Study of mobility issues and different types of attacks on Smartphone.

Tejas amrut patil, Shraddha Subhash gujar
ASM's IMCOST, Mumbai University
C-4, Wagle Industrial Estate, Near Mulund (w)
Check Naka, Thane (w)-400604

Abstract:
India is the developing nation of the 21st century and is developing in several sectors, especially, the secondary and the tertiary sector. India, as a developing economy heavily relies in its network connectivity. However, several issues are encountered in its connectivity, one of which is the high cost of broadband and other network infrastructure. Roaming network is one of the grave (serious) issues network consumer face in India. To resolve this issue India provides best broadband infrastructure of the network which is affordable and convenient for out coming sources. The smart phone is one of the most widely used platforms by business and users. This paper describes the functional requirements of mobility issues in wireless networking. Hence, one can say that India does have connectivity issues. This research study aims to explore the types of attacks in smart phones.

Keywords:
bandwidth, Quality of service (QoS), internetworking, mobility, signaling, Internet, Telecommunication, Threats.

I. INTRODUCTION

The first generation analog cellular system used large cells and multi directional antennas in the 800MHz band. First generation analog cellular systems were followed by second-generation, digital cellular system. Digital wireless technologies supports a much larger number of mobile subscribes within a given frequency allocation. Quality and lay the foundation for the value added services that will continue to be developed and enhanced in future. The network operator recognize that future revenue stream in competitive and mature markets will not be generated solely from providing voice connections, but also more sophisticated services. The existing digital wireless standards continue to be developed as related to value-added services, capacity, coverage, cost and bandwidth. Therefore, one of that it provides a seamless path of migration from present day digital wireless networks that it be capable of inter-working. A smart phone is a device with an advanced mobile operating system. Smartphone's typically combining the features of a cell phone with other popular mobile devices, such as personal digital assistant (PDA), media player. Smartphone provides digital voice services as well as any combination of email text messaging, voice recognition. Smartphone were introduced by IBM and Bellsouth in 1994 under the name "Simon". These Smartphone were very heavy and costly Smartphone use mostly used cellular networks like GSM, GPRS and 3GP. Smartphone have powerful capabilities. There are different sources of attacks on Smartphone which include internet, PC to Smartphone data transfer and attacks during wireless connection to other devices, Infrared, Bluetooth etc.

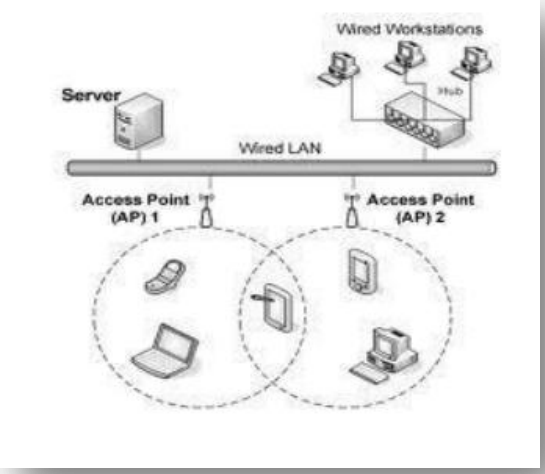

Fig 1 : Infrastructure Of Mobile Networks.

II. MOBILE DATA ISSUE

User face differing mobile data issues depending upon location, connection quality and reliability have a higher tendency to occur indoors, while session failures and poor app accessibility are problems faced by outdoor Smartphone users. 63% of users report that they are face quality and reliability issues, such a lost connection and inconsistent network speeds, when using mobile

networks indoors. Application related issues, such lengthy lag times, app taking a long time to refresh, map failing to load, and session failure affects 68% of consumers. Such problems are more common in mid-size and small towns compared to large cities. For all consumers in India who do not used mobile broadband, affordability and digital literacy are the main obstacles to adoption. 88% of Indian consumers on 2g feel that mobile broadband is too expensive. 53% feels that mobile broadband adds no values and as many as 48% believes that there is no difference between the 2G &3G speeds. Mobile internet uses is expected to grow with the consumer's better understanding of that plans on offers. As per the study they understand there plane perfectly, and are able to make an accurate judgment when deciding on plan.

