An Analytical Framework of Survivability Model for VoIP

Vandana Gupta
Department of Mathematics
IIT Delhi, India
vandana_iitd@yahoo.com

S. Dharmaraja
Department of Mathematics
IIT Delhi, India
dharmar@maths.iitd.ernet.in

***Abstract*—Nowadays Voice over Internet Protocol (VoIP) has become an evolutionary technology in telecommunications, and hence it is very important to study and enhance its survivability measures. In this paper, an analytical framework of survivability model for VoIP is proposed. The study is mainly focused on analyzing the combined effects of resource degradation and security breaches on Quality of Service (QoS) of VoIP, to enhance its overall performance. Software rejuvenation methodology is adopted as a preventive maintenance policy to prevent or postpone software failures. The VoIP system is modeled and analyzed as a stochastic process based on semi-Markov model to capture the effects of time spent at various states of the system. The model analysis indicates the feasibility of our approach. In addition, a comparison is made between the performance of our model with the existing models, and it is observed that our model provides better results.**

***Keywords*-VoIP; Survivability; Software rejuvenation; Semi Markov model**

I. 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. Hence, it is essential for well-designed VoIP networks to meet certain quality-of-service (QoS) requirements, such as reliability, availability, confidentiality and performance. And there is a need for VoIP networks 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 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 confidentiality. This problem is considered as a survivability problem. Survivability of a system can be defined as the capability to fulfill its mission, in a timely manner, in the presence of intrusions, attacks, accidents and failures [1]. A considerable amount of research work has been conducted over the past decade on survivability issues in traditional network [2], [3]. In [4], a general survivability quantification approach applicable to a wide range of system architectures, applications, failure/recovery behaviors, and metrics is presented. However, to the best of our knowledge, a general analytical framework for VoIP survivability has not been developed till date.

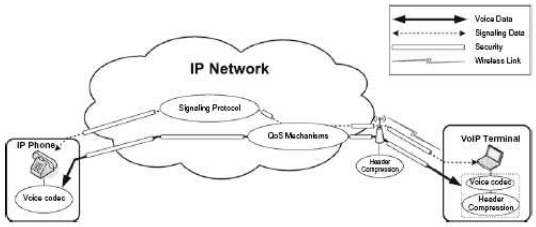

Figure 1. General VoIP architecture

The general VoIP architecture [5] 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 [6]. 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 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 [7], [8]. 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 [9]. 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 [6], [10].

In [11], Dong Seong Kim *et. al.* 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 [12] 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 [13], have addressed a two-level software rejuvenation policy for aging in software systems. In [9], 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 survivability 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 as a stochastic process based on SMP, and analyze the embedded discrete time Markov chain (DTMC) of SMP model using numerical analysis. The results of numerical analysis indicate the feasibility of our proposed approach.

The rest of this paper is organized as follows. The proposed analytical framework of survivability model is explained in section II and model analysis is followed in section III. The survivability attributes are discussed in section IV and numerical results are given in section V. Finally concluding remarks are presented in section VI.

II. VoIP SURVIVABILITY MODEL DESCRIPTION

A configuration of the framework of survivability 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.

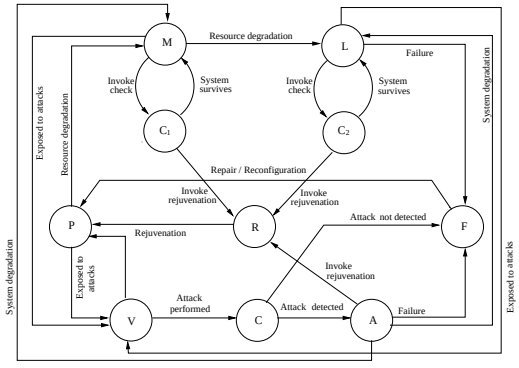

Figure 2. VoIP survivability model

- 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.
- State **V** (Vulnerable): This is vulnerable state V where the system is exposed to security breaches. This state is very critical because attackers and malicious users would want to exploit the vulnerabilities and try to make a successful attack. The system is *available* to users in this state.
- State **C** (Compromised): This is a compromised state which is reached when the system is successfully exploited by the attackers, and then unwanted damage follows. System is *available* to users in this state also.
- State **A** (Adaptation): This too is a decision making state. It assesses the impact of damages occurred because of a successful attack and determines the appropriate strategies for recovery. The system is off line here, hence it is *unavailable* to users in this state.
- State **R** (Rejuvenation): In this state, the system goes for rejuvenation, and is *unavailable* to users.
- State **F** (Failure): The system crashes in this state, and goes for repair or reconfiguration. It is *unavailable* to users in this state.

