Reliability Engineering and System Safety 96 (2011) 1627–1636

Contents lists available at SciVerse ScienceDirect

Reliability Engineering and System Safety

journal homepage: www.elsevier.com/locate/ress

Semi-Markov modeling of dependability of VoIP network in the presence of resource degradation and security attacks

Vandana Gupta [1], S. Dharmaraja *

Department of Mathematics, Indian Institute of Technology, Delhi, India

ARTICLE INFO

Article history:
Received 19 August 2010
Received in revised form
26 July 2011
Accepted 2 August 2011
Available online 25 August 2011

Keywords:
VoIP
Software rejuvenation
Semi-Markov model
Dependability attributes: availability, reliability and confidentiality

ABSTRACT

Nowadays VoIP has become an evolutionary technology in telecommunications. Hence it is very important to study and enhance its dependability attributes. In this paper, an analytical dependability model for VoIP is proposed. The study is focused on analyzing the combined effects of resource degradation and security breaches on the Quality of Service (QoS) of VoIP, to enhance its overall dependability. As a preventive maintenance policy to prevent or postpone software failures which cause resource degradation, software rejuvenation is adopted. The dependability model is analyzed using semi-Markov process which captures the effects of non-Markovian nature of the time spent at various states of the system. The steady-state as well as the time-dependent analysis of the dependability model is presented. The steady-state results are obtained analytically, whereas the time-dependent results are obtained from simulation. Also, the analytical model is validated via simulation. The model analysis using a numerical example indicates the feasibility of our approach. Various dependability attributes such as *availability*, *reliability* and *confidentiality* are also obtained. A comparative study is also done between our proposed model and the existing models.

1. Introduction

Voice over Internet Protocol (VoIP), also known as Internet telephony, is the technology that enables people to use the Internet as the transmission medium for voice communications. It is a technology that allows to make voice calls using a broadband Internet connection instead of a regular (or analog) phone line. It has been evolving quite rapidly in the telecommunication area in recent years as it provides long distance calls at a very low cost [1]. Hence, it is essential for well-designed VoIP networks to be reliable and safe, to meet certain quality-of-service (QoS) requirements, and to provide its services in a timely manner, in the wake of resource degradation and also in the context of intrusions, attacks and accident failures in a hostile environment. Therefore, the main focus of this paper is on the QoS of VoIP in the case of resource degradation and security breaches to improve its availability, reliability and safety. The QoS issues (availability, reliability, security) addressed in this paper can be considered as a *dependability* issue. Dependability is global concept that subsumes the usual attributes of availability, reliability, security, integrity, maintainability, etc. [2,3]. The consideration of security brings in concerns for confidentiality, in addition to availability and reliability.

Network dependability is an important issue for service providers, vendors, and users. A lot of research has been done on the area of network dependability. A survey on the existing model-based techniques for evaluating system dependability is done in [4], and it is summarized that how these techniques can be extended to evaluate system security. A comparative study on the analytical models of computer system dependability and security is carried out in [5]. The paper [6] outlines the details of how redundancy may be implemented by making enhancements to the basic IEEE 802.11 channel access protocol. In this paper, the authors have presented the reliability, availability and survivability analysis of the two configurations to evaluate the dependability of the network under study, and compared them with the scheme with no redundancy. In [7], a comprehensive dependability analysis of WLAN for system dependability measurement, modeling and evaluation is presented, and methods are suggested to increase the communication link reliability and availability of wireless LANs. An integrated solution to increase the dependability of wireless mesh networks (WMNs) is proposed in [8]. The approach in this paper combines network coverage planning on the physical layer, bandwidth management on the link layer and live network monitoring to improve the reliability, availability and maintainability of a WMN. Hence, we can see that

* Corresponding author. Tel.: +91 11 26597104; fax: +91 11 26581005.
E-mail addresses: vandana_iitd@yahoo.com (V. Gupta), dharmar@maths.iitd.ac.in (S. Dharmaraja).
[1] Current affiliation: Department of Applied Mathematics, Delhi Technological University, Delhi.

0951-8320/$ - see front matter © 2011 Elsevier Ltd. All rights reserved.
doi:10.1016/j.ress.2011.08.003

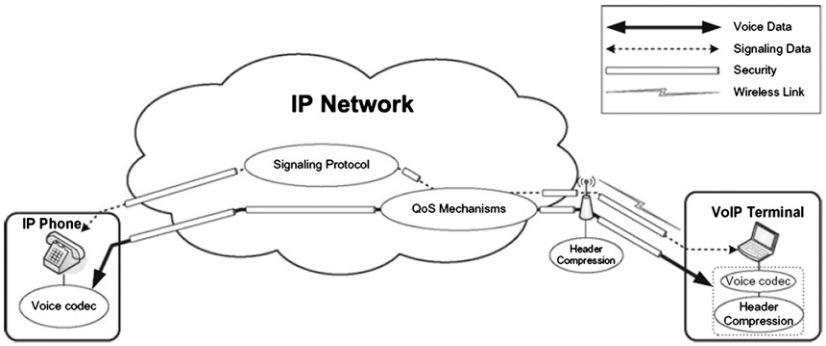

Fig. 1. General VoIP architecture.

a considerable amount of work has been conducted over the past decade on dependability issues in traditional networks [9]. However, to the best of our knowledge, a general analytical framework for dependability of a VoIP network has not been developed till date.