III. FUNCTIONAL REQUIREMENTS

A. *Very high speed and high quality transmission*

Future mobile communication system should be able to handle a large volume of multimedia information a fill song or sending a complete data file or several video clips. This would be possible by various means like transmitting data at 50-100 mbps , having an asymmetric data speeds in up an a down links , having continuous coverage over a large geographical are, applying a quality of service (Qos) mechanism at low, affordable and reasonable operating costs etc. Flexible and varied service functions: future mobile communication networks should be "seamless" with regards to media that means whether it is wireless or optical fiber or satellite or wire lines , with regards' to corresponding hosts or service provider as well as other connectivity with other networks are like GSM and CDMA or other telecom network.

B. Open platform

Future mobile communication system should be "open" regarding to mobile terminal platform, service nodes, and mobile network mechanism. Which means that users can freely select the protocol, application and networks?

C. System perspective

Now, let us see how the future mobile communication system can be realized. Advanced cellular system and high speed access system will be functionality integrated into the future mobile communication system.

D. Spectrum requirement:

So far we have to discuss that future mobile system should be able to provides enhanced data transmission capabilities. This estimates of additional spectrum is based on

- Enhanced service requirements.
- Introduction of ultra high-speed multimedia i.e. downlink 100mbps , uplinks 30mbps
- Rate of increase in traffic at least to be @50% per year.

At presents 3G mobile system like GSM cellular are operating in the frequency band of 900 MHz or 1.8 GHz, and CDMA based cellular system are operating at 1.9 GHz.

IV. MOBILITY

Without the limitations proposed by the wired connections between devices, all devices in a wireless network are free to move. To support mobility, a going connection should be kept alive as a user roams around. In an infrastructure network, a handoff occurs when a mobile host moves from the coverage of a base station or access points to that of another one. A protocol is there for required to ensure seamless transition during a handoff. This includes deciding when a handoff should occur and how data is routed during the handoff process.

V. SIGNAL FADING

Unlike wired media, signals transmitted over a wireless medium may be distorted because they are propagated over an open, unprotected, and ever changing medium with irregular boundary. Beside the same signals may disperse and travels on different path due to reflection, diffraction and scattering caused by obstacles before it arrives at the receiver. The dispersed and travels on different times to reach destination. This unreliable nature of the wireless medium causes a substantial number of packets losses.

A. Seamless Mobility

There is powerful trends towards seamless mobility in the cellular world, where mobile professionals today and eventually all consumers in the future would like to communication and be able to do their routines business anytime's, anywhere. As a result, there is real demand for ubiquitous connectivity between a wide variety of mobile

devices and access technologies, which includes wireless wide-area networks (WWANs) and wireless local-area networks (WLANs). Roaming and communication among these technologies are therefore "must-haves" for seamless mobility to occur. The new generation of wireless networks is intended to provide accessing information anywhere, anytime with a seamless connection to a wide range of information and services and receiving a large volume of information and images, videos, and so on. The future network using IP as a common protocol so that users are in control to choose every application and environment.

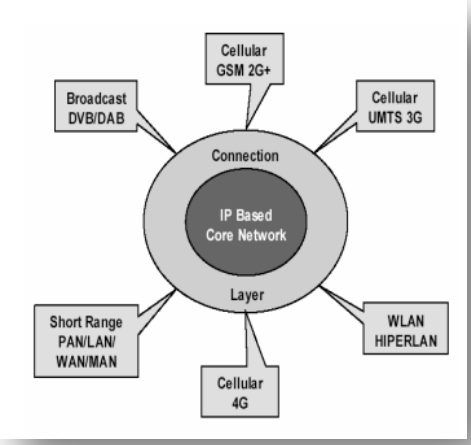

Fig 2 : Seamless Connectivity Of Communication Networks

VI. SEAMLESS CONNECTION ISSUES

Next generation wireless networks will have broader bandwidth, higher data rates, and smoother and quicker handoff and will focus on ensuring seamless services across a multitude of wireless systems and networks.

A. *Present:*

seamless handoffs can be designed for homogeneous networks (IEEE802.11 WLAN & CELLUER)- at layer2 and with limited participation of the mobile node (MN) in the decision.

