J. Basic. Appl. Sci. Res., 2(12)12694-12698, 2012
© 2012, TextRoad Publication

ISSN 2090-4304
Journal of Basic and Applied Scientific Research
www.textroad.com

Next Generation Networks Challenges for Ensuring the Security and Availability of NS/EP Communications

Arash Kalami

Department of Electrical Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran

ABSTRACT

The convergence of wireless, wireline, and Internet Protocol (IP) networks into global Next Generation Networks (NGN) is changing how the Federal Government will meet its needs for national security and emergency preparedness (NS/EP) communications today and in the future. The NGN will offer significant improvements for NS/EP communications as bandwidth and software continue to improve, but the transition to the NGN presents challenges for ensuring the security and availability of NS/EP communications. Although the complete network evolution is expected to take many years, the process is well underway. It has become clear that the scale, scope and character of the NGN will fundamentally change the way NS/EP communications are planned for, prioritized, and ultimately delivered. It is critical that this issue be addressed.

KEYWORDS: EP communications, NS communications, Next Generation, Networks.

INTRODUCTION

The market for information and communications technology is currently undergoing a structural change. The classic telecommunication networks were planned and implemented for the transfer of specific data such as telephone calls or pure data packages. The recent growth in competition, new requirements for the market and technological developments have fundamentally changed the traditional attitudes of the telecommunications industry. The present industry is characterized by the rapid growth of broadband connections, the convergence processes of various network technologies and the emergence of a uniform IP standard for individual and mass communications [1].Traditional telecommunications operators find themselves confronted with a host of new challenges. In particular, their previously successful fixed-network business is coming increasingly under pressure. New communication possibilities, such as telephoning via the Internet, and also growing market shares in mobile telephony are causing a great deal of Concern. To counteract these losses, the network operators are investing more strongly in the growth driver, broadband. The bundling of phone, Internet and television – known in the telecommunications industry as Triple Play Services – has moved into the limelight of these new business models. The traditionally familiar market boundaries between fixed networks, mobile telephony and data networks are disappearing more and more quickly [2]. This gives the customer the advantage that he can call on an extremely wide range of services, regardless of his access technology. This development requires a Meta infrastructure beyond the existing, subordinated networks a core network for all the access networks. This new network is called the Next Generation Network. The Internet Protocol is the most significant integration factor because it is available globally and, at least in principle, it can use almost all the services and applications in all the networks.

REQUIREMENTS for Next-Generation RADIO ACCESS

Next-generation radio access is expected to provide a 1 Gb/s or less data rate under station-ary conditions and about a 100 Mb/s data rate under vehicular conditions. A personal area network (PAN) is used for short-distance, stationary communications. The other types are candidates for middle-distance, mobile communications. Wide frequency band operation and high spectral efficiency are needed for data transmission rates over 100 Mb/s. Low latency and flexible operations are also needed for multi-media services. Furthermore, all users should be able to easily receive services under various conditions. We summarize the requirements for next-generation radio access below and describe some techniques for satisfying these requirements.

1) High peak data rate operation
•Wide frequency band operation
– Orthogonal frequency division multiplexing (OFDM)
•Improvement of spectral efficiency (more than 5 b/s/Hz)
–Multiple input multiple outputs (MIMO) multiplexing
– Higher-order modulation
• Improvement of data rate at the cell-edge
– Low-rate channel coding
– Interference coordination/cancellation
– Transmitter beam-forming/adaptive array antenna reception
2) Multimedia operations

***Corresponding Author:** Arash Kalami, Department of Electrical Engineering, Urmia Branch, Islamic Azad University, Urmia, Iran. Email: Ar.kalami@gmail.com

• Realize low-delay and highly reliable radio transmission using error control techniques.
– Hybrid automatic repeat request (HARQ)
• Enable flexible allocation of radio resources according to the required transmission rate and QoS.
–Orthogonal frequency division multiple access (OFDMA)
– Frequency and time domain scheduling 100 km/h (preferably, a maximum of approx-station executes the frequency and time domain scheduling and dynamically allocates subchannels to the users. OFDMA improves the average channel quality between the base station and mobile terminals, which in turn improves total cell throughput. OFDMA has been adopted by the IEEE as standard 802.16e (mobile WiMAX) and is also under discussion at the 3GPP LTE as one of the most promising candidates for the new radio access scheme [3-5].

