EVALUATION OF COMMUNICATION SCENARIOS INSIDE THE ELECTRICAL POWER SYSTEM

D. Codetta-Raiteri, R. Nai
Dipartimento di Informatica, Università del Piemonte Orientale
Viale T. Michel 11, 15121 Alessandria, Italy
e-mail: raiteri@mfn.unipmn.it, robertonai@libero.it

Abstract. The paper presents the modelling and the dependability evaluation of communication scenarios inside the distribution grid of the Electrical Power System. In particular, it deals with the communication between one area control centre and a set of substations exchanging commands and signals by means of a redundant communication network. The communication may be affected by threats such as the network failure, or intrusions into the communication, causing the loss of commands or signals. Such scenarios have been modeled and simulated in form of Stochastic Activity Network, a particular form of Petri Net, in order to evaluate in quantitative terms the effect of the threats to the communication. In particular, two measures have been computed: the probability and the number of failures in the communication, as a function of the time.

Keywords: communication, scenarios, Electrical Power System, distribution grid, modelling, simulation, Stochastic Activity Network.

1 Introduction

This work was developed inside the EU funded project named CRUTIAL (*CRitical UTility InfrastructurAL resilience*) [1] and addressing the Electrical Power System (EPS) intended to be composed by two infrastructures: the physical infrastructure consisting of all the artifacts realizing the electricity transportation from the generation plants to the consumers, and the ICT infrastructure for the management, the control and the monitoring of the physical infrastructure [2, 3]. These two kinds of infrastructure are considered to be interdependent [4, 5, 6] meaning that an accidental failure or a malicious attack affecting one infrastructure may negatively influence the behaviour of the other one. The general purpose of the CRUTIAL project is investigating the possible ways to realize the resilience of the EPS. This goal is motivated by several aspects, such as the increase of power consumes, the occurrence of recent black-out events, the market liberalization, and the use of Internet protocols for the communication among the sites of the EPS. Several activities are carried out in CRUTIAL, such as the investigation of architectures preventing faults and attacks, together with the identification, the modelling and the analysis of critical scenarios consisting of particular event sequences occurring in a certain portion of the EPS as a consequence of a failure or an attack.

The EPS can be structured in three subsystems: the *power generation*, the *transmission grid* and the *distribution grid*. In Sec. 2, we take into account some of the critical scenarios defined in [3] and dealing with the communication trough the Internet, between a control centre and a set of substations inside a distribution grid, where the communication can be affected by attacks or failures. In Sec. 4, we model the scenarios under exam in form of *Stochastic Activity Network* (SAN) [7], a particular form of Petri Net (Sec. 3); the purpose is evaluating the impact of attacks and failures to the communication dependability. The design and the simulation of the SAN models have been performed by means of the *Möbius* tool [8]. In Sec. 5, we present the simulation results about the probability and the quantity of failures of the communication, in case of attacks, failures, or both.

2 The case study

The scenarios under exam [3] deal with the communication between a control centre and a set of substations inside a distribution grid of the EPS, with the aim of sending commands from the control centre to the substations, and signals from the substations to the control centre. Such transmissions are performed by means of a redundant communication network (Fig. 2).

Typically a substation is connected to several electrical lines for the electrical power transportation, and executes the commands coming from the control centre. Such commands usually concern some operations to be performed on the electrical lines. In the case of the distribution grid, the same command may be sent to all the substations, for instance, an arming or disarming command [3]. The generation of a command by the control centre happens as a consequence of a command coming from the transmission grid, or as a consequence of the signals transmitted periodically from the substations. These signals may describe the state of the substations or the state of the electrical lines connected to them. Such information are useful to monitor the portion of the distribution grid under the control of the control centre.

Command and signal sessions. In our case study, we suppose that each command generated by the control centre has to be executed by all the substations; therefore, a copy of the command is sent to each substation. Moreover, we assume that the execution of a command by a substation is notified to the control centre by the transmission of an acknowledgment coming from the substation. So, the generation, the transmission and the execution of a command are performed according to the following sequence of operations that we call *"command session"*: **1)** the control centre opens the command session: it generates the command and starts collecting the acknowledgments coming from the substations and concerning the command execution, until a certain time out expires. **2)** A copy of the command is transmitted on the available communication network to each substation. **3)** Each substation executes the command and generates an acknowledgment proving the execution of the command. **4)** Each acknowledgment is transmitted on the available communication network to the control centre. **5)** The time out for the acknowledgments collection expires and the command session is closed.