B. Future:

For ip to mobile node application where there is a multiplicity of potential access technologies, the requirement of functionality in the MN and access router (AR) to facilities seamless transfer and the need of Quality of service (QoS), authentication as well as the need of security infrastructure changes are to established.

C. *Challenges:*

How do we help facilities the future vision during transition? Assuming that IPv6 specification has fundamental mobile ip functionality and multiplicity of wireless access technology in a particular geographic area.The key concept is integrating the 4G capabilities such as application adaptability and being highly dynamic with all of the existing mobile technologies through advanced technology. Future mobile communication system will certainly and surely achieve the concept of a "global village".

VII. MANAGING LOCAL MOBILITY

A. *Limited scale solution*:

As ratio of mobile to non-mobile endpoints grows, address aggregation becomes increasingly difficult and routing table size increases. It increases seamlessness over basic mobileIP and in turn depends upon wireless access technology used (i.e. IEEE802.11, GPRS, Bluetooth, IR).

B. *No mobile ip delay:*

only routing update delay for an interior routing protocol. It may need to supports temporary bi-casting near handoff.

VIII. QOS AND MOBILE ROUTER ISSUES

A. QoS issues:

cellular voice packets are processed differently than data packets. Voice frames are optimized for minimum overhead & maximum utilization. Cellular "data packets "are limited persistence protocol on wireless link. This is certainly not acceptable for VoIP.

B. *Mobile wireless networks /routers issues:*

MobileIP was not designed for high frequency mobility or for more than one ip access link. In practice, seamless mobility across trust domains requires layer 3 solutions. Limited scale of layer2 technology solutions can be suitable to nano-mobility application. SCTP (single connection transmission protocol) based mobility can also be used when endpoints have SCTP capability.

IX. BACKGROUND OF SMARTPHONE ATTACKS

Smartphone is the unified communications system which combines telecom and Internet services into a single device. Smartphone's are end points to both telecom networks and the internet, it means that Smartphone's are connected to both internet and telecommunication networks. Following figure illustrate this fact.

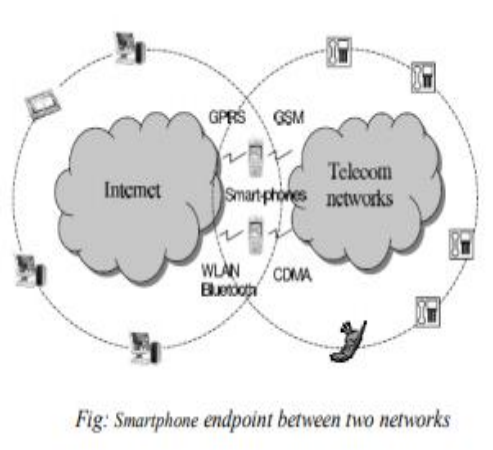

Fig: Smartphone endpoint between two networks

Fig 3 : Smartphone Endpoint Between Two Networks

Although the detailed design and functionality vary among these OS vendors, all share the following features:

1. Access to cellular network with various cellular standards such as GSM /CDMA and UMTS.
2. Access to the Internet with various network interfaces such as infrared, Bluetooth, GPRS/CDMA1X, and 802.11; and use standard TCP/IP protocol stack to connect to the Internet.
3. Multi-tasking for running multiple applications simultaneously.
4. Data synchronization with desktop PCs.
5. Pen APIs for application development.

X. GENERAL ARCHITECTURE OF SMARTPHONE

Smart devices are grouping of mobile phones and platform with rich connectivity and powerful computing proficiency. Therefore, a Smartphone has the necessary modules of computing platforms, operating systems, third-party applications and Smartphone. Unlike Android, the iOS operating system works only on iPad, iPhone, and iPod devices. To manage all operating systems and devices, the OS provide necessary technology and interface and support to implement the new application to meet a variety of Smartphone user needs.

On another hand, the operating system can access user data and communicate directly with other services as well as devices. In general operating system can only access hardware directly, but the access to user's data might result in compromising user information and the information from the Smartphone can be maltreated by attackers just like attacks on the computer such as viruses, Trojans, etc.

