Communication in Change – Voice over IP in Safety and Security Critical Communication Networks

Heimo Zeilinger, Berndt Sevcik, Thomas Turek, and Gerhard Zucker

Vienna University of Technology, Institute of Computer Technology,
Gusshausstr. 27-29, 1040 Vienna, Austria
{zeilinger,sevcik,turek,zucker}@ict.tuwien.ac.at

Abstract. During the last decade communication technology has changed rapidly. Due to its decreasing costs and rising expansion, IP (Internet Protocol) technology has found its way to areas that have long been the domain of public-switched telephone networks (PSTN). Voice over IP (VoIP) applications are widely used not only for phone calls or common Internet conferences, but also tend to be used for safety critical communication applications. Hence security and safety topics arise, which pose new challenges in this area of research. The authors are convinced that new issues on the network layer as well as on the application layer require detailed analysis. Hence this paper gives an overview on latest developments in this area, and states the authors' view on this topic. Thereby safety and security issues are faced from different abstraction layers. On the one hand the network layer and on the other hand the application layer focusing on middleware systems in the area of service oriented architectures (SOAs).

Keywords: VoIP, communication networks, safety, security.

1 Introduction

Within the last decade VoIP benefited from the massive expansion of IP networks and related decrease in acquisition and operation costs. Today a trend towards the use in public safety communication networks can be identified. Because the quality of a call is mainly influenced by delay and jitter, the current development implicates new challenges in safety and security which have to be faced.

The term safety describes the ability of a system not to cause environmentally harming events, due to loss of mission critical information – e. g. signaling and media transport in VoIP – under normal and exceptional operations. The term security deals with authentication, authorization, integrity, confidentiality and non-repudiation.

Especially in areas of public safety a packet loss of the voice and signaling stream can result in safety critical events. On the other side the access of unauthorized users who may cause safety issues have to be handled.

This paper gives insight into safety and security in critical communication systems regarding two different abstraction layers - the network and the application layer. As the network layer includes issues typical for IP networks like network failure or security gaps, the application layer has to be investigated towards the use of service

M. Ulieru, P. Palensky, and R. Doursat (Eds.): IT Revolutions 2008, LNICST 11, pp. 186–193, 2009.

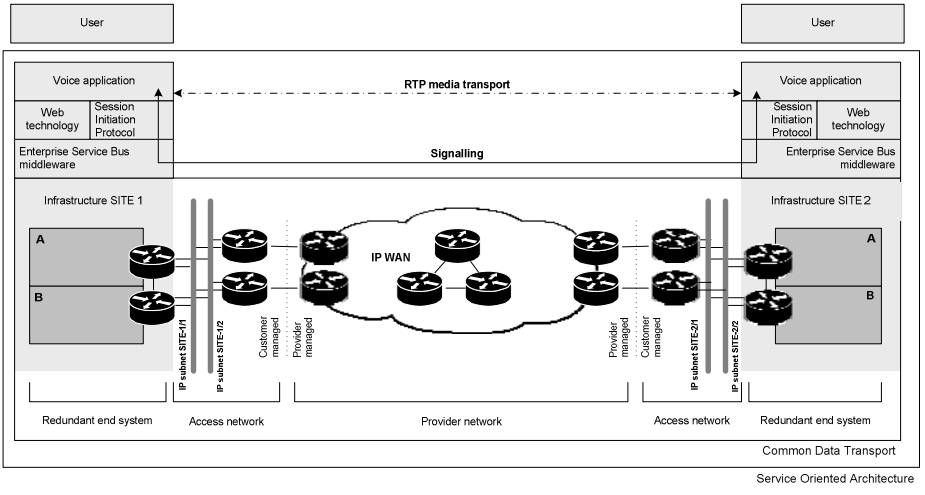

Fig. 1. Service oriented architecture for a safety capable voice service

oriented architecture (SOA). Current developments show a trend towards the use of middleware in order to loosely couple applications and services from their underlying transport system.