In this model, the system starts with perfect state P. At this state, when many resource requests arrive at the VoIP server and a high amount of calls are initiated, the system experiences a resource degradation, and moves to the medium efficient state M. At this point, a check on the remaining

resources has to be performed in order to determine whether the system needs to be rejuvenated, or it can still serve new calls. This check is performed at state C_1. Depending on the status of the remaining resources, the system either returns to state M where new calls arrive, or the system enters rejuvenation state R. When system returns to state M, the same call setup procedure is initiated resulting in a higher level of resource degradation and hence system enters less efficient state L. On reaching state L, the system has to be checked once again. As in state M, the system enters the checking state C_2. From here, it either transits to state R, or it returns to state L. On returning to state L, system accepts new call requests. At this state, on experiencing further resource degradation, system enters the failure state F. In this case, the system is reconfigured/repaired and returns to state P.

Apart from resource degradation, the VoIP system can be exposed to security breaches anytime. Hence, when the system is in state P, M or L, and if any kind of penetration into the resistance mechanism occurs, the system enters the vulnerable state V. If the present monitoring system can successfully detect the state, it takes necessary actions and returns once again to state P. But if the system remains in state V and a successful attack is made, it causes the system to enter the compromised state C. If the intrusion detection system can successfully recognize the compromised state, the system goes to adaptation state A, otherwise the system goes to state F, from where it goes back to state P. In state A, the impact of the damages caused due to the attack is assessed and recovery strategies are determined. The recovery actions depend on the requirement of the survivability and types of attack detected. If the critical requirements of the system are integrity and confidentiality, the system moves to rejuvenation state R. On the other hand, if the requirement is only the availability of the system, the system moves to either state M or state L. Otherwise, if the impact of attack is such that the system can no longer survive, it goes to state F. From here, the system returns back to state P after repair/reconfiguration.

Note that the resource exhaustion depends on the time that the system spends at each degradation state, and the time that the system enters a new degradation level state is not exponentially distributed [12]. Consequently, an SMP is used to model the VoIP system.

The SMP model for VoIP survivability is shown in Fig. 3. To cover real life scenarios, we consider general distributions, i.e. both exponential and non-exponential distributions, of the transitions between different states. Their cumulative distribution functions (cdfs) are shown in Fig. 3. The distributions F_2, F_3, F_5 and F_7 follow general distribution function, whereas all the other distributions F_1, F_4, F_6, F_8, ... follow exponential distribution function. Note that the time to trigger rejuvenation is of fixed duration and hence its cdf can be given as $F_3(t) = F_5(t) = u(t-r)$, where $u(t)$ is

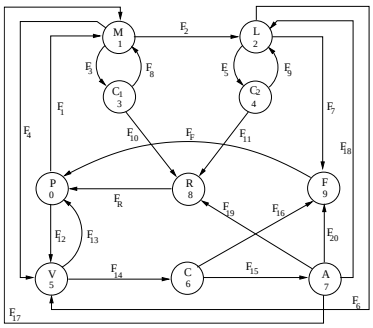

Figure 3. SMP model for VoIP survivability

the unit step function and r is the time to trigger rejuvenation [12]. The time to resource exhaustion (following general distribution F_2 and F_7) can be modeled by an increasing failure rate (IFR) distribution as the software resources are exhausted in an increasing manner with respect to the time that the system has served [14]. Each state in this model is a regenerative state, because from any state, enabling of an event will disable the occurrence of any other event from the same state, and hence at each state Markovian property is held. Therefore, the underlying stochastic process is an SMP. In the next section, we analyze the SMP model using embedded discrete time Markov chain (DTMC).