XI. SMARTPHONE PROBLEMS

Powerful hardware, advanced operating system, latest applications, increasing capabilities of Smartphone and functionality are enough, but an increase in present security threats in Smartphone's became a prominent issue.

XII. SOURCE OF SMART-PHONE ATTACKS

The Smartphone problems can be categorized into four categories: Authentication, Data Protection and Privacy, Vulnerabilities and Attacks. Fig.1 shows such categorization of Smartphone security problems.

A. Authentication in Smartphone's:

Authentication could be achieved using one of the following three methods. The first one is to use what users knows such as PIN or password. The second method is which users have certain code such as a token. The third method is commonly known as biometric. After introducing the general architecture of Smartphone and its main parts or assets, we classify Smartphone's security threats and vulnerabilities.

B. Data Protection and Privacy:

Boshmaf et al., address the problem of data protection from user-centered perspective and analyzed the user's need for data protection for Smartphone's systems. The authors outlined the types of data that users want to protect; they also investigated the practices of current users in the protection of such data and show how the security requirements vary across different types of data.

C. *Vulnerabilities:*

There are many several attacks and vulnerabilities in Smartphone's that can lead to insecurity or be victimized by malicious attackers to create attacks. Smartphone's vulnerabilities include the following: System fault/defects, insufficient management of

applications, insecure wireless network and lack of user awareness.

XIII. ATTACKS ON SMARTPHONE

A. Logical Attack:

Browser: In addition to the usual browser vulnerabilities (Web standards processing), Smartphone's offer further targets due to the interaction between browser and phone. For example, the user identity connected to the SIM card may be abused. Remote Maintenance: Disabled automatic updates or an insecure configuration may promote attacks just as much as insufficiently protected interfaces to the remote device management.

B. Physical Attack :

Wireless Interfaces: When an attacker is located in the immediate vicinity of a device, manipulated data can be sent allowing vulnerabilities in radio communication (Bluetooth, NFC, Wi-Fi, etc.) to be taken advantage of in order to obtain user data and passwords illegally. Memory Cards: Data on external storage media is frequently unprotected. An attacker may be able to read the data directly if a Smartphone ends up in his hands. When an attacker is able to store manipulated data on the memory card, the Smartphone's vulnerabilities can be taken advantage of. If a manipulated Smartphone is hooked up to the company's PC, the attackers may use it as a host for infections and attack the computer during synchronization and beyond that the overall enterprise network as well.

C. Spamming :

Attackers can manipulate smart-phone to send junk through SMS. compromised smart-phone can spam for "free"; and therefore its owner may not even notice its bad behavior. Free SMS spamming gives attackers good incentives to compromise smart-phones.

D. Bluetooth:

Bluetooth is wireless device. Now a day's Bluetooth is in-build in Smartphone This wireless device spread worm automatically.

XIV. THREATS

Threats can be malicious code to the Smartphone's that can destroy or damage your Smartphone, that means it can stops functioning and give the chance to the attacker to access the information and data which is stored in your device. Malware means malicious code. It is a computer program that aims to harm the system in which it resides. That means it used to attack to the computing devices including Smart phones. Today there are more than 300 types of malware which is aiming at Smart phones. Worms, Trojan, viruses , Malware , Misuse available resource and service , Enterprise/private Data Loss, Data tamper and spyware this are some types of Threats. The major classifications of malware for Smart phones are:

A. Worms:

A worm is a small program or application designed to copy itself from one device to another automatically in another words a worm is a program that reproduces on multiple computers across a network.

B. Trojan:

Trojan is any malicious computer program which is used to hack a computer by misleading users of its true intent. Trojans do not replicate by infecting other files or computers. Instead, Trojans survive by going unnoticed: they may sit quietly in your computer, collecting information or setting up holes in your security, or they may just take over your computer and lock you out.

C. Virus**:**

A virus is a piece of software that can infect other programs by changing them. The changes contain a copy of the virus program, which can then go on to infect other programs. Virus attaches itself to another program and executes when the main program is run. Once a virus is executing, it can perform any function, such as erasing files and programs.