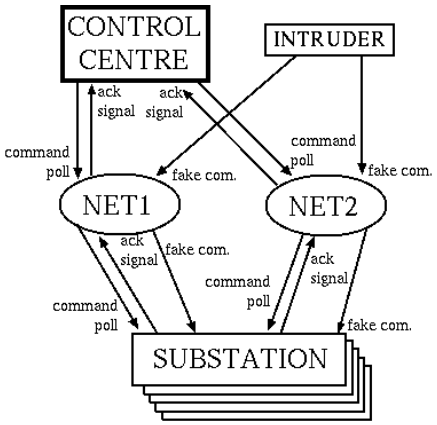

Figure 1: The scheme of the scenario.

We suppose that signals are not sent by a substation in an autonomous way, but they are generated as a reply to a poll request: periodically the control centre polls all the substations by sending a poll request to each of them, and they reply by sending a signal to the control centre. The protocol for the communication of signals is similar to the case of the communication of commands: we call *"signal session"* the following sequence of operations: **1)** the control centre opens the signals session: it generates a poll and starts collecting signals coming from the substations, until a certain time out expires. **2)** A poll request is transmitted on the available communication network to each substation. **3)** Each substation generates the signal. **4)** Each signal is transmitted on the available communication network to the control centre. **5)** The time out for the signals collection expires and the signal session is closed.

We assume that if the number of substations is N, a command (signal) session is successful if at least $N-1$ acknowledgments (signals) are received by the control centre before that the time out expires. If instead, more than one acknowledgment (signal) is missing when the time out expires, then the command (signal) session is considered to be failed. We suppose that N is equal to 10 and that at most one command (signal) session is running at any time.

Packets transmission. In our case study, we suppose that two communication networks ($NET1$ and $NET2$) can be exploited to transmit command copies, acknowledgments, poll requests and signals. $NET1$ is usually used for the communication between the con-

trol centre and the substations. We suppose that the bandwidth of each communication network is equal to 16 $kbps$ and that the transmission of each packet consumes 1 $kbps$ of the bandwidth. This means that no more than 16 packets can be transmitted on the same communication network at the same time. For example, if 10 signals are generated at the same time, they will consume 10 $kbps$ of the bandwidth of $NET1$: during their transmission, the bandwidth of $NET1$ available for the eventual transmission of other packets is 6 $kbps$. When $NET1$ completes the transmission of the signals, the available bandwidth of $NET1$ is 16 $kbps$ again. But, it may happen that the current available bandwidth of $NET1$ is not enough to transmit all the packets. In this case, $NET2$ is used to transmit the packets that $NET1$ can not transmit. This may happen if a command session and a signal session are running in parallel way. For instance, let us assume that the bandwidth of $NET1$ is currently consumed to transmit 10 signals, and before their transmission is complete, 10 acknowledgments are generated. In this case, 6 acknowledgments will be transmitted by $NET1$ with the consequent complete consume of its bandwidth, while the remaining 4 acknowledgments will be directed to $NET2$ for the transmission. Another situation where $NET2$ can be exploited for transmission is the case of the failure of $NET1$, as described in the following.

Actually, we could have specified that the transmission of a packet requires less than 1 $kbps$ of the bandwidth, or that a communication network has a bandwidth higher than 16 $kbps$; in this way, the communication network would be able to transmit more than 16 packets at the same time. Our choice depends on the fact that one of the goals of our study is evaluating the effect of the bandwidth consumption to the communication reliability. To this aim, if the communication networks had an higher transmission capacity, then we would need to consider more than 10 substations in the scenario, eventually making the simulation computational costs worse.

