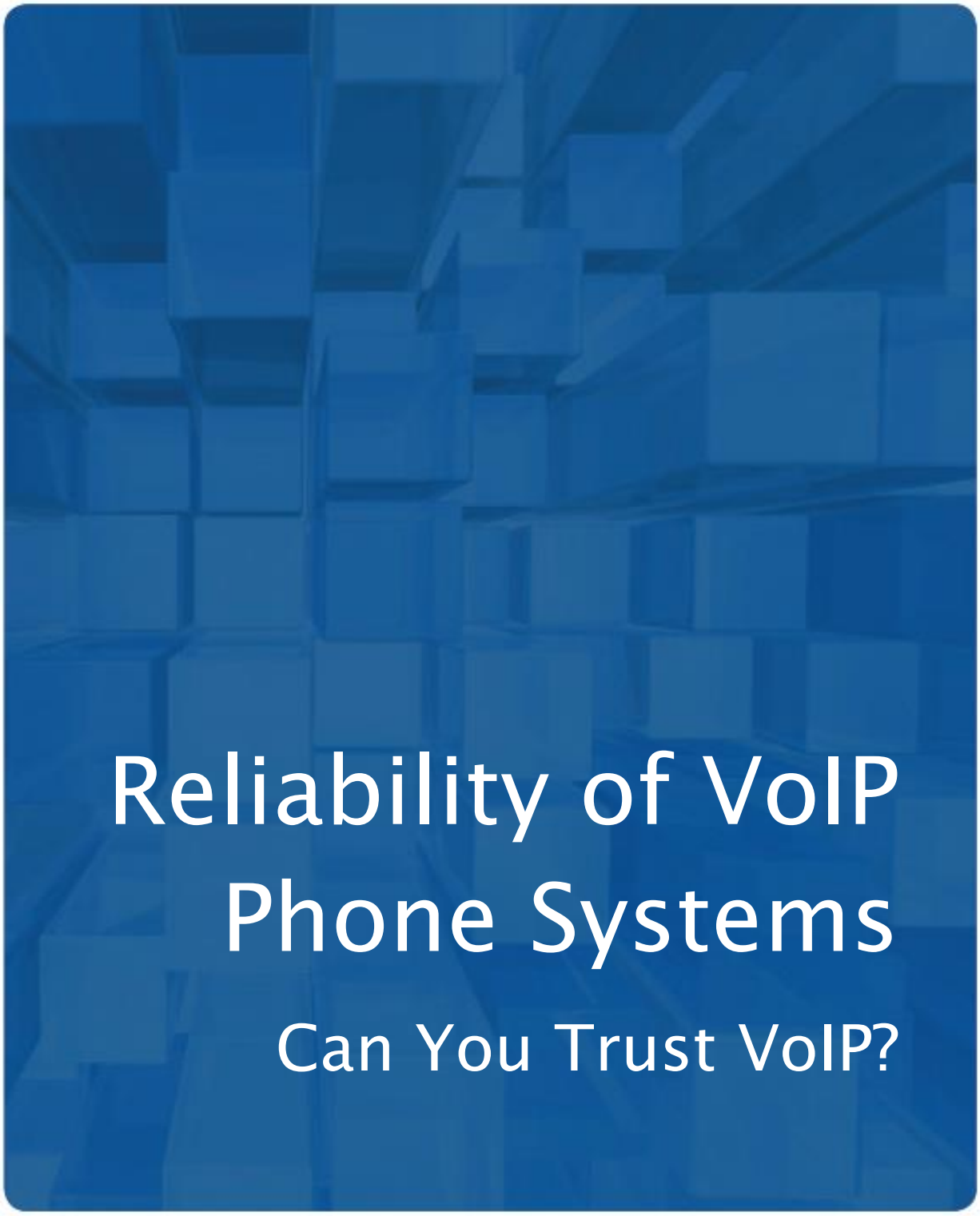
COMPARE BUSINESS PRODUCTS



Reliability of VoIP Phone Systems

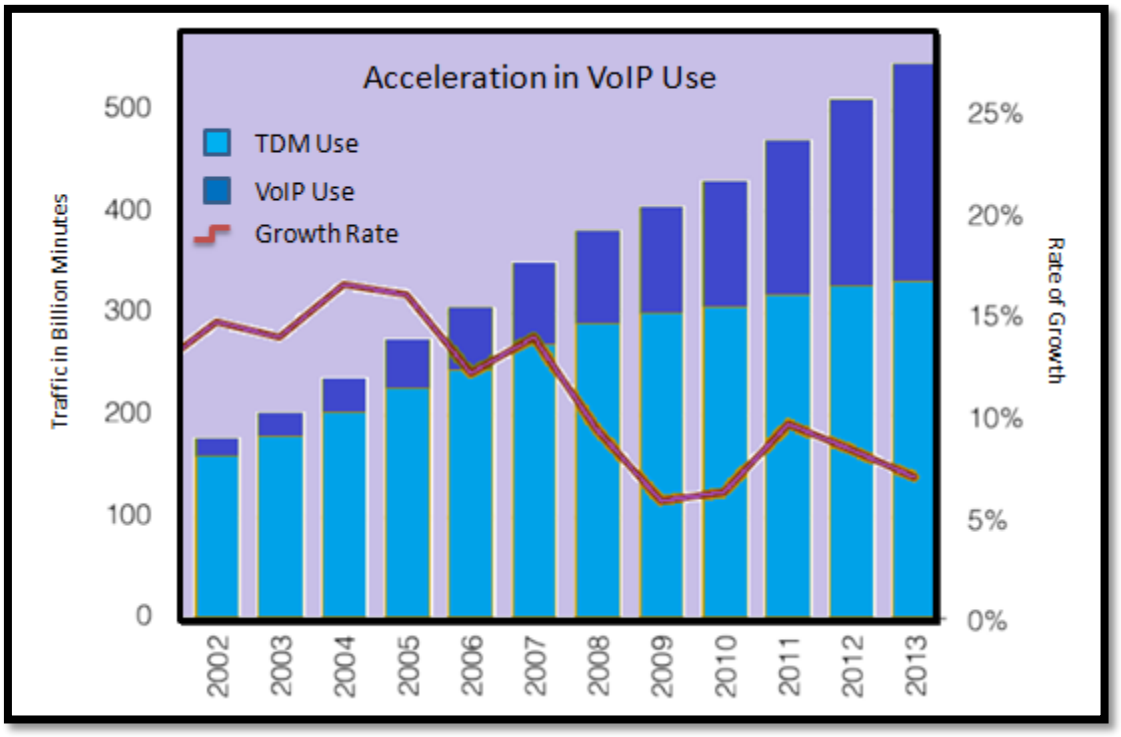
Can You Trust VoIP?

Contents

Reliability of VoIP Business Phone Systems

There can no longer be a debate about the fact that analog phone systems are on their way out. While there are still a number of TDM (Time Division Multiplexing – technology used by older, analog systems) systems in use, they are mostly legacy. As spare support and expertise becomes increasingly difficult to find, companies are switching over to IP PBXs.