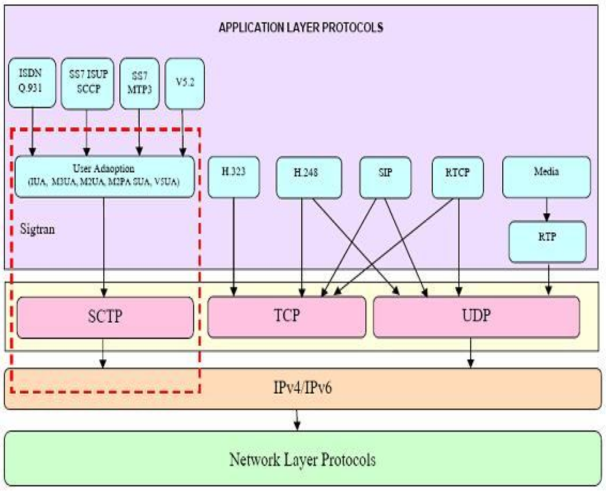

Fig. 1 protocol stacks for NGN

NGN Protocols

NGN architecture is characterised by the separation of service, transport and control layers, which are inter connected by open interfaces and use standards protocols. Legacy TDM networks are interconnected with NGN via interfaces based on open standards and protocols [2].
This paper on 'NGN Protocols' describes some of the standard protocols used in NGN architecture.
A protocol is set of rules that govern the control connections, HTcommunicationTHs and HtdataTH transfer between two computing devices. A protocol stack denotes a specific combination of protocols that work together. As shown in Fig 1.

TIMING IN NGN SERVICES

New forms of timing requirements are emerging for IP services and Ethernet transport, where timing is a critical enabler for the implementation and assurance of Quality of Service (QoS) in NGN. Some of these requirements are discussed below.

Next-Generation SERVICE ARCHITECTURE

Intense competition is expected in the information networking arena over the next 5-10 years. As the competition increases, it will be essential for companies to position themselves appropriately to take advantage of their core competencies and to prepare for the emerging telecommunications environment. In this competitive environment, mergers, alliances, and the onslaught of new entrants into the market have service providers struggling to find innovative ways to retain and/or attract the most lucrative subscribers. Today's service providers are striving to differentiate themselves within this expanding competitive landscape by searching for ways to brand and bundle new services, achieve operational cost reductions, and strategically position themselves in relation to their competition. The top 15% of today residential subscribers in the US are said to account for about 95% of carrier profits! Thus, many service providers are looking to Next Generation Network (NGN) services as a means to attract and/or retain the most lucrative customers. As shown in Fig 2.

QoS ASSURANCE FRAMEWORK

The backbone of the QoS assurance framework consists of recording and collecting the events raised by the platforms implementing the JAIN APIs. Central to this framework are event collection and aggregation applications (ECAs) which will register with the JAIN platforms to be notified of the events generated by the platform. The ECAs will then receive a stream of JAIN events generated by the platform. This raw stream of events will be aggregated in two ways. In the first type of aggregation, event counts for different types of events will be generated for a specified interval. For example, an event count indicating the number of call origination attempts over a 30 minute interval may be generated.

The events generated from a single session will be aggregated to track the progress of the session. These aggregated events may be subject to various types of analysis to assess the quality of the services provided by the various applications and the JAIN platform. Some of these analyses types include:

Performance and dependability analysis: Aggregation of events from a single session will allow us to determine the performance of the service requested by that session. Also, the number of successfully completed service requests for a given service will provide a view of the reliability of that service.

Statistical anomaly detection: Event counts of different types of events will enable us to obtain a view of the expected number of each type of service requests over a specified service interval. A departure from this
Expectation can then be detected as an anomaly.