III. Semi Markov model analysis

For convenience, the ten SMP states are numbered sequentially as shown in Fig. III. The state space can be denoted as $\mathbf{\Omega} = \{0, 1, 2, \ldots, 9\}$. In this section, we study the semi-Markov model presented in Section II for the VoIP survivability model in detail. We take the two-stage method to solve the semi-Markov model [13], [15], which can be fully described by its kernel matrix $K(t)$ as follows in which $k_{ij}(t) = P\{Y_1 = j,\ T_1 \leq t | Y_0 = i\};\quad i, j \in \Omega$

$$
\mathbf{K(t)} = \begin{array}{c} \\ \mathbf{0} \\ \mathbf{1} \\ \mathbf{2} \\ \mathbf{3} \\ \mathbf{4} \\ \mathbf{5} \\ \mathbf{6} \\ \mathbf{7} \\ \mathbf{8} \\ \mathbf{9} \end{array}
\begin{array}{c}
\begin{array}{cccccccccc} \mathbf{0} & \mathbf{1} & \mathbf{2} & \mathbf{3} & \mathbf{4} & \mathbf{5} & \mathbf{6} & \mathbf{7} & \mathbf{8} & \mathbf{9} \end{array} \\
\begin{bmatrix}
0 & k_{01}(t) & 0 & 0 & 0 & k_{05}(t) & 0 & 0 & 0 & 0 \\
0 & 0 & k_{12}(t) & k_{13}(t) & 0 & k_{15}(t) & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & k_{24}(t) & k_{25}(t) & 0 & 0 & 0 & k_{29}(t) \\
0 & k_{31}(t) & 0 & 0 & 0 & 0 & 0 & 0 & k_{38}(t) & 0 \\
0 & 0 & k_{42}(t) & 0 & 0 & 0 & 0 & 0 & k_{48}(t) & 0 \\
k_{50}(t) & 0 & 0 & 0 & 0 & 0 & k_{56}(t) & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & k_{67}(t) & 0 & k_{69}(t) \\
0 & k_{71}(t) & k_{72}(t) & 0 & 0 & 0 & 0 & 0 & k_{78}(t) & k_{79}(t) \\
k_{80}(t) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
k_{90}(t) & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{bmatrix}
\end{array}
$$

where $\{(Y_n,\ T_n),\ n \geq 0\}$ is the underlying Markov renewal sequence of random variables. In other words, $k_{ij}(t)$ is the probability that if the SMP has just entered state i; the next transition occurs within time t and the next state is state j. Therefore, the non-zero elements

of $K(t)$ could be derived as given in the following example:

$$k_{12}(t) = \int_0^t \overline{F}_3(x)\overline{F}_4(x)dF_2(x)$$

Following the two-stage analysis of SMP, let $Z = K(\infty) = \lim_{t\to\infty} K(t)$ be the one-step transition probability matrix of the embedded Markov chain (EMC) of the SMP.

$$Z = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \\ 4 \\ 5 \\ 6 \\ 7 \\ 8 \\ 9 \end{array} \begin{array}{c} \begin{array}{cccccccccc} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \end{array} \\ \begin{bmatrix} 0 & p & 0 & 0 & 0 & 1-p & 0 & 0 & 0 & 0 \\ 0 & 0 & p_{12} & p_{13} & 0 & p_{15} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & p_{24} & p_{25} & 0 & 0 & 0 & p_{29} \\ 0 & q & 0 & 0 & 0 & 0 & 0 & 0 & 1-q & 0 \\ 0 & 0 & r & 0 & 0 & 0 & 0 & 0 & 1-r & 0 \\ s & 0 & 0 & 0 & 0 & 0 & 1-s & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & u & 0 & 1-u \\ 0 & p_{71} & p_{72} & 0 & 0 & 0 & 0 & 0 & p_{78} & p_{79} \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \end{array}$$

where for simplification, we take $p_{01} = p$, $p_{05} = 1 - p$, $p_{31} = q$, $p_{38} = 1 - q$, $p_{42} = r$, $p_{48} = 1 - r$, $p_{50} = s$, $p_{56} = 1 - s$, $p_{67} = u$ and $p_{69} = 1 - u$. By solving the following system of linear equations, $\vec{v}$ of the steady-state probabilities of the EMC are derived:

$$\vec{v} = \vec{v}K(\infty), \quad \sum_i v_i = 1, \quad i \in \Omega \tag{1}$$

According to the literature on SMPs, the steady-state probability of state i, for the SMP are given according to following equation

$$\pi_i = \frac{v_i h_i}{\sum_{j\in\Omega} v_j h_j}, \quad i \in \Omega \tag{2}$$

where h_i is the mean sojourn time that the process spends at each state i. These sojourn times could be derived as given in the following example:

$$h_2 = \int_0^\infty \overline{F}_5(t)\overline{F}_6(t)\overline{F}_7(t)dt$$

The mean sojourn times at the check states are assumed to be equal to zero in comparison with the remaining of the sojourn times. Hence, $h_3 = 0$ and $h_4 = 0$.

