Advances in Wireless and Mobile Communications.
ISSN 0973-6972 Volume 10, Number 5 (2017), pp. 913-924

http://www.ripublication.com

Study of Various Generation and Bandwidth Sharing Issues in Mobile Network

Abhishek Prabhakar[a], Dr. Amod Tiwari[b], Prof Vinay Kumar Pathak[c]

[a]Asstt. Prof., Dr,AITH Kanpur, India.

[b]Director, NCET Kanpur, India.

[c]VC, APJ Abdul Kalam Technical university, Lucknow, India.

Abstract

An important performance index of a mobile system among other indices is "number of users" that a system can support. For a system to be supported by a single base station catering to large number of users there is need of high power transmitter. The enhancement in the capacity can also be achieved by using an array of lower power transmitter in cellular array arrangement. Security however remains an important concern for all mobile networks. The kind of infrastructure in new generation networks has been observed to be packet and IP based. An important improvement seen in 4G systems over 3G systems is that it provides broadband internet access in addition to usual voice and other services. This can be made use of in Laptops using wireless modems, smart phones and in other mobile services. In transferring data using wireless communication at high speed in mobile phones and other data terminals, 4generation long term evaluation (4G LTE) is much in use. An effort has been made to analyze the next generation mobile networks in light of threats to security of access points in networks supported by cellular networks.

Keywords: Ad-hoc network; mobile generation; AODV; DSR; mobile network security

1. INTRODUCTION

Over the last decade, there has been lot of development in mobile technology. The systems that have been upgraded from first generation to second to third and now some companies have launched even 4G systems. The technology too has changed a great deal. The first generation (1G) wireless systems while use frequency division multiple access(FDMA)as multiple access technology, the second generation (2G) wireless system use digital transmission communication system that have been in use for some time are those in the first generation and second generation. Third generation system are also under use these days. .The first generation (1G) wireless communication system use frequency division multiple access (FDMA) as the multiple access technology. The second generation (2G) wireless system use digital transmission .The multiple access technology makes use of both time division multiple access (TDMA) and code division multiple access (CDMA).The third generation (3G) is based on CDMA as multiple access technology also support multimedia services. The Cellular system is changing very fast. In cellular communication technology the change in the nature of service, on compatible transmission technology, and new frequency bands have been observed to have been used frequently. With introduction of Wireless LAN (WLAN) technology, networks have been able to achieve connectivity with useable amount of bandwidth .The Mobile devices used while travelling, such as mobile smart phones, laptops allowed users to access data with more flexibility especially when people on the move. At present, the wireless networks though are quite in vague they are unsafe and are prone to attack by attackers .The main elements that a new generation of mobile network contain are given in figure 1. As is seen in figure they are mainly femtocell and wifi. While using wireless communication [1], data has to be protected by applying security checks and this is done at several levels. The present paper seeks to analyze the mobile networks and the potential threats that a system, specially, cellular network is faced with regarding bandwidth sharing issues..

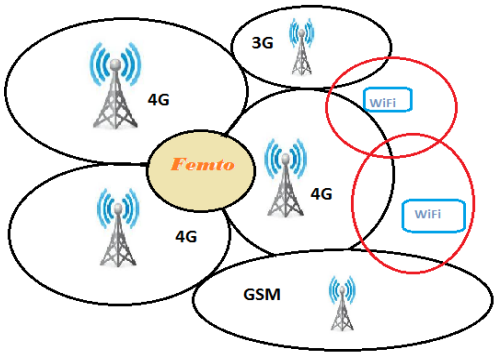


Figure 1. Next Generation of Mobile Networks

2. RELATED WORK

A commercially available femtocell can be modified and used to track phones intercept communication and even modify traffic. A security analysis of femtocells [2] was conducted by Borgaoankar et. al. They pointed out several security drawbacks which allowed a hacker to attack femtocell's firmware. They also showed how location verification techniques can be surrounded and how an attacker can use a femtocell from an unregistered location to avoid roaming charges [3].

The use of honeypot system [4] to detect infected mobile devices proposed by Lance spitzner et al. Their system analyzed and monitored the communication aspect of the mobile devices. The honeypot however has not been designed to detect or analyze attacks against the mobile networks. A method to use nomadic honeypots[5] to collect threat intelligence directly on smart phones was proposed by Liebergeld et al.The solution they proposed allowed to contain attacks even in case of complete capture of smart phone operating system. It required modification of Smartphone firmware. Software to prevent against attacking and exploiting pocket pc's Smartphone [6] was proposed by mulliner et al.This includes vulnerability analysis of smart phones.

