On Scalable and Efficient Security Risk Modelling of Cloud Computing Infrastructure based on Markov processes

Dimitrios A.Karras

Sterea Hellas Institute of Technology, Automation Dept, Psachna, Evoia, 34400, Greece, dakarras@teiste.gr, dimitrios.karras@gmail.com, dimitrios.karras@ieee.org

Abstract. While cloud computing infrastructures proliferates in nowadays computing and communications technology there are few reports investigating models for their security. In this paper, new efficient models are developed and evaluated for analyzing the security-related behavior of cloud computing architectures and networks comprising complex interconnected communication systems adapted towards a generalized analysis. These cloud related models, based on Markov processes, allow calculation of critical security factors for the cloud infrastructure, related to intrusion detection, of such interconnected and distributed systems components and the evaluation of the associated security mechanisms. Although, at this step an architecture of at least three interconnected systems is analyzed, the systematic model introduced allows for a generalized model of N interconnected systems in a cloud architecture under reasonable assumptions. We herein show the principles of such an analysis. Security parameters calculation and Security mechanisms evaluation may support the risk analysis and the decision making process in resolving the trade-offs between security and quality of service characteristics corresponding to the complex interconnected computing and communication systems.

Keywords. Cloud infrastructures, Security Risk Analysis, Interconnected Systems, Markov Processes, Intrusion Detection

1. Introduction

The increasing role of communication services makes crucial the issue of ensuring the security attributes of the underlying computing and communication infrastructures in terms of secrecy, integrity and availability. The security attacks in computer and communication systems may result in [1]: information disclosure, unauthorized modification of files, messages and transactions, masquerading or successful break-in, decreasing communication services availability, repudiation in sending and receiving messages of electronic orders or in creating and modifying files, and the possibility of traffic analysis and the creation of user/consumer profiles. These attacks may emanate from legitimate users, unauthorized users and processes, such as malicious software.

Security is often cited as one of the greatest barriers to communications services, including Internet commerce. Of course, security is important to communication services in many ways, but it is really part of the way that business is enabled by the technology. Indeed, the security of communication systems, for instance for electronic commerce, is a business problem, not merely a technology one. Technologies such as public key encryption provide critical components of an overall solution, but they are not enough. Such technologies can be applied both to systems designed from scratch as well as to systems built around off-the-shelf products for Internet commerce. The important issue is to properly design the whole interconnected communication system so that security technologies could be applied. To this end a significant help could be provided by attempting to model the system computing and communication infrastructure. This is precisely the goal of this paper, namely, to model such interconnected infrastructures in terms of security.

Security violations leave abnormal patterns of system usage and accounting [2,3]. To cope with intrusions or attempted break-ins, system monitoring techniques or intrusion-detection mechanisms and audit trails are used, that rely on the collection of audit data and their comparison with the usage and accounting profiles maintained by the system [4]. The conditional probability of detecting an intrusion given that the intrusion has occurred is called intrusion coverage and used as a measure of the effectiveness of the intrusion-detection mechanism. The number of normal and abnormal usage and accounting types (patterns) is extremely high and

they can be differentiated only partially so that it is very difficult to have an intrusion coverage close to 1. An alarm is triggered if certain thresholds are reached. The detection sensitivity level and the false alarm rate depend on the thresholds set [5]. Increasing the detection sensitivity level leads to higher false alarm rates, i.e., better intrusion coverage appears to be in trade-off with false alarms.

Audit trails, i.e., data that allow tracing from users and transactions of related processes aim at detecting or deterring system intrusion and helping assessing the damage caused by intrusions in the case of successful ones. Issues regarded in research efforts in the context of audit trails include the analysis and specification of auditable events and the quality improvement of the mechanisms related to efficiency, protection and the prevention of denial of service. They, also, include the association and analysis of related events and the automation of intrusion detection and damage assessment functions [4].