Pattern based misuse detection*:* Pattern based misuse detection seeks to detect abnormalities by observing

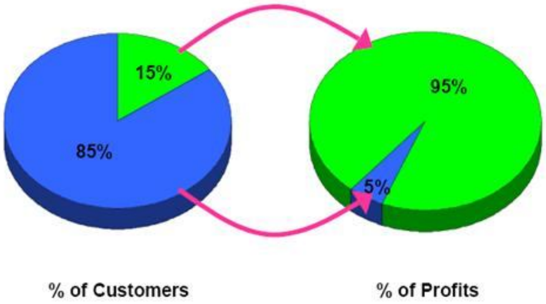

Fig. 2 Carrier profiles from residential Comments in US

Known patterns of anomalous behaviour such as calls originating from a given set of numbers. Analysis of the events from a single session can enable us to observe such known patterns and detect intentional or unintentional misuse[10].

Choice of Signalling Protocols

Numerous different signalling protocols have been developed that are applicable to a VoIP solution. They include

- Device control protocols such as H.248 (Mega co), MGCP, NCS, etc
- Access services signalling protocols such as SIP, H.323, etc
- Network service signalling protocols such as SIP, SIP-T, BICC, CMSS, etc

The choice of which protocol to use in a service provider network is dependent upon both the service set being offered and the equipment available to provide these services. For example a network must support SIP in order to provide access to SIP phones.

DENIAL OF SERVICE

A denial of service attack prevents legitimate users of a network from accessing the features and services offered by that network. Denial of service attacks is extremely difficult in the PSTN but all too common in IP networks. There have been several successful attacks on web servers on the Internet, even including the high security government sites.

In a complex network, there are many possible denials of service attacks. Some examples include sending false signalling messages so that a call agent is fooled into believing that a party has gone on-hook, bombarding a device with pings or other packets so frequently that it has no spare processing power to process legitimate requests and hacking a Subscriber Gateway to send ftp or other data traffic as high priority voice traffic.

THEFT OF SERVICE

Theft of service attacks are aimed at the service provider, where the attacker simply wants to use a service without paying for it. The most common form in the current PSTN is called subscriber fraud, where a subscriber sets up an account with a service provider using false billing information, for example a stolen credit card. Other forms of theft are more technical, often utilizing black boxes or similar to fool the network into providing free service. It is interesting to note that fraudulent long-distance calls were more common when the network used in-band DTMF signalling which could be mimicked using a blue box.

Even in a VoIP access network using for example DSL, bandwidth is still a limited resource especially the low packet loss and jitter required for good voice quality. Therefore, the network needs to be protected from subscribers misusing this high-priority bandwidth, one example would be if two SIP User Agents could set up a direct call between them, accessing the high priority bandwidth but bypassing the SIP Server(s) and hence not get billed.

INVASION OF PRIVACY

Subscribers to the PSTN expect that their calls are private, and that no third party can eavesdrop (with the exception of lawful interception). The PSTN achieves this privacy mainly by physical security mechanisms i.e. the wire from a subscriber's home is only connected to the local exchange or digital loop carrier and cannot easily be accessed.

This is not necessarily the case with VoIP networks; in particular cable and wireless networks use a shared media which allow eavesdropping unless encryption is used. However it is important to note that there is no one size fits all approach to security for VoIP, for example networks that use an ATM based DSL access are fundamentally point to point networks and for these networks encryption is unnecessary provided that the core network is suitably secured.

A LAYERED APPROACH

Instead of a technical or architectural focus, we recommend the framework be approached from an activity-based-solution perspective so the operator can control each layer within a comprehensive security framework. As shown in Figure 1, the complexity is high and security must be addressed at every layer and at each step of every layer. As shown in Fig 3.