D. Malware**:**

Virus hosted on a legitimate code, replicable spread worms, Trojan horses with action in purpose.

E. Misuse available resource and service:

Email/SMS spam or denial of service. A group of the attacking devices send volume data to one target on the Internet to impact the target's services.

F. Enterprise/private Data Loss:

Work place data on a mobile device may be uploaded to home PC while synchronizing of

entertainment downloading or Enterprise/private data loss due to stolen device.

G. Data tamper**:**

Intentionally modify/corrupt device data without the permission such as device's contact list.

XV. TYPES OF ATTACKS

A. Pop-up ads

Adware forces users to click on an ad that directs user to download/install malicious program such as Trojan horse in a word or pdf file. The downloaded may also be the key logger which monitors mouse operations and keyboard strokes to steal personal data.

B. Man-in-the-middle(MITM)

Hacker may hijack a session by eavesdropping where the hacker makes independent connections with the victims and relays messages between two persons so that both parties think that they are talking directly to each other over. The MITM hacker intercepts all conversation and attacks.

C. Botnet

One attacker controls a group of devices to send a large volume of traffic to a victim resulted in a denial of service (DoS) attack. Afterwards, the hacker Demands the victim a payment to stop the attack.

XVI. MALWARE DETECTION AND PROTECTION SOLUTION

A. Filtering with blacklisting and white listing

Many search engines place malicious website a Blocked list "blacklist." The search engine will warn to potential visitor who intends access such sites on the list. An enterprise or a personal can also setup their own blacklist. A whitelist filter only access to these on the list if a whitelist is exclusive. The filter techniques are widely used for spam email filtering.

D. View page source code

Use Page Source (Firefox) or Source (IE) to view the actual source code to find out the injected malicious code

XVII. CONCLUSION:

This paper describes the issues of a network connectivity of mobility for sharing files in an seamless manner over an geographic location. Overview of a comprehensive list of research issues of the wireless network connectivity like signal fading problem, mobility problem, data rate and the quality of service issues problems of the wireless networks connectivity. In additional the popularity of wireless networks growing at a exponential rate, the data rate enhancements , minimizing size, cost, low power networking , user security and the best requirement to obtain the required QoS problems becomes more challenging because wireless networks are rapidly becoming popular, and user demand for useful wireless applications is increasing. Smartphone's are advanced computing and communication devices regarding mobility and their usage. Very little research is found on Smartphone attacks and their mitigations. We try to find counter measures too many kinds of attacks and how to avoid them. We have discussed telecommunication networks, internet, software and hardware. Before launching new Smartphone's on the market all the companies including both hardware and software developers should ensure that the product is secure in all ways. We have outlined a number of defense strategies, many of which demand much further research.

REFERENCE

[1]Bitcoin transaction and security implementation.
[2] http://en.wikipedia.org/wiki/Wireless_network
[3] IEEE 802.11-1999, IEEE Standard for Local and Metropolitan Area Networks Specific Requirements – Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, June 12, 1999.
[4] V.O.K. Li and X. Qiu, ―Personal Communication Systems (PCS),‖ Proc. IEEE, vol. 83, no. 9, Sept. 1995,
[5]Mobilethreatsattacks https://www.utc.edu/faculty/li-yang/5.mobilethreatsattacks.pptx
[6]Research on Different Types of Attacks in Smart Phones http://ijarcet.org/wp-content/uploads/IJARCET-VOL-5-ISSUE-6-2065-2069.pdf
[6] MicrosoftResearch http://research.microsoft.com/enus/um/people/helenw/papers/smartp hone.pdf
[7] Mobile Malware: Threats and Prevention by Zhu Cheng available at www.mcafee.com
[8] Jim Kurose ―Open issues and challenges in providing quality of service in high-speed networks‖ Computer Communication Review, 23(1):6-15, January 1993.
[9] J.H.Schiller, Mobile Communications, 2nd ed., Addison-Wesley, 2003. [5] Y. Hu and V.O.K. Li, ―Satellite-Based Internet: A Tutorial,‖IEEE Commun. Mag., vol. 39, no. 3, Mar. 2001, pp. 154–62.
[10] Antivirus Software http://antivirus.about.com