Intrusion detection mechanisms can be used in stand-alone or networked systems. They are based on the development of user and system or network resources usage profiles and knowledge-oriented or statistically oriented methods. They have limitations, since the absence of rules for all possible intrusion scenarios or inaccurate statistical distributions do not lead to detection of intrusions or attempted break-ins. On the other hand, they may lead to false alarms, if unexpected user actions or resource usage patterns occur, which are not foreseen by the rules or the distributions used.

To study the behavior of security attacks or intrusion processes, models have to be developed and used, since it is quite impossible to directly analyze real computer systems and networks or information infrastructures to this respect.

In section 2, the model is described and the mathematical notations and the system equations are discussed. In section 3, we apply the model and discuss the various results obtained for a set of parameter values. Finally, section 4 summarizes this paper with conclusions and future directions.

2. Cloud Security Models Description and Analysis

In this research we develop and use Markov models by considering the states of each system component of the interconnected information infrastructure, which reflect system functioning with respect to the above stated possible attacks. These states are explicitly associated with the security attributes of secrecy, integrity and availability. On the other hand, the existing dependencies between the component systems comprising the cloud infrastructure are taken into account in the proposed models. While single system security models exist in the literature [4,6], the suggested models for analyzing security parameters in infrastructures is one of the first research efforts for investigating the effects of multiple dependent systems operation in the interconnected communication and information infrastructure security planning.

We assume constant arrival rates of attacks and constant state transition rates, which allow the use of exponential or geometrical distributions, since there are no exact analytical solution methods for non-Markovian models. (Approximation techniques could be used in the case of non-constant rates.)

Model A- the cloud as a single system being in attack

Figure 1 shows the model, which relates to a single system and consists of 7 states. The system is in state 0 when there are no security violations or attempted attacks. All security attributes are well maintained. With the first attempted attack, the system enters in state 1. The system remains in this state as long as it is under attack, the attacks are not detected and the system has not been penetrated. From this state, transition back to state 0 takes place if the attacks are detected or to state 2, if the attacker obtains authentication information and penetrates the system. The attacker remains in state 2 as long as he obtains (disclosures) confidential information and may move to state 3 if he starts to modify files, programs and messages or to state 4 if he chooses to hinder the access of authorized users to programs, hardware and data. When the attacker is detected, the system enters in the state 5, where it is reconfigured and transition back to state 0 occurs. Transition from state 0 to state 6 may take place if a false alarm is triggered. After the reconfiguration the inverse transition occurs. Transitions between states 2, 3 and 4 take place according to the actions of the attacker, which lead to unauthorized information disclosure, modification and access to system or network resources, respectively.

Notation and system of equations

In this research we use the following notation, which is common in textbooks on stochastic processes, queueing theory and Markovian chains in particular [7].

λ_{ij}, is the transition rate from state i to state j, τ_{ij}, is the transition probability from state i to state j and P_i, is the probability of the system or network or infrastructure to be in state i (steady state).

From the state-transition-rate diagram shown in Fig. 1, it is obvious that the Markov chain is irreducible and we accept the limit that $P_k = lim\ P_k(t)$ as $t \to \infty$. In the equilibrium case we are interested in that the flow must be conserved in the sense that the input flow must equal the output flow for any given state. By inspection we can establish the following equilibrium (steady-state) equations for the cloud model A.

$$(\lambda_{01}\tau_{01} + \lambda_{06}\tau_{06})P_0 = \lambda_{10}\tau_{10}P_1 + \lambda_{50}\tau_{50}P_5 + \lambda_{60}\tau_{60}P_6 \quad (1)$$

$$\lambda_{10}\tau_{10}P_1 + \lambda_{12}\tau_{12}P_1 = \lambda_{01}\tau_{01}P_0 \quad (2)$$

$$(\lambda_{23}\tau_{23} + \lambda_{24}\tau_{24} + \lambda_{25}\tau_{25})P_2 = \lambda_{12}\tau_{12}P_1 + \lambda_{32}\tau_{32}P_3 + \lambda_{42}\tau_{42}P_4 \quad (3)$$

$$(\lambda_{32}\tau_{32} + \lambda_{34}\tau_{34} + \lambda_{35}\tau_{35})P_3 = \lambda_{23}\tau_{23}P_2 + \lambda_{43}\tau_{43}P_4 \quad (4)$$