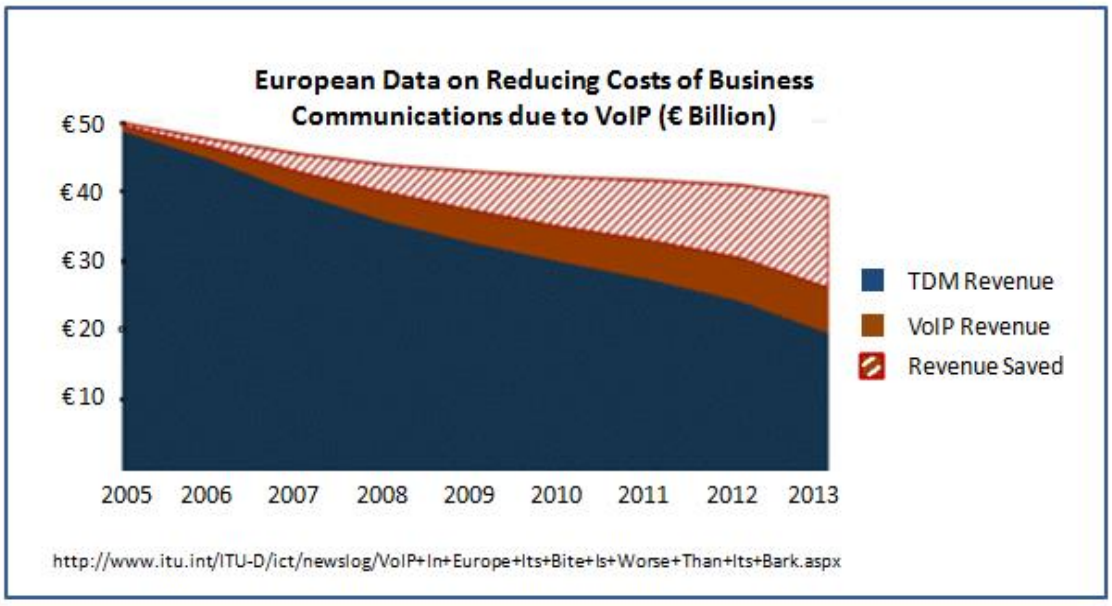
Nevertheless, growth continues in the telecom sector and as the graph below shows, while growth in TDM devices has reached a plateau, VoIP minutes are growing rapidly. Most of the growth is now in VoIP devices.



For many people, there was something comforting about the Public Switched Telephone Network (PSTN) and the fact that there was a physical copper line connecting the phone

to the central office. You could see the technology involved and it worked. IP phones on the other hand connect through the LAN in the office or via Wi-Fi and the large number of buttons, screens and messages can seem to be intimidating and complex.

Businesses are naturally concerned about the reliability of VoIP technology and no business wants to miss out on a customer call. Most people accept that VoIP gives more features at a lower cost. Therefore once reliability can be understood and built to a level where VoIP phone systems are as reliable as TDM ones, we can expect a large jump in VoIP usage. This jump in VoIP minutes will naturally be accompanied by a drop in revenue expenditure of companies. This trend is already visible in the graph below.



What then is the issue with VoIP reliability?

VoIP Technology Issues

To understand one aspect of the problem, we need to understand how the Internet transfers information in packets. While your company could set up its own network

between branches and thereby control traffic somewhat, the underlying mechanism would stay the same.

In real life speech comes to us in a continuous stream (even if it is over the plain old telephone system). Any transfer of information over the Internet is in packets of data. Therefore, what is being said into a VoIP phone is converted into packets, suitable addressing information is added and the packet is handed over to the network (internal LAN, proprietary network or the Internet) for transfer to the other party.

The advantage with IP networks (of which the Internet is the largest) is that these packets can take any of a number of alternate paths to their destination. This is what gives the Internet its robustness. Your packets generally reach – and therefore if you are using the Net to download a file or open a web page, the system works.

> VoIP can be affected by packet loss, latency and jitter. Just as any other Internet communication can.

In case a certain packet gets lost in the way, the recipient browser just asks for a resend. Therefore, depending on the quality of the network and its congestion, your file can take a little longer to load, but eventually it arrives.

This system cannot work well with voice. There is no way you can make up for a missing voice packet by asking for a resend because in any case it will lead to a break in speech. Unfortunately packets tend to go missing in groups and therefore you could get breaks in conversation across long distance networks, this is especially so if one of the parties is using a network that has limited bandwidth.

VoIP protocols are not built to guarantee flawless communications. They originated when the capabilities of the Internet were recognized and people discovered that they could even speak across the network besides using email and FTP.