Figure 1 sketches different sections of a VoIP communication line which will be in the focus of discussions of this article as well as from the authors' point of view in future evolvements. Figure 1 assumes the use of Internet conferencing architecture protocols – e. g. Real time Transport Protocol (RTP), Session Initiation Protocol (SIP), Session Description Protocol (SDP) standardized by the Internet Engineering Task Force (IETF) – for organizing a VoIP session. Latest developments like the use of SIP by the 3rd Generation Partnership Project (3GPP) for the IP Multimedia Subsystem (IMS) [1] suggest the assumption that SIP increases its impact to the area of VoIP applications.

Contrary to IP, PSTNs already provide a high level of availability to its users. There is no need to develop new standards or mechanisms in order to achieve availability of five nines (99.999% availability) – PSTN already provides this availability for voice communication. RTP, which is used for the payload data transfer in VoIP sessions, bases on the connectionless User Datagram Protocol (UDP) and therefore does not guarantee any reliability or ordering of data packets. Failures on packet transmission can cause considerable interrupts of the voice signal like delayed delivery or loss. IP networks have to be highly available in order to provide safety and need to block any unauthorized access.

Hence, the question has to be asked if the use of VoIP in safety critical systems makes sense if this development is affiliated with a number of problems – the use of VoIP in the area of public safety communication systems seems to be paradox. The reason for its use involves economic considerations as well as service compatibility. Combining different kinds of services on technologically identical networks saves maintenance and operational costs to the operating company respectively the user. In addition, current commercial off -the-shelf (COTS) equipment shows performance to

fulfill the requirements for designing highly available and fast reacting networks. Hence the development heads towards critical voice communication over IP and we have to face all related safety and security issues. This paper discusses these issues and gives insight to authors' point of view on this topic regarding the transport layer as well as the application layer.

2 Network Layer

Since the Quality of Service (QoS) of VoIP relies on the underlying network, this section is about upcoming safety and security issues. In the following, the access network as well as the provider network – shown in Figure 1 – are discussed separately.

2.1 Access Network

The access network represents the connection between the end-system and the provider network. As mentioned above Internet conferencing architecture protocols do not ensure reliable data packet delivery, because it would cause transfer delays. Nevertheless, high network availability – five nines regarding to availability and reliability standards of the Eurocontrol [2] – as well as low convergence time has to be ensured. Even though five nines of availability correspond to a network downtime of about five minutes per year, a sub-second failover time as a maximum has to be achieved in safety critical communication networks, that is, the network can at most fail five minutes per year, but must never fail for more than one second at any given time. Typical IP protocols suffer from poor failure detection times and provide a failover time far above one second due to conservative timing parameters. Technologies like the Resilient Packet Ring [3] on the one hand and proprietary and on the other hand similar protocols like HiPER-Ring [4] or EAPS [5] show convergence behavior far beneath one second. However the requirement of specific hardware or the binding to manufacturers wipe out the advantage of using cheap COTS components and standardized protocols.

In Sevcik et al. [6] different ways to reach low convergence times for the access network represented in Figure 1 have been investigated. The maximum network convergence time is specified with 200 ms. Hardware redundancy is applied to the access network. Using different providers would additionally require proper coordination and an identical IP address plan of both. As Layer-2 protocols are known to show slow network convergence, Layer-3 protocols are investigated for this task within the access network. While protocols like OSPF or IS-IS show convergence times above one second in worst case scenarios it is verified that the combination with the bidirectional forwarding detection (BFD) speed up the network convergence to 160 ms. BFD was launched in 2004 by the IETF for controlling connectivity in the forwarding path and provides failure detection in single-hop, multi-hop, and end-to-end scenarios. In addition, BFD avoids the problem of hiding link breakdowns to the end-system by layer-2 nodes. Sevcik et al. showed that low convergence times can be achieved even thought timing parameters are defined on the side of conservatism due to a software implementation of BFD. The authors' state that the use of BFD allows configuring lower timing parameters and resulting in further decrease of the network convergence

duration. Even thought BFD supports short timing parameters, stability issues have to be kept in mind. In [7] it is stated that a reduction may result in higher jitter of the detection time and an increased failure probability by declaring a node as down. BFD is currently released as a draft. However, the authors advance the view that it will become an IETF standard soon. BFD seems to be a step towards low failover times.