$$(\lambda_{42}\tau_{42} + \lambda_{43}\tau_{43} + \lambda_{45}\tau_{45})P_4 = \lambda_{24}\tau_{24}P_2 + \lambda_{34}\tau_{34}P_3 \quad (5)$$

$$\lambda_{50}\tau_{50}P_5 = \lambda_{25}\tau_{25}P_2 + \lambda_{35}\tau_{35}P_3 + \lambda_{45}\tau_{45}P_4 \quad (6)$$

$$\lambda_{60}\tau_{60}P_6 = \lambda_{06}\tau_{06}P_0 \quad (7)$$

By means of this model we may analyze the systems comprising an interconnected information infrastructure separately. The security-related dependence between these systems can be taken into account if we adapt the probability transitions from state 1 to state 2 of the controlled system by adding to its initial value the equilibrium probability of the controlling system being in state 2.

We assume that successful attacks in the various systems are independent. However, if the controlling system is penetrated, the controlled system may be penetrated immediately or with higher probability than when it is attacked directly and not through the controlling system.

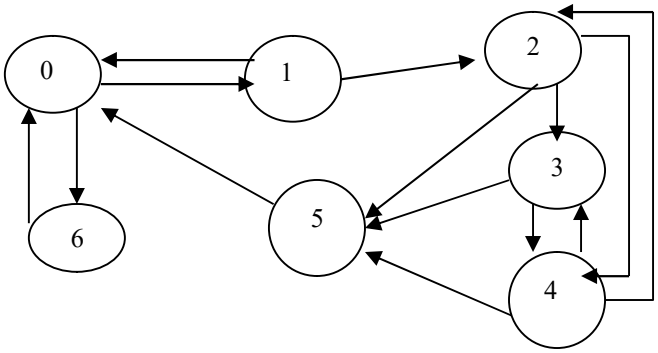

Fig. 1. State-transition-rate for the diagram of model A for the cloud modelled as a single system

However, the cloud is an interconnected system of let's say N components. In order to find out the related probabilities for every component we could assume that all components are independent, each corresponding to a probability Pc(state-k), with probabilities Pc(state-k) being equal for all components c, and for every state k of the above defined system of equations. In order to estimate Pc(state-k) from the relevant P(state-k) of the cloud system, after solving the previously mentioned equations, we have to model the events involved for c=1..N and k=0..6. Under these assumptions we could have, involving the theory of total probability for independent and mutually disjoint events, since each cloud component state could be considered as such compared to the rest of cloud components,

P(state-k)= P(all possible combinations of events for c=1..N components being in state k) =>

$$P(\text{state-k}) = C(N,1)* Pc(\text{state-k}) (1-Pc(\text{state-k}))^{(N-1)} + C(N,2) * Pc(\text{state-k})^2 (1-Pc(\text{state-k}))^{(N-2)} + C(N,3) * Pc(\text{state-k})^3 (1-Pc(\text{state-k}))^{(N-3)} + \ldots C(N,r) * Pc(\text{state-k})^r (1-Pc(\text{state-k}))^{(N-r)} + \ldots. C(N,N) * Pc(\text{state-k})^N (1-Pc(\text{state-k}))^{(N-N)} \quad \textbf{(8)}$$

where it is known that,
$C(n,r)=n!(r!(n-r)!)$

If P(state-k) is known by solving the previously mentioned Markov process based system of Model A, then every Pc(state-k) can be calculated solving equation (8).

Initial Ad-Hoc Model B for cloud in intrusion

The interconnected communication and information infrastructure is modeled by a Markovian chain again for two non local systems under the same cloud. In this case an Ad Hoc analysis and model is presented, where some states are omitted. In the general form, the model relates to n systems and m states of each system, which may lead to mxn states of the Markovian chain if transitions from all states to all others are possible. We assume Markov chains which are irreducible and for which exists the limit $Pk = \lim Pk(t)$ as $t \to \infty$ for all states k.