Intrusions. The communication between the control centre and the substations may be affected by several threats causing the loss of commands, acknowledgments, poll or signals, and therefore determining the failure of command or signal sessions. We suppose that attackers may succeed in performing intrusions into the communication between the control centre and the substations: during an intrusion and by exploiting $NET1$ or $NET2$, the attacker may send several fake commands to the substations pretending to be the control centre. We assume that each fake command is sent to all the substations, and each substation is able to distinguish the fake commands from the original ones: if such protection is successful the fake command is discarded, but it may happen (with probability 0.01) that the protection fails and as a consequence, the fake command is executed by the substation. This determines the temporary failure of the substation functions, so during the period of unavailability, the substation does not react to the command copies or poll requests received from the control centre (or to eventual other fake commands). This may lead to the failure of command or signal sessions because the control centre will not receive any acknowledgment or signal from the unavailable substations. The substation unavailability is temporary: the failure of the substation due to the execution of a fake command, can be recovered, so the substation can turn available again replying to commands and polls. A fake command may be generated while a command session, a signal session, or both are running. We assume that at most one intrusion can be on act at any time.

Network failure. The communication between the control centre and the substations is allowed by the communication networks *NET1* and *NET2*. Each of them may become unavailable due to its own failure; we assume that such unavailability is temporary because the failure can be recovered. Since $NET1$ and $NET2$ are redundant, if $NET1$ is not available, then $NET2$ can be used for the transmission among the sites. Since a communication network can not transmit more than 16 packets at the same time, if only one network is available at a certain time, its bandwidth may not be enough to transmit all the packets; this may happen if a command session is running in parallel with a signal session, or if a fake command has been generated during a command or signal session. In this case, some packets may be lost. For instance, if $NET1$ is failed, $NET2$ is working, its bandwidth is currently used to transmit 10 signals, and 10 acknowledgments are generated in the meanwhile, then 6 acknowledgments will consume the available bandwidth of $NET2$ and the remaining 4 acknowledgments can not be transmitted and will be lost. Besides the command and signal sessions, the failure of the communication network $NET1$ or $NET2$ may compromise the transmission of fake commands as well. The communication between the control

centre and the substation becomes impossible if both $NET1$ and $NET2$ are unavailable at the same time.

In our case study, the time for an event to occur can be a deterministic value, or a random value ruled by the *negative exponential distribution*. In Table 2, the (mean) times to occur of all the events in the case study are reported. In this paper, we are interested to evaluate the case study in these scenarios: **Scenario 1**: the communication network failures may not occur, but the intrusions may occur; **Scenario 2:** the communication network failures may occur, but the intrusions may not occur; **Scenario 3**: both the communication network failures and the intrusions may occur.

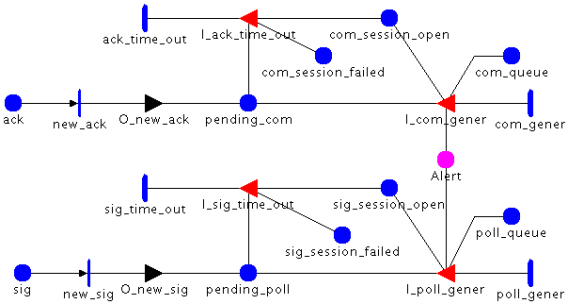

Figure 2: The SAN model of the control centre.

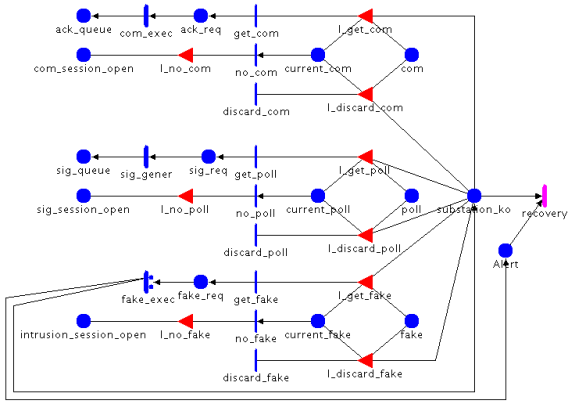

Figure 3: The SAN model of the substation.

3 Basic notions about SAN

SAN can be considered as a particular form of Petri Net (PN). A SAN model is characterized by *places*, each containing a certain number of tokens (*marking*). A place graphically appears as a circle. A particular marking of a certain set of places enables the completion (firing) of *activities* (transitions) whose effect is modifying in some way the number of tokens inside the places. Activities graphically appear as vertical bars. In the SAN formalism, the completion of an activity can be instantaenous or timed. In the second case, the completion time can be a constant value, or a random value ruled by a probability distribution such as the negative exponential one. The marking enabling the completion of an activity can be expressed by connecting the activity to the places by means of oriented arcs, as it is possible in PN. The effect of the activity completion can be specified in the same way. Another way to rule the completion of ativities consists of using *input gates*. An input gate is characterized by a *predicate* enabling the activity completion, and a *function* expressing the effect of the activity completion. Besides input gates, a SAN model can contain *output gates*. The role of an output gate is specifying only the effect of the activity completion; therefore, an output gate is characterized only by a function. Gates graphically appear as triangles.