2.2 Provider Network

This section discusses upcoming safety and security issues by outsourcing the backbone network to a provider. In Figure 1 the provider-managed network – also called provider network – is symbolized by a cloud. It is characterized by a black box, because the customer has no possibility to modify it. As the customer manages the access network, the SIP registrar, proxy, redirect servers, and the end system, the core network is managed only by the provider. Even though security services like the management of firewalls or virtual private networks (VPN) and the monitoring of QoS can be outsourced to the customer, the provider still has to arrange the routing mechanisms and network security. Sevcik et al. [6] assumed a network failover time of 200 ms for the access network in order to ensure an adequate voice information transfer. The provider network has to match these requirements by guaranteeing a low network failover time using common IP technology.

In circuit switched networks for safety critical communication systems – e. g. air traffic control – routing is generally performed by fixed alternative routing (FAR) algorithms. These algorithms show stability and usability in loosely meshed networks. Failures are handled by redirecting data packets over fixed and predefined direct or alternative routes. Even thought FAR algorithms show some issues in case of multiple simultaneous failures [8] for the use in safety critical communication networks they are preferred to dynamic routing algorithms (DAR). DARs show high complexity and require fully meshed networks to ensure performance. Looking at VoIP, packet switched technologies have different routing requirements. Network protocols generally implement dynamic routing algorithms and therefore implicate avoidable complexity – avoidable regarding safety critical communication networks which generally base on few network nodes compared to commercial provider networks. Multi Protocol Label Switching (MPLS) is a data-carrying mechanism commonly used in core networks. In general it is combined with an Interior Gateway Protocol (IGP) and achieves stability in operation but lacks in network convergence time.

Security is another issue the provider has to deal with when providing a core network for safety critical VoIP communication. Network administrators as well as providers try to protect their networks against unauthorized access and attacks. Distributed denial-of-service (DDoS) attacks represent common threats where the intruder causes a denial of service by attacking a single target within the network. The resulting service downtime has direct influence on safety issues in a safety critical communication system. A possible solution would be to physically separate the safety critical network from the common Internet and therefore eliminate an access from the outside. Hence, the provider has to avoid contact between both networks by directing the traffic over separated infrastructures in the network nodes. This seems to be highly sophisticated and it is questionable if any provider can give a guarantee on a complete

physical separation. Additional complexity is introduced by providing a redundant path to the main path like it is done in circuit switched networks to increase network availability. Not only the common IP network has to be separated from the critical VoIP network but also two sub networks have to be introduced. In an ideal case both networks are conducted over different network nodes in order to evade a system breakdown in case of a catastrophic event. One solution would be to use different providers for both sub networks. Beneath additional management of failover procedures and IP address plans it cannot be ensured that different providers will not intersect each other's network at any point.

From the authors' point of view the most likely way to cope with these issues is the construction of an IP network for safety critical VoIP applications without provider infrastructure. Otherwise the listed requirements can hardly be achieved. Even though already available infrastructure cannot be used and upcoming developing costs rise, the advantage of using a uniform and widespread technology, which allows the bonding of numerous services, remains.

3 Service Oriented Architecture in Communication Systems

Trends in telecommunication systems show a convergence of different forms of communication and supporting applications. The idea is building a global Next Generation Network (NGN) based on top of IP [9]. The main challenge of today's companies is to get different platforms together and exchange data when required.

3.1 Overview

SOA [10] defines a type of architecture that abstracts the transport itself to a service definition and can be seen as development of Component Based Architecture (CBA). The service definition targets need to build loosely coupled, standard based, protocol independent and location transparent software components. Services communicate with each other using messages and allow the coordination of activities between them. Business processes are modeled by composition of distributed services shared through a network.

The term service is often confused with Web Service (WS). A WS can be seen as a possible connection technology of SOA. WSs are often used, but do not represent the only possibility for service integration and definition of new services. Services are made accessible by using standard Internet protocols. WSs will play a big role in future VoIP implementations by offering voice communication platforms out of the web browser. Therefore different implementation approaches exist proposing dual (WS using HTTP and SIP) and single stack solutions (purely WS based) [11].