Figure 2 shows the initial model B, which relates to two systems or networks comprising an information infrastructure and consists of 12 states. The systems are in state (0,0) when there are no security violations or attempted attacks. With the first attempted attack, the attacked systems enter in state (1,0) or (0,1) if it is the first or the second system attacked. From this, state transition to state (1,1) may occur if both systems are under attack. Transition to state (2,0), (2,1) or (0,2), (1,2) takes place if the attempted intrusion leads to successful penetration of the first or the second system, respectively. If one of the systems is occupied then the second system is penetrated as well, (2,2). From this, state transition to state (3,3) occurs when the penetration is detected. After the reconfiguration of the systems, state (0,0) is entered. From state (0,0) transition may occur to state (4,0) or (0,4) if a false alarm of the first or the second system is flagged.

After the false alarm is resolved current state becomes the (0,0). From Fig. 2 we obtain the following equilibrium equations by simplifying the numbering of the states in an ad hoc way as follows: (0,0) – 0, (1,0) – 1, (0,1) – 2, (1,1) – 3, (2,0) – 4, (0,2) – 7, (2,1) – 5, (1,2) – 6, (2,2) – 8, (3,3) — 9, (4,0) – 10, (0,4) – 11.

If p is the matrix of the transition probabilities and P the vector of the steady state probabilities then, the following equation holds, as it is known: pP=P

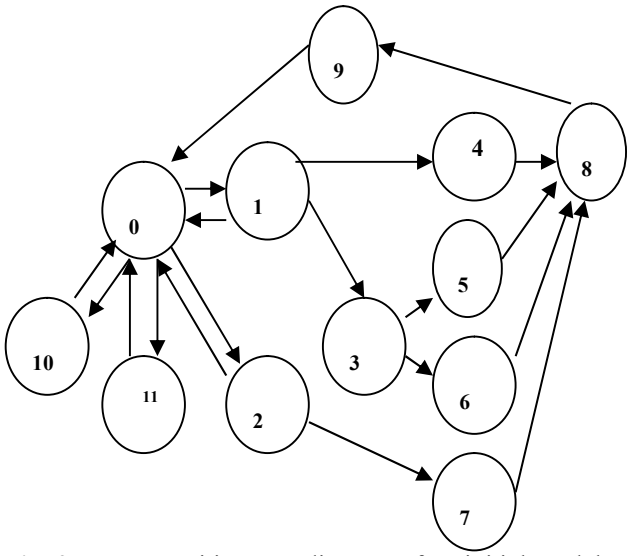

Fig. 2. State-transition-rate diagram of an initial model B for two interconnected systems or networks of the same cloud infrastructure.

$$(\lambda_{01}\tau_{01}+\lambda_{02}\tau_{02}+\lambda_{10,0}\tau_{10,0}+\lambda_{11,0},\tau_{11,0})P_0$$
$$=\lambda_{10}\tau_{10}P_1+\lambda_{20}\tau_{20}P_2+\lambda_{30}\tau_{30}P_3+\lambda_{10,0}\tau_{10,0}P_{10}+\lambda_{11,0}\tau_{11,0}P_{11} \quad (9)$$
$$(\lambda_{13}\tau_{13}+\lambda_{14}\tau_{14})P_1=\lambda_{01}\tau_{01}P_0 \quad (10)$$
$$(\lambda_{23}\tau_{23}+\lambda_{27}\tau_{27})P_2=\lambda_{02}\tau_{02}P_0 \quad (11)$$
$$(\lambda_{35}\tau_{35}+\lambda_{36}\tau_{36})P_3=\lambda_{13}\tau_{13}P_1+\lambda_{23}\tau_{23}P_2 \quad (12)$$
$$\lambda_{48}\tau_{48}P_4=\lambda_{14}\tau_{14}P_1 \quad (13)$$
$$\lambda_{58}\tau_{58}P_5=\lambda_{35}\tau_{35}P_3 \quad (14)$$
$$\lambda_{68}\tau_{68}P_6=\lambda_{36}\tau_{36}P_3 \quad (15)$$
$$\lambda_{78}\tau_{78}P_7=\lambda_{27}\tau_{27}P_2 \quad (16)$$
$$\lambda_{89}\tau_{89}P_8=\lambda_{48}\tau_{48}P_4+\lambda_{58}\tau_{58}P_5+\lambda_{68}\tau_{68}P_6+\lambda_{78}\tau_{78}P_7 \quad (17)$$
$$\lambda_{90}\tau_{90}P_9=\lambda_{89}\tau_{89}P_8 \quad (18)$$
$$\lambda_{10,0}\tau_{10,0}P_{10}=\lambda_{0,10}\tau_{0,10}P_0 \quad (19)$$
$$\lambda_{11,0}\tau_{11,0}P_{11}=\lambda_{0,11}\tau_{0,11}P_0 \quad (20)$$