3. GENERATION OF MOBILE NETWORKS

The first to arrive were the first generation of wireless telephones known as 1G .They were introduced in 1980's,used analog telecommunications standard .They were replaced by second generation known as 2G during 1990's and used digital telecommunication signal .The main difference between 1G and 2G system has been while the radio signals that used 1G systems were analog ,those used by 2G have been digital.This generation included data access to mobile phones. 2G cellular telecom networks were commercially launched on the GSM(Global system for mobile communication) standard in Finland by Radiolinja.The technology used in second generation 2G systems provided the services like sending text messages ,picture messages and multimedia messages(MMS).All text messages sent over 2G were first digitally encrypted and then the data was transferred in such a way that only the authorised receiver could receive and read it.

The third generation, 3G mobile phones use the technology that allows them to access the internet. This enables the users to surf web page, make video calls and download music. In addition to this the access to the internet is even faster .3G telecommunications networks support services that provide higher data transfer rate .The applications of 3G technology used include wireless voice telephony ,mobile internet access video calls and mobileTV .General packet radio service (GPRS)is a packet oriented mobile data service on 2G and 3G cellular communications.GPRS provides data rates of 56-114 kbit/sec.2G cellular technology combined with GPRS is sometimes described as 2.5G i.e. a technology between 2G and 3G generation of

mobile telephony.4G refers to fourth generation of mobile phone technology. A 4Gsystem provide high speed internet access. 4G provide mobile web access, gaming and IP telephony mobile TV, cloud computing and video conferencing.4G technology offers increased voice, video and higher data rates. 5G or fifth generation of mobile network provide next mobile standards beyond current 4G standards.5G technology are theoretical and not real. 5G is also called as complete wireless communication and having no limitations.5G transmission has high transmission speed .It offers worldwide connectivity and high data rate capabilities. The hand held phones have more –power, large memory and good quality of audio and video. The speed in 5G technology can extend up to 1Gbps having low cost than previous generations. The user can connect with various wireless devices. 5G provides high resolution for cell phone users with 25Mbps connectivity speed. Uploading and downloading can be up to 1Gbps and supports virtual private network.5G is sixth sense technology with AI (Artificial intelligence) capabilities. 5G uses IPV6 technology and IP is assigned as per connected network and geographical location.5G uses UWB (ultra wide band) networks having bandwidth of 4000Mbps which is much higher than today's wireless networks .

4. MOBILE AD-HOC NETWORKS (MANETS)

MANET is short term used spontaneously in wireless network of mobile nodes communicating with each other without the interaction of any fixed infrastructure or central control. Usually it is a system in which mobile nodes or mobile station serving as routers interconnected by wireless links. Network communication and management tasks are usually performed in a distributed manner .Since the nodes moves or adjust their transmission and reception parameters, MANET topology may vary from time to time. The use of ad-hoc networks in mobiles makes use of advanced networking mechanism. The ad-hoc wireless network does not need any infrastructure in other words it is a network without a base station .In mobile network since the nodes are mobile the likelihood of change in topology randomly over a period is fair .The technology used enables the system to be decentralized where the inclusive network activity including discovering the topology and the delivery of message need to be executed by the nodes themselves by incorporating the routing functionality over mobile nodes.

Chances of likelihood of mobile networks being corrupted:

The use of wireless links makes the network susceptible to attacks.. In Wired networks, attackers do not need physical access to the network to carry out these attacks. The Wireless networks have lower bandwidths than wired networks and hence attacker can exploit network bandwidth with ease.

Dynamic Topology:

In mobile ad-hoc network nodes are free to move, they can leave or join the network and can move independently. This leads to frequent changes in network topology. In dynamic environment it is difficult to differentiate between the malicious and normal behavior of network. A node sending disruptive routing information may be said to be in malicious mode. MANET nodes can leave and join the network, and move independently. As a result the network topology can change frequently. It is hard to differentiate normal behavior of the network from malicious behavior in this dynamic environment. For example, a node sending disruptive routing information can be a malicious node. Nodes with inadequate physical protection are prone to being hacked.