IV. Survivability attributes

- ***Availability***: In our model, states 0, 1, 2, 5 and 6 are the only states in which VoIP service is available to the users. Hence, the steady-state service availability is given by

$$AV = \pi_P + \pi_M + \pi_L + \pi_V + \pi_C$$
$$= \pi_0 + \pi_1 + \pi_2 + \pi_5 + \pi_6$$

where $\pi_i's$ can be obtained from equation (2).

- ***Confidentiality***: By confidentiality [9] of a system, we mean that sensitive information is not disclosed to any unauthorized recipients. Confidentiality can be computed in the context of some security attacks. The exploitation of the vulnerability of the system allows an attacker to traverse the entire system, thus compromising confidentiality. Therefore, in the context of such attacks, states C and F are identified with the loss of confidentiality. Therefore, the steady-state confidentiality measure can then be computed as

$$C = 1 - (\pi_C + \pi_F) = 1 - (\pi_6 + \pi_9)$$

- ***Reliability***: For quantifying the reliability of a software system, mean time to failure (MTTF) is a commonly used reliability measure. In order to study the reliability of the presented VoIP system, state F of Fig. II is assumed to be an absorbing state. In other words, no repair action is taken when the system runs out of resources or there is a security breach, and the system eventually fails. Hence the state space Ω of the model is partitioned into two new subsets, $T = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ and $A = \{9\}$, containing the transient and the absorbing states, respectively. In this case the corresponding one step transition probability matrix of the EMC is given by Z' which is same as the matrix Z with the last row replaced by $[0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 1]$. Using the approach introduced in [16], MTTF can be computed according to following equation

$$MTTF = \sum_{i\in T} N_i h_i \tag{3}$$

where h_i is the mean sojourn time of state i, and N_i denotes the average number of times that state i, $i \in T$ is visited, before the EMC is absorbed. These elements can be obtained by solving the system of equations:

$$N_i = p'_i + \sum_{j\in T} N_j p'_{ji}, \quad i, j \in T \tag{4}$$

with p'_i denoting the probability that the EMC starts at state i and p'_{ij} the ij^{th} element of matrix Z'. In our case, we assume that P is the initial state, hence, the initial probability vector is

$$\vec{p'} = [p'_i] = [1\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0\ 0] \tag{5}$$

V. Numerical results

In this paper, we focus on analyzing the feasibility of the framework of survivability model. We illustrate the evaluation of the survivability attributes of the VoIP system in this section. For the model to be accurate, it is important to accurately estimate the model parameters (i.e., mean sojourn times and the DTMC transition probabilities) listed

above. However, in this paper, our focus is primarily on developing a methodology for analyzing quantitatively the survivability attributes of the system rather than accurate model parameterizations. Since at this point accurate model parameter values for the SMP model are not known to us, we assumed some values for them.

Mean sojourn times: It is assumed that the system spends more time in state P than in state M, and the time spent in state M is in turn more than that in state L. Hence, we assume that the mean time spent in state P is more than that of state M, which is again more than that of state L. Also, a good system must spend more time in state P and state V than in state C. The time spent in state C must be as short as possible. Accordingly, we assume that the mean time of state C is less than that of both the states P and V. On the other hand, rejuvenation must be faster than any other activities to avoid denial of service attack. Hence, we assume that the mean time of being in state R is shorter that that of F, M and L. Moreover, the mean sojourn times at the check states C_1 and C_2 are very small when compared to rest of the sojourn times. Hence, without loss of generality, we assume the mean sojourn times at states C_1 and C_2 to be zero [12]. The following values of mean sojourn times are randomly chosen for our analysis in time unit.