We solve the above equations for steady-state probabilities. From these we may calculate the probabilities for each system of the underlying interconnected cloud communication and information infrastructure.

However, again, this model B based cloud infrastructure is an interconnected system of let's say N components. In order to find out the related probabilities for every such component we could assume that all components are independent, as in model A, each corresponding to a probability P_Bc(state-k), with probabilities P_Bc(state-k) being equal for all components c, and for every state k of the above defined system of equations. In order to estimate P_Bc(state-k) from the relevant P_B(state-k) of the cloud system, after solving the previously mentioned equations, we have to model the events involved for c=1..N and k=0..12. Under these assumptions we could have, involving the theory of total probability for independent and mutually disjoint events, since each cloud component state could be considered as such compared to the rest of cloud components,

P_B(state-k)= P(all possible combinations of events for c=1..N components being in state k) =>

$P_B(\text{state-k}) = C(N,1)* P_Bc(\text{state-k}) (1-P_Bc(\text{state-k}))^{(N-1)} + C(N,2) * P_Bc(\text{state-k})^2 (1-P_Bc(\text{state-k}))^{(N-2)} + C(N,3) * P_Bc(\text{state-k})^3 (1-P_Bc(\text{state-k}))^{(N-3)} + \ldots C(N,r) * P_Bc(\text{state-k})^r (1-P_Bc(\text{state-k}))^{(N-r)} + \ldots.. C(N,N) * P_Bc(\text{state-k})^N (1-P_Bc(\text{state-k}))^{(N-N)}$ **(21)**

where it is known that,
C(n,r)=n!(r!(n-r)!)

If P_B(state-k) is known by solving the previously mentioned Markov process based system of Model A, then every P_Bc(state-k) can be calculated solving equation (21).

A systematic Model B for cloud in intrusion-Towards a Scalable Analysis for interconnected cloud subsystems

In this interconnected cloud model, again, the communication and information cloud infrastructure is considered as a Markovian chain moxdel. In the general form, the model relates to n systems and m states of each system, which may lead to mxn states of the Markovian chain if transitions from all states to all others are possible. We herein employ, however, a scalable model B, which leads to more unknown variables than the previous initial model B but it leads to a better, scalable and more systematic model B of two interconnected system than before. We assume again Markov chains which are irreducible and for which exists the limit Pk =lim Pk(t) as t->∞ for all states k.

Figure 3 shows the model, which relates to two systems or networks comprising an information infrastructure and consists of 14 states. Figure 3 can be obtained from figure 1 and it is its generalization for two interconnected systems. It bares similarities with figure 2 architecture, which is ad hoc. Such a systematic view could lead to other possible meaningful generalizations. Taking into account that mn states of the Markovian chain if transitions from all states to all others are possible, this means that in our case 72 = 49 states would exist. However, the proposed meaningful generalization of model A, in the case of two interconnected systems, leads, as we will see in m x n = 14 states only. The systems are in state (0,0) when there are no security violations or attempted attacks. With the first attempted attack, the attacked systems enter in state (1,0) or (0,1) if it is the first or the second system attacked. From this, state transition to state (1,1) may occur if both systems are under attack. Transition to state (2,0), (2,1) or (0,2), (1,2) takes place if the attempted intrusion leads to successful penetration of the first or the second system, respectively. If one of the systems is occupied then the second system is penetrated as well, (2,2). The attacker remains in state (2,2) as long as he obtains (disclosures) confidential information and may move to state (3,3) if he starts to modify files, programs and messages or to state (4,4) if he chooses to hinder the access of authorized users to programs, hardware and data. When the attacker is detected, the system enters in the state (5,5), where it is reconfigured and transition back to state (0,0) occurs. After the reconfiguration the inverse transition occurs. Transition from state (0,0) to state (6,0) or (0,6) may take place if a false alarm of the first or the second system is flagged.