A large part of SOA concepts focus on the implementation of a hub-and-spoke integration pattern realized as an Enterprise Service Bus (ESB) [12]. The ESB represents a Message Oriented Middleware (MOM) allowing simple integration and re-use of business components by the use of open standards. It provides all necessary services like connectivity, message routing, data transformation and adoption to different applications to allow interaction of different distributed resources supporting mediation and orchestration of them. Beside the transport network the software components

(e.g. message router, component framework, management) implementing the ESB functionality introduce additional safety critical aspects to the system. Safety has to be considered on distinct levels like message, service or infrastructure. Message transport, service discovery and service interaction are only a few of the many possible safety related issues. It is important that data and events are sent to the right consumer within the required time constraint. Reliable message exchange is needed. It is also of importance that services are available even if components in the network will fail. The ESB infrastructure has to address the problem of isolating faults caused by server and communication infrastructure. Distributed, reliable and available ESB systems need to be developed to allow the usage in safety critical application fields.

Looking at Air Traffic Management (ATM) as a safety critical application area for voice integration, we see that big effort is made to challenge the increasing air traffic capacity demands and enhance safety and security at the same time. The Federal Aviation Administration (FAA) is designing a System Wide Information Management (SWIM) combining data from different sources e.g. flight and flow data, weather information and surveillance using the principles of SOA. In Europe the SESAR project was defined to build the next generation air transportation system where SOA is described as a suitable paradigm to allow Collaborative Decision Making (CDM) [13] by the use of COTS communication and middleware standards. Standards are currently defined to guarantee safe and secure ATM interoperability with VoIP [14]. This paves the path to integrate VoIP services to a SOA based communication network.

This safety critical application field is a good example for lots of other convergence activities, where voice and data converge into a single service capable network. The integration of voice service allows the forwarding of signaling information to a business process management system (BPMS) which handles the call. Service definitions will support presence, call routing, alert generation and data collection. The couplings with other information systems help the operator to make quick and accurate decisions using a clear user interface. Improved workflows and more efficient operations are achievable using intelligent process modeling to build clear situational awareness. Safety objectives identifying minimum requirements to be achieved by the ESB system need to be specified for the different system elements. Consequences by inserting an additional software abstraction layer encapsulating the packet transport have to be investigated carefully to conform to the strict safety requirements.

3.2 Security Issues and Concerns

SOA as an architectural paradigm and discipline for analyzing, designing and implementing distributed systems not only has advantages with respect to efficiency, flexibility and interoperability but also disadvantages in terms of security. Issues and concerns are often disregarded, although they play an important role when talking about safety critical voice and data communication in the field of ATM.

Due to its distributed hardware and software structure, open and manufacturer-specific (proprietary) interfaces, protocols and formats, SOA has new and more comprehensive demands on security with respect to identification, authentication, authorization, confidentiality, integrity and non-repudiation. One by one can be investigated from the perspective of a user and a service. To deal with SOA specific and non-SOA

specific requirements, threats and vulnerabilities of valuable assets and liabilities security has to be implied on several levels [15].

In the past, security mechanisms were concentrated on the transport layer. There the security standard Transport Layer Security (TLS) [16] works fine. TLS is wide-spread and its predecessor Secure Socket Layer (SSL) is e. g. used for securing SIP based VoIP communication [17]. However, problems remain with its use in SOA. TLS offers point-to-point security but no end-to-end security. This, however, is the requirement of SOA. The messages are protected only on the transport level. Therefore, security cannot be ensured after the arrival in the end-system. In SOA a message is sent over several intermediary services, which may operate on individual elements of this message. That is the reason why security needs to concentrate on the message level.

The stated weakness of a SOA has to be confronted with new and promising approaches. In other words, a SOA must be supported by a security framework, which reacts to a considerable degree on the varying requirements of the service environment. Hence, a security architecture including identity, authentication and authorization management, intranet, extranet and Internet security, registry security, Universal Description, Discovery and Integration (UDDI) security and messaging security has to be considered [15].