$h_0 = 1$, $h_1 = 0.5$, $h_2 = 0.4$, $h_3 = h_4 = 0$, $h_5 = 0.35$, $h_6 = 0.2$, $h_7 = 0.4$, $h_8 = 0.3$, $h_9 = 0.4$,

Transition probabilities: We assume that resource degradation which brings the system from state P to state M is more likely to happen than getting exposed to some vulnerabilities, as new calls keep coming. Also, it is assumed that a successful attack that brings the system from state V to state C is less likely to occur than the detection of the attack and bringing the system back from state V to state P. The probability of returning to state M after the resource check completion in state C_1, is greater than the probability of returning to state L after check in C_2, because the level of resource exhaustion in state L is higher than that in state M, as more calls are served at this time. Similarly, other transition probabilities are defined based on the likelihood of the occurrence of the event. The non zero elements of the transition probability matrix Z of the EMC taken for our analysis are given below

$p = 0.6$, $p_{12} = 0.4$, $p_{13} = 0.4$, $p_{15} = 0.2$, $p_{24} = 0.3$, $p_{25} = 0.35$, $p_{29} = 0.35$, $q = 0.8$, $r = 0.2$, $s = 0.6$, $u = 0.8$, $p_{71} = 0.4$, $p_{72} = 0.3$, $p_{78} = 0.2$, $p_{79} = 0.1$

For the case of DTMC, the steady state probabilities are obtained by equation (1), and are given below

$v_0 = 0.1941$, $v_1 = 0.2084$, $v_2 = 0.1102$, $v_3 = 0.0834$, $v_4 = 0.0331$, $v_5 = 0.1579$, $v_6 = 0.0632$, $v_7 = 0.0505$, $v_8 = 0.0532$, $v_9 = 0.0461$

For the case of SMP the steady state probabilities are obtained by equation (2) and are given below

$\pi_0 = 0.4175$, $\pi_1 = 0.2241$, $\pi_2 = 0.0948$, $\pi_3 = 0$, $\pi_4 = 0$, $\pi_5 = 0.1189$, $\pi_6 = 0.0272$, $\pi_7 = 0.0435$, $\pi_8 = 0.0343$, $\pi_9 = 0.0397$

Using the assumed values of the input parameters and the steady state probabilities of the SMP, we predict that the steady state availability of the system, $A = 0.8825$, and the steady state confidentiality, $C = 0.9331$. The MTTF is obtained by equation (3), and we predict that for the assumed values of input parameters, $MTTF = 9.6602$ time units.

We also compare the performance of our model with the model given in [12] (where availability is obtained in presence of resource degradation), and with the model presented in [11] (where availability is obtained in case of security attacks). We henceforth refer to the model given in [12] as *model 1*, model given in [11] as *model 2*, and model presented in this paper as *model 3*.

Fig. 4 represents that the system availability increases as the probability of invoking check C_1 increases. This shows that when system is in state M, the check for system survival should be done more frequently. Moreover, the graph also shows that model 3 gives more availability as compared to model 1.

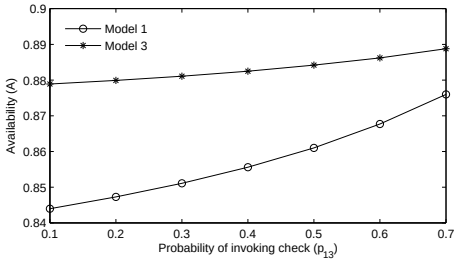

Figure 4. Availability Vs probability of invoking check C_1

Fig. 5 represents that the system availability decreases as the probability of an active attack increases, as expected. Further, it also shows that model 3 outperforms model 2 in this regard.

Fig. 6 represents that the steady state probability of the system getting stuck in failure state (π_F for SMP) decreases as the probability of triggering adaptation mechanism, p_{67} increases. The graph also shows that model 3 gives better results than model 2.