As a result, all VoIP systems can be affected by packet loss, latency and jitter. How they impact our communications is discussed below:

Packet Loss

VoIP systems attempt to cover for missing voice packets by providing some kind of 'comfort noise' to generate background noise, or repeat the last packet received before the one that was lost or try and fill the gap of the missing packet by synthesizing a voice from packets on either side of this packet. Since a typical voice packet is covers only 10 to 20 milliseconds (ms) of speech, this does not create a problem unless too many packets get lost.

Things are not as bad as the foregoing suggests. In developed countries, the urban infrastructure is quite capable of handling VoIP traffic. Problems could arise when connecting to rural areas or to those parts of the world where infrastructure bottlenecks still exist.

> In most developed countries the urban infrastructure is robust enough to support VoIP. Problems could arise in rural areas or in lesser developed countries.

Latency

Latency refers to the delays that the system introduces due to the processing involved. This is an inevitable consequence of the processing that is required to make a VoIP call. There are many activities that have to be completed before a voice can be generated at the other end. All of these take time and add up. If you are using VoIP within your own premises, latency is about 50 – 60 ms. Over long distances, it can be up to 150 ms. Add a satellite hop and you could add 250 ms per hop.

The International Telecommunication Union (ITU) defines rules for latency that limit latency to –

150 ms for public switched telecom networks - above 150 ms, the gaps in speech begin to interfere with the conversation and speakers could begin talking together without realizing that the other person is still speaking.

250 ms – using satellite propagation – echoes can be created and even if they are cancelled, voice collisions are almost guaranteed to occur.

During videoconferencing, audio and video are handled separately and their latencies are different. This results in a loss of lip synch that can be disconcerting.

The solution to handling latency lies (at least partly) in selecting appropriate compression schemes. Different vendors have differing approaches to compression. Some apply compression by default, others allow users to configure it as they want, yet others turn off compression to give you better audio quality and allow fax messages to be sent as well via VoIP. While the vendor solution will work, you could want to experiment with different compression schemes that the equipment supports to get the quality you want. Ultimately, compression, bandwidth requirement and quality of voice and video have to be balanced to give you the best possible experience.

Many service providers also offer dedicated lines for a VoIP, in which case many latency issues could be resolved.

Jitter

In the course of a VoIP conversation, many thousands of packets could be exchanged between the two parties who are communicating. These packets could follow different routes to their destination and be subjected to different queue lengths at various points in the transit. Naturally, these packets will face different delays at various stages and will therefore arrive at their destination at slightly varying time frames (even if they are all in sequence and none are lost). This causes jitter in the connection.

> Jitter in VoIP communication impacts Fax the most.
>
> Jitter cannot be eliminated in an IP network.

We never encountered jitter in a PSTN connection because once a call was set up, a clearly defined copper path was formed and there could be no jitter in the signals received.

Jitter in VoIP communication has implications besides merely impacting the quality of conversation. Fax over VoIP lines can be severely affected by jitter and many special systems have to be devised to handle this.

Infrastructure Needs

In a traditional PSTN phone system, the power was supplied from the telephone exchange via large battery banks. Since this was a centralized location, providing power was simple. In the event of a mains failure, there were battery banks and generators. In many cases, all other systems could fail in the event of a natural disaster, but any phone lines that survived would continue to function.

> In general, your VoIP experience is determined by the quality of your internal network.

With VoIP, indeed as with any other computer network, it is the user's responsibility to ensure that the infrastructure inside the premises works. This means providing it uninterruptible power as well. The requirement is not of your IP phones alone, the switches, routers and any other connecting devices need to be powered reliably. If you are going to make a switch to VoIP, then ensuring reliable power supply to all your networking devices is essential. Depending on the criticality of requirement, many organizations may find it useful to lay a separate UPS line to their networking devices or to provide them power over Ethernet wherever feasible.

The point that is being made is that every networking component has to be studied and dealt with individually. Procedures need to be evolved to ensure that any new devices being added to the network are not overlooked.