After the false alarm is resolved current state becomes the (0,0). From Fig. 3 we obtain the following equilibrium equations by simplifying but in a systematic way easily shown below, the numbering of the states:

(0,0) – 0, (1,0) – 1, (0,1) – 2, (1,1) – 3, (2,0) – 4, (2,1) – 5, (0,2) – 6, (1,2) – 7, (2,2) – 8, (3,3) — 9, (4,4)-10, (5,5)-11, (6,0) – 12, (0,6) – 13.

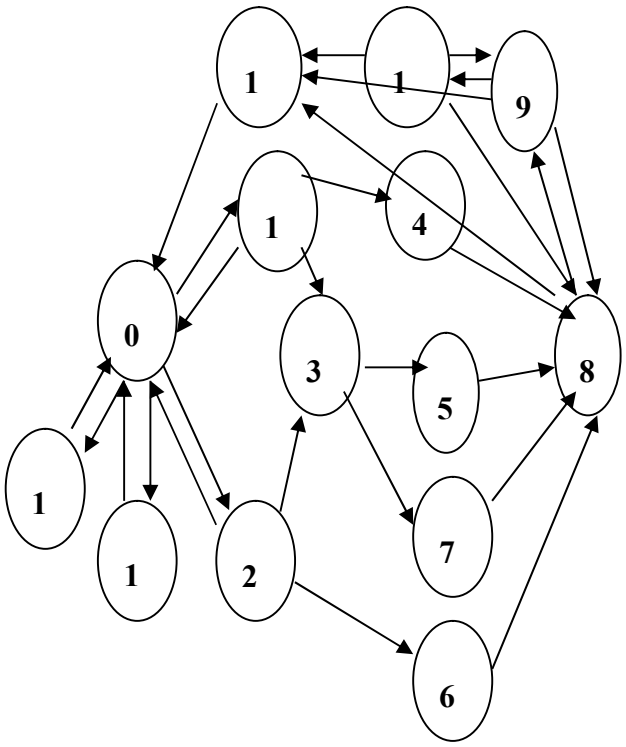

Fig. 3. State-transition-rate diagram of model B for two interconnected subsystems of the cloud infrastructure.