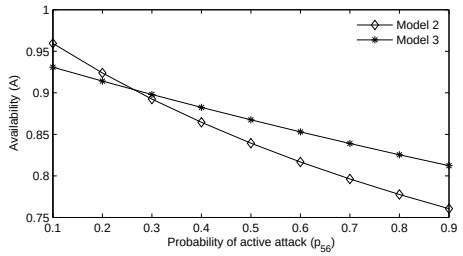

Figure 5. Availability Vs probability of active attack

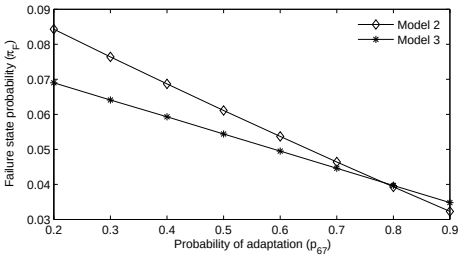

Figure 6. Failure state probability Vs probability of adaptation

VI. Conclusion

In this paper, a general analytical framework of survivability model for a VoIP system is presented and the model is analyzed in a mathematical manner. A state transition model that describes the dynamic behavior of such a system is used as a basis for developing a stochastic model. Since the memoryless property of exponential distribution implies the absence of aging and learning, it would not be appropriate for modeling system degradation and attacker's behavior. Hence, the model is studied under semi-Markov Process in order to capture the dependencies of the systems behavior on the time that the system spends at each state. The theoretical analysis of the SMP model is provided in closed-form. Also, various survivability measures such as availability, confidentiality and reliability of the VoIP system are obtained. The model analysis is illustrated with the help of a numerical example. The issue of the absence of exact values of model parameters is addressed by studying the sensitivity of different attributes to small changes in the parameter values. The results of our model are also compared with the results of the models proposed in [11], [12], and the comparison points towards the fact that our model has the potential to enhance the survivability level of the VoIP system.

Acknowledgement

This research work is supported by the Department of Science and Technology, India under the grant number RP 01907. One of the authors (V.G.) would like to thank CSIR, India for providing her financial support through Senior Research Fellowship.

References

[1] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, N. Mead, "Survivable network systems: An emerging discipline", *Technical Report, CMU/SEI-97-TR-013*, 1997.

[2] Vaneeta Jindal, S. Dharmaraja, Kishor S. Trivedi, "Analytical survivability model for fault tolerant cellular networks supporting multiple services", In Proc. *SPECTS*, 505-512, 2006.

[3] S. Dharmaraja, Vaneeta Jindal, Upkar Varshney, "Reliability and survivability analysis for UMTS networks: An analytical approach", *IEEE TNSM*, 5, 132-142, 2008.

[4] Yun Liu, Kishor S. Trivedi, "Survivability quantification: The analytical modeling approach", *International Journal of Performability Engineering*, 2(1), 29-44, 2006.

[5] Stylianos Karapantazis, Fotini-Niovi Pavlidou, "VoIP: A comprehensive survey on a promising technology", *Computer Networks*, Vol. 53, 2050-2090, 2009.

[6] V.P. Koutras., A. N. Platis, "Optimal rejuvenation policy for increasing VoIP service reliability, In Proc. *European Safety and Reliability Conference*, Vol. 3, 2285-2290, 2006.

[7] D. Richard Kuhn, Thomas J. Walsh, Steffen Fries, "Security Considerations for Voice Over IP Systems", *NIST Special Publication 800-58*, 2005.

[8] Himanshu Dwivedi, "Unconventional VoIP security threats", *Hacking VoIP: Protocols, Attacks, and Countermeasures*, No Starch Press San Francisco, 131-152, 2008.

[9] B. Madan, K. Goseva-Popstojanova, K. Vaidyanathan, K. S. Trivedi, "A method for modeling and quantifying the security attributes of intrusion tolerant systems", *Performance Evaluation*, Vol. 56, 167-186, 2004.

[10] K. S. Trivedi, K. Vaidyanathan, K. Goseva- Postojanova, "Modeling and Analysis of Software Aging and Rejuvenation", In Proc. *IEEE Annual Simulation Symposium*, 270-279, 2000.

[11] Dong Seong Kim, Khaja Mohammad Shazzad, Jong Sou Park, "A Framework of Survivability Model for Wireless Sensor Network", *ARES*, 515-522, 2006.

[12] V. P. Koutras, A. N. Platis, "VoIP availability and service reliability through software rejuvenation policies", *International Conference on Dependability of Computer Systems*, 262 - 269, 2007.

[13] W. Xie, Y. Hong, K.S. Trivedi, "Analysis of a two-level software rejuvenation policy". *Reliability Engineering and System Safety*, Vol. 87, 13-22, 2005.

[14] V. P. Koutras, A. N. Platis, "Semi-Markov availability modeling of a redundant system with partial and full rejuvenation actions", In proc. *DepCoS-RELCOMEX*, 127-134, 2008.

[15] V. G. Kulkrani, "Modeling and analysis of stochastic systems", Chapmanv & Hall, 1995.

[16] K. S. Trivedi, "*Probability and Statistics with Reliability, Queuing, and Computer Science Applications*", John Wiley and Sons, 2nd ed, 2001.