In many cases, users of PSTN phones connect cordless sets to them to give them a degree of mobility in their premises. These phones have many other advanced features as well. If you are using such systems, ensuring reliable power supply to these as well is your responsibility. In the event of a power failure the base station would not be able to transmit a signal and would go off the air.

Quality of Service

Quality of service (QoS) has long been a worry in the minds of users (and potential users) of VoIP. Some of these fears are justified because of the very nature of the Internet and Internet Protocols. The Internet does not guarantee the delivery of packets (although packets do get delivered most of the time) and it does not guarantee that VoIP packets will go through with an acceptable latency / delay.

However, if you look around, you will find that VoIP is being used in a large number of really critical applications. Military circuits use VoIP and air defense aircraft are scrambled using VoIP links. No other application can get any more critical than these. Therefore plainly, VoIP QoS can be raised so high that mission critical services can use these circuits.

How is this achieved?

The simplest way to explain how QoS is provided is by understanding that VoIP creates packets of data that contain 10 to 20 milliseconds of voice that has been digitized. These packets have other information added on – the address of the recipient – for example, just as a letter has an address. Besides just the address, these packets have other information added on that allows the routers of the Internet to understand that these have to be given a certain additional priority.

Using this data, routers can guarantee delivery, offer assured service and premium service. In other QoS cases, route pinning can create a virtual route between the parties to the call. All data packets follow this route. Similarly, other techniques exist as well to give you the QoS that your applications need.

The underlying story is that most people can get by on a vanilla VoIP offering whereas some critical applications need and can get a higher QoS.

Fax Support

Fax continues to be an important mainstay of businesses since it is a method of delivering legally signed document. There are certain issues about fax over IP that need to be

understood and handled correctly. The problem arises because all fax machines have developed to be used over analog PSTN lines. Even though the networks are changing, deep down inside, fax machines still are built with PSTN specs that imply machines built to use lines that have nearly zero jitter and no interruptions once a link is established. These conditions, as we have seen earlier, cannot be guaranteed in a VoIP environment.

Suffice it to say that the fax problem has been solved and your faxes will travel over a VoIP network and reach intended recipients. However, there are some major differences still.

> There are legal issues with Fax servers. Companies need to be aware and take action to meet legal requirements.

There are three ways in which faxes can be sent. Some modes can offer enormous advantages over more traditional faxes but have some serious legal implications that managers must be aware of. These modes and their implications are discussed below briefly.

- Real time fax over IP – this is the simplest mode, your fax machine connects to the network via an adapter that handles the various technicalities involved, jitter and latency are handled and the fax is reassembled at the other end. The only problems that could arise is in case of excessive jitter when the message would appear garbled. However, no legal implications are involved a resend would probably cure the issue.
- Store and forward fax management – in many setups, all faxes are actually sent to a fax server. The fax server may store these messages and forward them subsequently. The fax server can also archive faxes and store them and enforces security by encrypting faxes, identifying users logging in and so on. This is where problems arise. Since confidential data is held in a server, the fax server has to be subjected to various data protection regulations such as HIPAA etc.
- A third method is originating faxes from within your computer network (say from your PC) and sending them off over PSTN. The solution is not very elegant but allows people to generate faxes from their desktops. In case the recipient machine is a fax server that holds faxes for subsequent delivery, then the security and legal requirements discussed previously will apply.

Given the complexities of fax over IP discussed in this section, it appears (at first reading) that businesses are getting into unnecessary complexity by opting for fax over IP and that a fax server is a dangerous device. However, it is not really so. A fax server can do many useful things besides merely receiving and forwarding faxes. Faxes can be converted to image or pdf or image files and emailed to intended recipients thereby allowing them to see messages even when they are not at their desks. People can dial into the server and have their faxes read out to them, the fax server can directly interface with enterprise applications and so on. The benefits of automation are enormous and go far beyond the overhead of managing the fax system.

