remotely but also control various activities of particular user and also serve the various requirements of the administrator. The main objective of this work is to provide maximum details about the network to the administrator on their mobile phone, when he/she is away from office / goes out station and to control and monitor the local area network from mobile phone. Using our system data transmission up to 40% fast after using new compression technique stream cipher algorithm.

### REFERENCES

- [1] Maria-Dolores Cano, Gines Domenech-Asensi- 'A secure energy-efficient m-banking application for mobile devices', The Journal of Systems and Software, G Model JSS-8740; No. of Pages 11.
- [2] Shashi Kumar N.R. 2 R. Selvarani 3Pushpavathi T.P, 'GPRS Based Intranet Remote Administration GIRA', JRI- Journal of Research & Industry Volume 1 Issue 1 December 2008.
- [3] Huafeng Wu, Chaojian Shi, Bingjie Zhao, Seiya Miyazaki , 'A Security Protocol Adaption Scheme for Health Monitoring System ',Supported by Innovation Program of Shanghai Municipal Education Commission (09YZ247), Shanghai Leading Academic Discipline Project (S30602) and China postdoctoral science foundation general program for top grade (20090450077)
- [4] Alexander Schacht, Robert Wierschke, Martin Wolf, Martin von Lowis and Andreas Polze, 'A Live Streaming of Medical Data- The Fontane Architecture for Remote Patient Monitoring and its Experimental Evaluation', 2011 14th IEEE International Symposium on Object / Component/Service-Oriented Real-Time Distributed Computing Workshops.
- [5] D. Boyle, T.Newe, 'Security protocols for use with Wireless Sensor networks', Conference on Wireless and mobile Communications (ICWMC'07), 2007 IEEE.