4.1 Cooperation:

Routing algorithms in MANETs usually assume that nodes behave according to expectation and are not malicious .If attacker can become important routing agent it can disrupt network by rejecting or disobeying protocol specification. In this way a node behaving as functioning to other nodes and participating in overall decision making mechanism can affect network significantly. So cooperation between nodes is of most importance. As a result, a malicious attacker can easily become an important routing agent and disrupt network operations by disobeying the protocol specifications. For example, a node can pose as a neighbor to other nodes and participate in collective decision-making mechanisms, possibly affecting networking significantly .So cooperation between nodes is of most importance and at the same time the differentiation between nodes that follow protocols and those don't should also be clear .This is serious shortcomings in such network .MANET don't have clear line of defense and hackers may attack from all directions .The line of demarcation between the internal network from the outside world is not very clear. Therefore the decision on the point where the traffic monitoring and access control mechanism should be deployed becomes difficult .The network information on MANET's is distributed across nodes that can only see the packet sent and receive in their transmission range whereas in wired network all traffic goes through switches, routers or gateways.

4.2 Limitations:

There are number of devices which use MANET's ranging from laptops to other handheld devices like PDA's and mobile phones .They generally employ different computing and storage capabilities and constitute the focus of new attacks. The mobile nodes generally run on battery, this has further paved way for new types of attacks targeting this aspect as well. In present day networks the introduction of

additional security features increasing the computation ,communication and management load poses serious challenge for network that are already resource constrained.

5. Ad-hoc ROUTING PROTOCOLS

Ad-hoc routing protocol deals with how mobile nodes decide which way to route packets between devices in a mobile Ad-hoc network. In MANETS initially nodes are not familiar with topology; rather they have to discover it. New mobile node announces its presence and should listen for announcements broadcast by its neighbors.

Ad-hoc Routing Protocol May be classified as under:-

5.1 Proactive (table driven) routing protocol:-

This type of protocol maintains fresh list of destinations and their routes by periodically distributing routing tables throughout the network. Examples are DSDV (Destination sequenced distance vector) routing protocol.

5.2 Reactive (on demand routing protocol):-

This type of protocol finds a route on demand by flooding the network with route requests packets. Examples are Dynamic source routing (DSR) and AODV (Ad-hoc on demand distance vector routing protocol)

5.3 Hybrid (both proactive and reactive):-

This type of protocol combines the advantage of both proactive and reactive routing protocols.

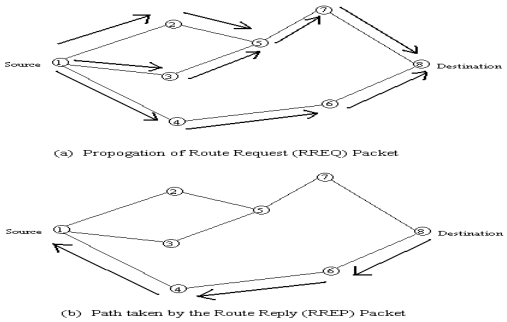
5.4 Hierarchical routing protocols:-

With this type of protocols the choice of proactive and reactive routing depends on hierarchical level where a mobile node resides

6. AODV ROUTING PROTOCOL

Ad-hoc on demand distance vector routing protocol (AODV) work best under dynamic link conditions as they offer quick adaptability. It is reactive routing protocol that discovers route only when they are required. They are also suited to low processing and memory overhead ,low network utilization and determine unicast routes to destination within Ad-hoc network[7] .It is believed that AODV can handle low ,moderate and high mobile rates along with variety of data traffic loadings. The

security provisions however are not taken care of that well. AODV functions mainly on three types of messages: (a) Route request RREQ messages.(b)route reply RREP messages(c)Route error(RERR) messages. When clear route for destination is not available to another node, the node start discovering the route by broadcasting a RREQ message .The routing table of the nodes within the neighborhood are organized to optimize the response time to local movements. The neighbor in turn broadcast the packet to neighbors till it reaches a node that has recent route information about destination.figure2 (a) the nodes receiving RREP messages and requesting route in the node, they update their routing table with new routes. Due to mobility of nodes in the network or due to transmission errors wireless network come across frequent link breakages .The Ad-hoc on demand distance vector routing enables the mobile nodes to respond to link breakages and changes appropriately at the same time. When AODV is functional the nodes can control their connectivity in two ways:-(a) Linking layer notification using control packets like link layer acknowledgement messages i.e. ACK or RTS-CTS (b) Passive acknowledgement i.e. notification by listning on channel to find out if the next node forwards the packet or not.AODV uses only symmetric links because the route reply packet follows the reverse path of route request packet figure.2 (b)



(a) Propogation of Route Request (RREQ) Packet

(b) Path taken by the Route Reply (RREP) Packet

Figure 2

DSR (Dynamic source routing):-

This protocol is similar to AODV but the route is maintained in the packet header. In this routing the intermediate nodes do not route information and also there is no requirement of periodic route advertisement. Intermediate nodes propagating a route request; add their ID in the packet header figure 3. When a packet reaches destination, route reply is returned.