The general VoIP architecture [1] is depicted in Fig. 1. As depicted in the figure, QoS and security issues are the two main concerns of any VoIP network. Service quality degradation due to resource exhaustion of the service provider is one of the major problems that VoIP experiences. VoIP provider may run out of resources when the resource demands by the users are increased in large numbers. In that case, when a call demand arises, the provider cannot serve it or even if the request is served, it may affect the quality of the ongoing calls [10]. Another most questionable aspect of VoIP is its security. Since VoIP works over Internet, it is prone to many security intrusions. VoIP packetizes phone calls (i.e., voice signals) through the same routes used by network and Internet traffic, and is consequently susceptible to the same cyber threats that plague these carriers today. Main service thefts include phreaking, eavesdropping, VoIP phishing, viruses and malware, DoS (Denial of Service), SPIT (Spamming over Internet Telephony), call tampering and Man-in-the-middle attacks [11,12]. Now, it may not be either possible or it may not be cost effective to design and implement software systems, that are guaranteed to be entirely secure. In this scenario, intrusion tolerance is a practical alternative for building secure software systems. An intrusion detection system (IDS) helps the administrators to monitor and defend against security breaches [13]. Further, an approach to overcome the problems of resource exhaustion and security attacks in a VoIP system is software rejuvenation, which can be regarded as a preventive maintenance policy to prevent or postpone software failures. It is a technique that can be periodically adopted to combat the phenomenon of software aging [10,14].

In Dong Seong Kim et al. [15], proposed a general framework of survivability model for WSN, in the context of security breaches and adopted software rejuvenation policy. A VoIP service system is considered in [16] and the effects of performing software rejuvenation in order to prevent system failures caused by resource exhaustion due to the increasing number of calls is examined. Authors in [17], have addressed a two-level software rejuvenation policy for aging in software systems. In [13], an approach is presented for quantitative assessment of security attributes for an intrusion tolerant system. In the literature mentioned above, either the software aging because of resource degradation is discussed or the security issues are handled separately, but not together. Hence, this motivates us to propose an analytical framework of dependability model for VoIP which models the QoS (availability, reliability and confidentiality) in the presence of resource degradation as well as in case of security breaches, with software rejuvenation procedure. We model this using a stochastic process based on semi-Markov process (SMP) because of the non-Markovian nature of the various events involved in the model [18]. We present the steady-state as well as the time-dependent analysis of the proposed dependability model. The results of numerical analysis indicate the feasibility of our proposed approach.

The rest of this paper is organized as follows. The proposed analytical dependability model is explained in Section 2. Section 3 deals with the steady-state analysis of the dependability model. The dependability attributes are discussed in Section 3.1. Section 3.2 gives simulative verification of the analytical model, and a steady-state numerical illustration is provided in Section 3.3. The time-dependent analysis is presented in Section 4. Finally concluding remarks are given in Section 5.

2. VoIP dependability model description

A configuration of the dependability model is depicted in Fig. 2. The figure represents a state transition diagram in which circles represent states and directed arcs represent transitions.

The states are explained as follows:

- State **P** (Perfect): This is the highly efficient and highly robust execution phase. Both rejuvenation and a repair/reconfiguration after a failure bring the system back to this state. The system works perfectly in this state and is *available* to the users. The objective of the attack resistance is to keep the system in this state as long as possible.
- State **M** (Medium efficient): This is the medium-efficient execution phase. Resource degradations start to occur in the system but they are not a threat yet. At this point, a check about the remaining resources has to be performed in order to determine whether the system needs to be rejuvenated, or the system can still serve the new calls without call quality degradation. The system still works well in this state, and is *available* to users.
- State **L** (Low efficient): In this state, the system is running at a low-efficient execution state. Some applications in the system are in the failure prone state but it is still *available*. At this point also, a check on the remaining resources has to be performed in order to determine whether the system can still serve new calls, or needs to be rejuvenated.
- States $\mathbf{C_1}$ and $\mathbf{C_2}$ (Checking states): These are the decision making states. In these states, the system is taken off line for checking, where it is determined whether the system can survive with the remaining resources, or it needs to be rejuvenated. Usually the decision is made very quickly, i.e. the sojourn time in this state is very short. The system is *unavailable* to users in these states.