$$(\lambda_{01}\tau_{01}+\lambda_{02}\tau_{02}+\lambda_{0,12}\tau_{0,12}+\lambda_{0,13}\tau_{0,13})P_0$$
$$=\lambda_{10}\tau_{10}P_1+\lambda_{20}\tau_{20}P_2+\lambda_{11,0}\tau_{11,0}P_{11}+\lambda_{12,0}\tau_{12,0}P_{12}+\lambda_{13,0}\tau_{13,0}P_{13} \quad (22)$$
$$(\lambda_{13}\tau_{13}+\lambda_{14}\tau_{14})P_1=\lambda_{01}\tau_{01}P_0 \quad (23)$$
$$(\lambda_{23}\tau_{23}+\lambda_{26}\tau_{26})P_2=\lambda_{02}\tau_{02}P_0 \quad (24)$$
$$(\lambda_{35}\tau_{35}+\lambda_{37}\tau_{37})P_3=\lambda_{13}\tau_{13}P_1+\lambda_{23}\tau_{23}P_2 \quad (25)$$
$$\lambda_{48}\tau_{48}P_4=\lambda_{14}\tau_{14}P_1 \quad (26)$$
$$\lambda_{58}\tau_{58}P_5=\lambda_{35}\tau_{35}P_3 \quad (27)$$
$$\lambda_{68}\tau_{68}P_6=\lambda_{26}\tau_{26}P_2 \quad (28)$$
$$\lambda_{78}\tau_{78}P_7=\lambda_{37}\tau_{37}P_3 \quad (29)$$
$$\lambda_{89}\tau_{89}P_8+\lambda_{8,11}\tau_{8,11}P_8=\lambda_{48}\tau_{48}P_4+\lambda_{58}\tau_{58}P_5+\lambda_{68}\tau_{68}P_6+\lambda_{78}\tau_{78}P_7 \quad (30)$$
$$\lambda_{98}\tau_{98}P_9+\lambda_{9,10}\tau_{9,10}P_9+\lambda_{9,11}\tau_{9,11}P_9=\lambda_{89}\tau_{89}P_8+\lambda_{10,9}\tau_{10,9}P_{10} \quad (31)$$
$$\lambda_{10,9}\tau_{10,9}P_{10}+\lambda_{10,11}\tau_{10,11}P_{10}+\lambda_{10,8}\tau_{10,8}P_{10}=\lambda_{9,10}\tau_{9,10}P_9 \quad (32)$$
$$\lambda_{11,0}\tau_{11,0}P_{11}=\lambda_{10,11}\tau_{10,11}P_{10}+\lambda_{9,11}\tau_{9,11}P_9+\lambda_{8,11}\tau_{8,11}P_8 \quad (33)$$
$$\lambda_{12,0}\tau_{12,0}P_{12}=\lambda_{0,12}\tau_{0,12}P_0 \quad (34)$$
$$\lambda_{13,0}\tau_{13,0}P_{13}=\lambda_{0,13}\tau_{0,13}P_0 \quad (35)$$

We solve again the above equations for steady-state probabilities. From these we may calculate the probabilities for each system of the underlying interconnected communication and information cloud infrastructure.

As in the previous initial model B, if we define P_B(state-k) the estimated steady state probabilities acquired by solving the system of equations 22-35 above, then every P_{Bc}(state-k), which is the relevant probability of state k=0..13 of each cloud infrastructure component c=1..N can be calculated solving equation (21) again.

2. Preliminary Numerical Examples using Excel

The selection of the parameter values is based on the tests and results of [4,5]. For model A, we assume transition rates equal to 1 per day from states 0 and 1, transition rates equal to 25 from states 2, 3, 4, 5, and 8 to all others and transition probabilities, τ01 = 1-τ06, τ10 = 1-τ = 0.1, τ23= τ24= τ32= τ34= τ42= τ43=(1-τ)/2, τ12=τ25=τ35=τ45=τ, τ50=τ60=1, τ=0.2,……,1.0 (intrusion coverage). In the same way, for model B we assume transition rates per day λ01= λ13= λ14= λ02= λ27=λ23= λ89= λ0,10= λ10,0= λ0,11= λ11,0=1, λ10= λ20=12, λ48= λ35= λ36= λ58= λ68=25, λ78= λ90=3 and transitions probabilities, τ01=(1- τ0,10)/2 , τ13= τ14= τ27= τ23=0.1, τ02=1- τ0,10 , τ10= τ20=0.9, τ48= τ68= τ58= τ78= τ89= τ90= τ10,0= τ11,0=1, τ35= τ36=0.08, τ0,11= τ0,10= τ (false alarm rate) and τ = 0.0,…,0.08

With these assumptions we have obtained preliminary numerical results, involving Excel, shown in the next two diagrams, which validate our interconnected communication and information cloud infrastructure modelling approach, in terms of results compatible with that of literature for single systems.