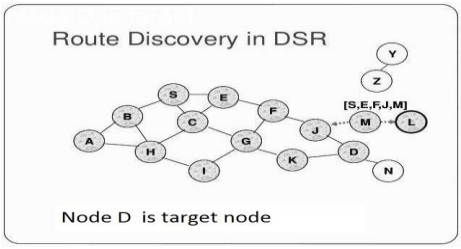


Figure 3. Route discoveries in DSR

7. PROACTIVE VS REACTIVE PROTOCOLS

Proactive: - It is more efficient when routes are used many times. It requires periodic route update .If the nodes are mobile it affects entire network.

Reactive:-It is more efficient when routes are used occasionally. In this approach node first find the route before transmission of data. There is no requirement of periodic route update.

8. CHALLENGING ISSUES IN MANETs

Some of the most challenging issues in MANETs are following-

(a) Limited wireless range.

(b) Broadcast nature of wireless

(c) Routing problem.

(d) Packet losses

(e) Battery constraints

(f) Security issues

9. ATTACKS AGAINST MOBILE NETWORKS

Among the ways to destroy the target devices most dangerous types are flooding and the denial of service(DoS) and distributed denial of service(DDoS).They could be accomplished individually or organised using botnet [8,9].Increasingly high number of requests could put most of the firewall security system out of service due to limitation in state tables. Therefore a denial of service (DoS) or distributed denials of service mode of protection service or product are employed against attacks coming from internet. Generally it is recommended that DDoS protection be placed in the ISP's side [10]. Various types of attacks which can be done on cellular communication networks are as follows:

9.1 Denial of Service attacks (DoS)

"Denial of Service (DoS) kind of attack is a attack that renders computer or a network incapable of providing normal services".DoS attack are normally carried out against a service running on a specific IP address in order to deny access to legitimate users and cause damage to service owner. The most common types of DoS attacks targets the computer network bandwidth or connectivity.Bandwidth attacks flood network with such a high volume of traffic that all available network resources are consumed and legitimate user requests cannot be completed .Connectivity attacks flood a computer with such number of requests that all available operating system resources are consumed and computer cannot process the legitimate user requests. The focus is mostly on local attacks i.e. jamming, as well as threats against Radio access networks RAN that could be leveraged from a single attacker.

9.2 Distributed Denial of Service attacks (DDoS)

DDoS are IP packet-based attacks launched at the network infrastructure. "A DDoS attack uses many computers to launch a number of DoS attack against the targets. A DDoS attack happens when multiple system flood the bandwidth of resources of a targeted system. In DoS attack a hacker uses a single internet connection to flood a target with fake requests usually to exhaust server resources. DDoS are launched with multiple connected devices that are distributed across internet. Unlike single source Dos attack DDoS attempts to target network infrastructure with huge amount of traffic. If pass bandwidth is p, where p is prime than with the help of Euler function

$$\Phi(p)=p-1 \quad \text{.....(1)}$$

Where Φ(p) is totient function[11] which counts the positive integer upto given integer n that are relatively prime to p .

Since all numbers less than p are relatively prime to p. If $m = p^{\alpha}$ (where $\boldsymbol{a}$ is a power of pass bandwidth p) is a power of a prime, then the numbers that have a common factor with m are the multiples of p: p , 2p, 3p, ..., $p^{a-1}(p)$. There are $p^{\alpha-1}$ of these multiples, so the number of factors relatively prime to p^{α} is

$$\phi(p^{\alpha}) = p^{\alpha} - p^{\alpha-1} \quad \text{.....(2)}$$

$$= p^{\alpha-1}(p-1) \quad \text{.....(3)}$$

$$= p^{\alpha}\left(1-\frac{1}{p}\right). \quad \text{.....(4)}$$

p^{α} is pass bandwidth of network.

9.3 Insider attacks

An insider attack is also known as insider threat. Insiders have advantage over external hackers because they have authorized system access and also know network architecture and system procedures. Usually organisation focus on external architecture, so there is less security against insider attacks.Now take a general m divisible by$p$. Let $\phi_p(m)$ be the number of positive integers $\leq m$ not divisible by p. As before, p, $2p$, ..., $(m/p)p$ have common factors, so

$$\phi_p(m) = m - \frac{m}{p} \quad \text{.....(4)}$$

$$\phi_p(m) = m\left(1 - \frac{1}{p}\right). \quad \text{.....(5)}$$

Where m is multiple factor of passed bandwidths

9.4 Overview of threats against mobility availability

Threats include all those potential factors or platforms that challenge the smooth running of the system from outside. These are based on attack platforms, the scope, the difficulty or cost incurred to launch such an attack and finally an estimate of the impact against the availability of an LTE network. The larger the impact the more is the chances of getting affected within the scope of attack. A smart jamming attack despite being of local nature has potential to block one or more multiple sections at very low cost. The cost of a signalling amplification attack or a threat against the HSS (home subscriber subsystem) is larger because it requires a large botnet of infected devices.