Although a few security requirements can be met with these mechanisms, many are not solved. Though there are many standards e. g. eXtensible Markup Language (XML) [18] and WS security frameworks promoted by World Wide Web Consortium (W3C) [19] and Organization for the Advancement of Structured Information Standards (OASIS) [20], where and how these solutions are applied in a SOA still need further research.

4 Conclusion and Outlook

Reusability and standardization are the direction to which voice communication is heading. We have listed the benefits of this development by using VoIP, but one must not forget the possible fallacies when doing so: when making elementary changes to a technology, the quality of the new system needs to be at least as good as the already available quality. This requires us to think about reliability and availability as well as the voice communication quality itself in terms of delay and distortion. From what we see today VoIP is the way to go and will bring technological benefits as well as cost reduction to providers and customers. But only if we are able to provide at least the same quality as we have today, we will see commercial success and thus replacement of existing technologies. Safety critical areas of voice communication have even higher requirements and in order to meet these requirements, we need detailed analysis of all related technologies.

As a consequence of the convergence of data and voice we are faced with new requirements in the architecture that is capable of enabling this convergence. Moving towards services looks promising and the proposed SOA paradigm is a candidate solution. But again, we must not forget that beside all benefits that we get from this new convergence, the quality that is provided to the user has to remain the same, if not increase.

References

1. Group Services and Systems Aspects: IP Multimedia Subsystem (IMS), Stage 2, 3GPP TS 23.228 Technical specification, Release 7, Version 7.7.0 (2007)
2. European Organization for the Safety of Air Navigation: Voice Communication Procurement Guidelines (2003)
3. IEEE Standard: P802.17-2004 Resilient Packet Rings (2004)
4. Schaub, M., Kell, H.: Produkt-Analyse: HiPER-Ring vs. RSTP Redundanzverfahren mit Hirschmann Switches, ComConsult Research (2003)
5. Shah, S., Yip, M.: Extreme Networks' Ethernet Automatic Protection Switching (EAPS) Version 1. IETF Request for Comments 3619 (2003)
6. Sevcik, B., Zeilinger, H., Zucker, G.: High Available and Reliable IP-Networks for time-critical Voice over IP Applications (to be published)
7. Cisco Systems, Inc.: Cross-Platform Release Notes for Cisco IOS Release 12.0 (28d) (2006)
8. Rausch, T., Zeilinger, H., Kaindl, A.: Routing Performance in Air Traffic Services Networks. In: Proceedings Seventh International Conference on Networking, pp. 669–674 (2008)
9. Blum, N., Magedanz, T.: Requirements and components of a SOA-based NGN service architecture. Elektronik and Informationstechnik, Ausgabe 7–8 (2008)
10. Papazoglou, M.P., van den Heuvel, W.H.: Service oriented architectures: approaches, technologies and research issues. VLDB Journal (2007)
11. Chou, W., Li, L., Liu, F.: Web Services for Communication over IP. IEEE Communications Magazine (March 2008)
12. Ning, F., Xingshe, Z., Kaibo, W., Tao, Z.: Distributed Enterprise Service Bus based on JBI. In: 3rd International Conference on Grid and Pervasive Computing (2008)
13. Eurocontrol: SESAR project, `http://www.eurocontrol.be/sesar/`
14. EUROCAE: European Organization for Civil Aviation Equipment, `http://www.eurocae.eu/`
15. Stephens, B.: Security architecture for system-wide information management. In: 24th Digital Avionics Systems Conference (2005)
16. Dierks, T., Allen, C.: RFC2246-The TLS Protocol Version 1.0, Network Working Group (1999)
17. Butcher, D., Xiangyang, L., Jinhua, G.: Security challenges and defense in VOIP Infrastructures. IEEE Transactions on systems, man, and cybernatics – Part C: Applications and reviews 37(6), 1152–1162 (2007)
18. Bray, T., Paoli, J., Sperberg-McQueen, C.M., Maler, E., Yergeau, F.: Extensible Markup Language (XML) 1.0, 4th edn., W3C (2006)
19. W3C: World Wide Web consortium, `http://www.w3.org/`
20. OASIS: Organization for the Advancement of Structured Information Standards, `http://www.oasis-open.org`