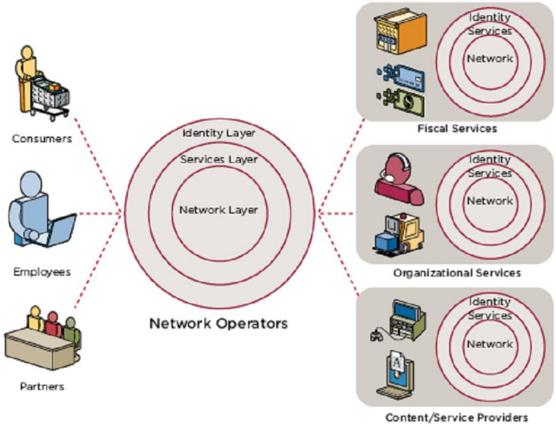

Fig 3: Later in NGN

Identity Layer and Security Level 1 (S-1)—this layer is concerned with the management of customer identities and forms the basis for interaction between the network operator and the end user. As the primary gateway, it serves as a mechanism for acceptance or exclusion, i.e., who should be allowed, what devices should be prohibited, etc.When a subscriber logs on to an operator’s portal, the operator must authenticate the identity of that subscriber. The operator also must help ensure that the device used to connect to the network is free from malware and in compliance with security guidelines for accessing services. The integrity of the code and application that is running on mobile devices is of paramount importance. The operators need to allow only trusted code and applications to be downloaded to the mobile devices. The Identity Layer and S-1 is the first line of defence, so any viruses or worms must be thwarted at this level, as well as strict controls in the form of device and application security policies enforcement must be exercised.

Service Layer and Security Level 2 (S-2) The Service Layer and its corresponding security level define the content and services allowed based on the subscriber’s access rights and privacy and preference settings. Instead of asking their customers to trust an assortment of third-party content providers, network operators may instead offer a method of access to a library of content and services (off-portal access) that does not require the subscriber to register with each provider individually. At this layer, the operator would also provide the infrastructure for pay-per-use billing so no additional financial and personal information is requested from the subscriber. When the operator (a known, trusted quantity) acts as the mediator; it protects the privacy and enhances the loyalty of the subscriber, thereby increasing the likelihood that a transaction will not be abandoned. By addressing security and privacy issues, operators are likely to see broader service adoption facilitating new revenue generation and improved customer loyalty.

Network Layer and Security Level 3 (S-3)—this layer can also be referred to as the core network. While somewhat less dynamic than the other two layers, the technical interactions between the network operator and the actual delivery of services are determined here. This layer opens up the network to third-party service applications, enabling application developers to develop, deploy, and manage service applications through the use of common open-standard application program interfaces (APIs), which expose the underlying network functionality. While reducing time to launch new services and delivering efficiencies in managing services on an on-going basis, it presents a new set of security challenges. Security at this layer defines the trust relationship between the operators and a variety of third-party content and service providers, ability to accept trusted software content and programs, and helps ensure overall security of the infrastructure that is delivering these services (e.g., location-based Services, PTT services and access to gaming sites) by leveraging core network functionality including Operations Support System (OSS) and Billing.

CONCLUSION

The market for telecommunications services in Europe has developed extremely dynamically since being liberalized. However, a weakening of the average annual growth on the various markets is to be expected by the end of the decade. The business with broadband connections is being treated as particularly lucrative in order to compensate for the market-share losses of the fixed network in particular. The network operators are attempting to provide a more efficient and cost-effective provision of services with the current conversion of the entire network infrastructure to IP technology. The aim is to unite fixed, mobile and data networks together and so to provide various services via a transparent network –the so-called Next Generation Network. The core of all communications services will then be a single platform, based on the Internet Protocol. The established network operators in particular are hoping for operating-cost savings of several billion euros per year from the reduction of the many different platforms.

Finally, there are still general doubts about how the successful business models of the future will look. A decisive factor will be the clear superiority of convergent end devices and services compared to the existing offers. The selective positioning of convergent services on the market will be crucially important to convince the customers of the added value. The successful development of NGN will presumably depend primarily on the close cooperation between network operators, system manufacturers and research institutions.

REFERENCES

1.V. Paxson, G. Almes, J. Mahdavi, “Framework for IP Performance Metrics”, RFC 2330 , May, 2008.

2.Handley, H.Schulzrine, E.Schooler, and J.Rosenberg, “SIP: session initiation protocol”, RFC 2543, March 2009.

3.V. Raisanen, G. Grotefeld, A. Morton, “Network Performance Measurement with periodic streams”, RFC 3432, November, 2002.

4.C. Demichelis, P. Chimento, “IP Packet Delay Variation Metric for IP Performance Metrics (IPPM)” RFC 3393, November, 2011.

5. R. Koodli, R. Ravikanth, “One-way Loss Pattern Sample Metrics”, RFC 3357, August, 2008.