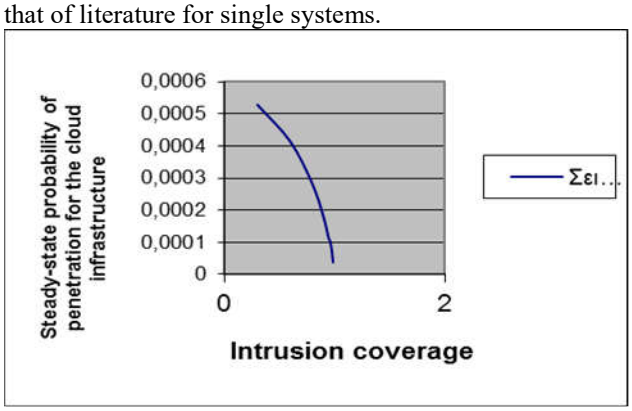

Fig. 4. Steady state probability of intrusion for model A as a function of intrusion coverage

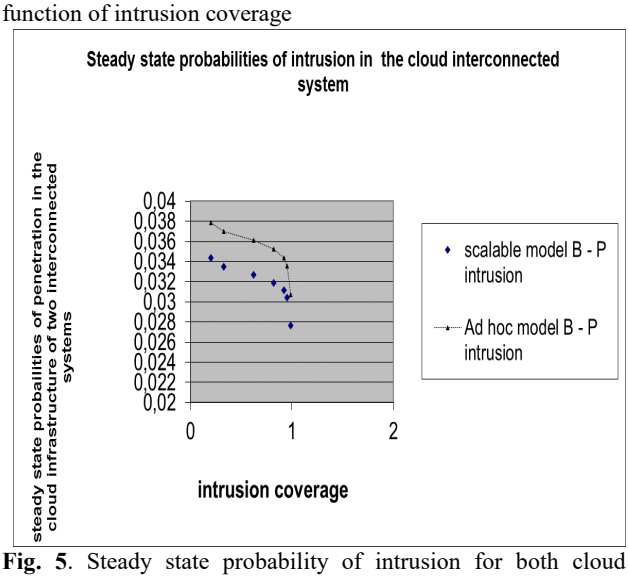

Fig. 5. Steady state probability of intrusion for both cloud models B as a function of intrusion coverage

Discussion and Prospects

In this research we presented three models for the analysis of cloud security-related attack processes by means of Markovian chains. The first model is proposed for use in the analysis of the cloud considered as a single system or network, while the second in the analysis of the cloud considered involving two interconnected systems or networks. The second model is an ad hoc initial model aimed at minimizing analysis costs, while the third one is a more detailed model defined towards a generalized model of security analysis for cloud involving interconnected systems. The models allow for the calculation of the expected probabilities of the systems to be in various states such as safe-state, under attack, in intrusion state and in false-alarm-state. For each such state and for each model we have estimated cloud components relevant probabilities. Future work will aim at generalizing, especially the third model, for N cloud interconnected subsystems as well as at expanding the models with respect to the probability distributions used. Also, future work will aim at the development of simulation models for the analysis of the security-related behaviour of cloud information infrastructures in complex communication systems, and as a validation tool for the analytical models. Furthermore, the involvement of neural networks and computational intelligence techniques for approximating the generalized probability distributions in the analytical models, might be investigated.

References

1. P. Helman and G. Liepins, “Statistical foundations of audit trail analysis for the detection of computer misuse”, IEEE Trans. On Software Engineering, SE-19, 1993, pp. 886-901.
2. D.E. Denning, ‘An Intrusion-detection Model’, IEEE Trans. On Software Engineering, SE-12, 1987, pp. 222-232.
3. C. Stoll, ‘Stalking the Wily Hacker’, Communications of the ACM, 1988, pp. 484-497.
4. B. C. Soh and T. S. Dillon, “Setting optimal intrusion-detection thresholds”, Computers & Security, Vol. 14, 1995, pp. 621-631.
5. G.E. Liepins and H.S. Vaccaro, ‘Intrusion Detection: Its Role and Validation’, Computers & Security, Vol. 11, 1992, pp. 347-355.
6. B. C. Soh and T. S. Dillon, “System intrusion processes: a simulation model”, Computers & Security, Vol. 16, 1997, pp. 71-79.
7. L. Kleinrock. “Queueing Systems, Volume I: Theory, John Wiley and Sons, New York, 1975