10. RESULT ANALYSIS

By comparing equation (5) and equation (4) at passing same band width. Yield

$$p^{\alpha}\left(1 - \frac{1}{p}\right). = m\left(1 - \frac{1}{p}\right). = \phi_p(m)$$

for higher degree calculation taking log both side

$\log[P^{\alpha}(1- 1/p)] = \log[m(1-1/p)] = \log[\Phi(p)]$

From the above equation we can yield Φ(p)= m InIn(p)

Table 1.0 Relation between input data and pass bandwidth

P	½	1	3/2	2	5/2
Φ(p)=mInIn(p)	1000	2000	3000	4000	5000

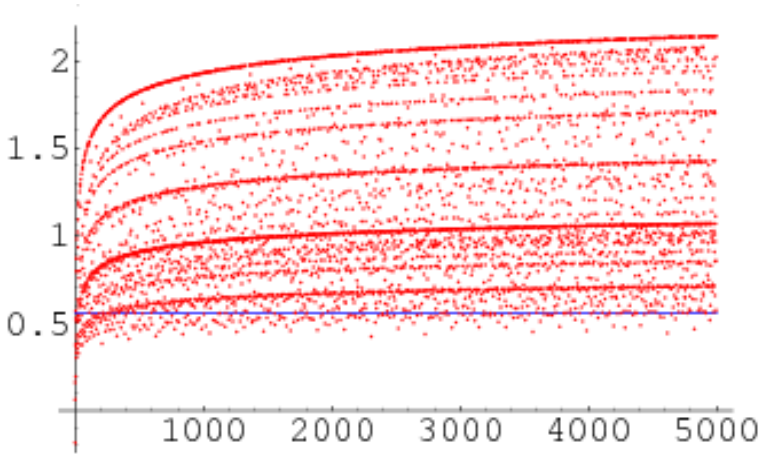


Figure 4: Passed p bandwidth with m multiple factor

11. CONCLUSION

Results after applying above equation on different values of P (passed bandwidth-Y-axis)) and number of users (x-axis)are shown in table 1.0 and it is also represented graphically in figure 4 shown above . If we increase the bandwidth and number of users simultaneously then after some time the number of users will increase but at optimum level the bandwidth remains constant or unchanged .The conclusion of research paper is that passed bandwidth is directly affected with number of users but at a constant bandwidth (p) where $0 \leq p \leq 2$ means that number of users does not affect bandwidth in a given transmission area.

Wireless technologies enable devices to communicate without an actual wired connection and used in areas where it is difficult to build connection using wires. Long term evaluation (LTE) provides increased speeds and greater bandwidth and gives users what they want, which is faster access to applications. Cellular Networks are open to attacks such as DDoS, DoS, channel jamming, message forgery etc. Therefore, it is necessary that security features are also added that prevent such attacks.

REFERENCES

[1] http://en.wikipedia.org/wiki/Wireless_network

[2] en.wikipedia.org/wiki/Femtocell

[3] en.wikipedia.org/wiki/Roaming

[4] Lance (2002). Honeypots tracking hackers. Addison-Wesley. pp. 68–70. ISBN 0-321-10895-7

[5] L4android: A generic operating system framework for secure smartphones - Lange, Liebergeld, et al. – 2011

[6] http://www.mulliner.org/pocketpc/

[7] Perkins C., Belding-Royer E., Das S., "RFC 3561: Ad hoc On-Demand Distance Vector (AODV) Routing", http://www.ietf.org/rfc/rfc3561.txt, 2003

[8] Tyagi, A.K.; Aghila G. A wide scale survey on botnet. Int. J. Comput. Appl. 2011, 34, 9–22.

[9] Sharma, R.K.; Chandel, G.S. Botnet detection and resolution challenges: A survey paper. Int. J.Comput. Inf. Technol. Bioinforma. 2009, 1, 10–15.

[10] Douligeris, C.; Mitrokotsa, A. DDoS attacks and defence mechanisms: Classification and state-of-the-art. Comput. Netw. 2004, 44, 643–666

[11] J J Sylvester 1879, "on certain ternary cubic form equation": American journal of mathematics 357-393:Sylvester coins the term totient on page 361.