VoIP Security

This section does not aim to get into the technical details of security issues and therefore readers looking for information on those aspects are recommended to browse Himanshu Dwivedi's excellent book, "Hacking VoIP". On our part we have used the lessons drawn from this and other readings to present a short list of VoIP vulnerabilities.

> VoIP faces many of the problems your networked applications do. The solutions could be similar as well.

To begin, VoIP being Internet technology, one can expect many of the vulnerabilities that software systems are subjected to. There are attacks that are specific to different vendors – primarily because a few vendors account for most of the market and therefore it is easy to focus attacks. Attackers can alter the configuration of hard phones or upload malicious configuration to these devices. However, the potential for damage is limited unless an attacker is able to gain access to the VoIP server itself.

Voicemail Security

In many cases, people tend to treat voicemail as secure whereas the same persons would not reside the same confidence in email. Voicemail passwords of 4000 persons were hacked by the newspaper “News of the World” in 2011 – an event that caused a media furor.

Voicemail at best requires you to put a four digit pin to secure access. With modern technology, a four digit pin can be broken in minutes unless special precautions are taken.

Denial of Service

We have heard of ticket sales sites becoming inaccessible just a few days prior to the big game when everyone is looking to buy a ticket. The owner is then held to ransom and could be made to pay to stop the denial of service attack that his website is being subjected to.

Could such a thing happen to VoIP infrastructure as well?

With VoIP being dependent on Internet Protocols and software being at the heart of VoIP phones and servers, a denial of service attack is a possibility. However, researchers have shown that certain VoIP servers are lesser vulnerable to denial of service attacks. Studies also point out to the requirement of implementing an Intrusion Detection System (IDS) in to the VoIP infrastructure.

Besides the above, implementing Quality of Service into VoIP systems also helps in handling denial of service attacks.

Some Final Points

How has the foregoing discussion affected your views of VoIP? Have we given you an impression that VoIP still has a lot to do before it catches up with the reliability of earlier systems? This final section is being written to correct that idea.

At one level the shift to VoIP is inevitable. PSTN vendors are slowly winding down their offerings. Spares support of legacy equipment is reducing and soon expertise will also be difficult to find. Therefore, the writing on the wall is clear. PSTN will go and VoIP will replace it.

VoIP technology is mature and reliable. When you find VoIP not living up to its potential, the problem often lies in the quality of network that has been provided. If your internal network is unreliable and power comes and goes at will, then the fault lies with your infrastructure and not with VoIP.

Costs are an obvious advantage. By switching over to VoIP, your company will save money even as it gets access to a range of features that could have cost the earth on a PSTN system.

While many of these features can probably be called good to have, the one standout feature made possible by VoIP is Computer Telephony Integration (CTI). CTI allows data from the ongoing call to be used to query the company database and provide the answer to the person attending the call. For example, the caller ID can be used to bring up caller details and the outstanding orders of that caller. Previous call history can be displayed and any terms agreed upon can be brought up. As a consequence of all this data, the agent answering the call is able to handle the call much better. Many other applications are possible and a company using CTI imaginatively can gain a major competitive advantage.

Just one last point before we close, there could be some applications in your environment that absolutely demand analog lines. One example that comes to mind is legacy machinery that needs such lines for its own operations. Such machinery may be difficult to replace and therefore you need to provide it with the analog lines it needs. If you are going to switch to VoIP, this is one aspect that must be thoroughly investigated. Hybrid PBXs are available to cater to this problem.

References

Ganguly, S and Bhatnagar, S, "VoIP Wireless, P2P and New Enterprise Voice over IP", John Wiley & Sons, Ltd

Flanagan, William A. "VoIP and unified communications: Internet telephony and the future voice network" , John Wiley & Sons, Inc

Dwivedi, Himanshu. "Hacking VoIP : protocols, attacks, and countermeasures", No Starch Press, Inc.

M. Zubair Rafique et al, *"Evaluating DoS Attacks Against SIP-Based VoIP Systems"* http://muhammadakbar.com/files/globecom09-zubair.pdf