A SAN model can be generated by composition of several sub-models. Two operators are available to this aim: the *Join* operator compose two or more SAN sub-models by superposition over their common places; the *Replicate* operator constructs a model consisting of a number of identical copies of a certain SAN sub-model (copies may share common places). The design, the composition and the analysis or simulation of SAN models is supported by the *Möbius* tool [8]. Further notions about the SAN formalism can be found in [7].

4 Modelling the scenarios

The case study described in Sec. 2 has been represented by several SAN models, each dedicated to a particular aspect. In this section, we briefly describe these models, while all their details can be found in [9]. Several places are shared by the SAN models and will be exploited in order to compose the models of the scenarios.

The SAN model appearing in Fig. 2 represents the functions of the control centre. The upper part of this model concerns the generation of commands and the collection of acknowledgments. The lower part represent the generation of polls and the collection of signals. The functions performed by a substation are modelled in the SAN model appearing in Fig. 3: the upper part

Table 1: The (mean) occurrence time of the events in the case study.

Event	Type of event	(mean) time to occur	occurring rate
command generation	stochastic	6.000E+0 h	1.667E-1 h^{-1}
command execution	stochastic	2.778E-4 h	3.600E+3 h^{-1}
time out for ack.	deterministic	5.556E-3 h	-
poll generation	deterministic	8.333E-2 h	-
signal generation	stochastic	2.778E-4 h	3.600E+3 h^{-1}
time out for signals	deterministic	5.556E-3 h	-
packet transmission	stochastic	2.778E-4 h	3.600E+3 h^{-1}
intrusion occurrence	stochastic	7.200E+2 h	1.390E-3 h^{-1}
intrusion duration	stochastic	5.000E+0 h	2.000E-1 h^{-1}
fake command generation	stochastic	1.000E+0 h	1.000E+0 h^{-1}
substation recovery	stochastic	1.200E+1 h	8.333E-2 h^{-1}
NET failure	stochastic	7.200E+2 h	1.390E-3 h^{-1}
NET repair	stochastic	1.200E+1 h	8.333E-2 h^{-1}

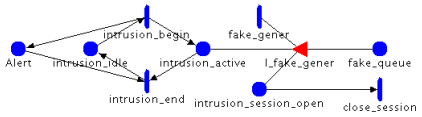

Figure 4: The SAN model of the intrusions.

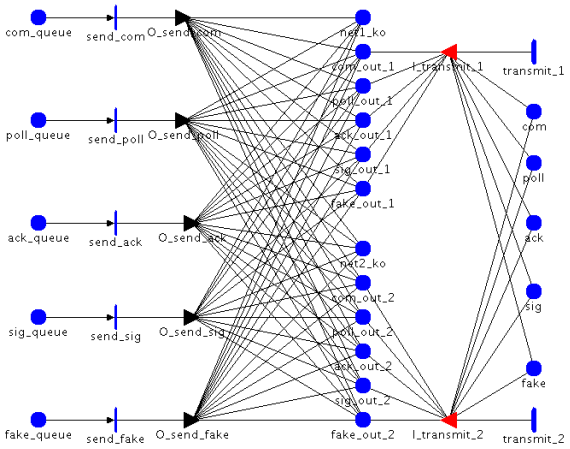

Figure 5: The SAN model of the packet transmission.

of the model is about the execution of commands, the central part concerns the generation of signals by the substation, while the lower part represents the discard or the execution of fake commands received from the intruder. The possibility of intrusions into the communication between the control centre and the substations, with the generation of fake commands directed to the substations, is modelled by the SAN in Fig. 4.

The transmission of packets can be performed by the communication network $NET1$ or $NET2$; packets can be command copies, acknowledgments, poll requests, signals or fake command copies. The SAN model in Fig. 4 represents this situation. The tokens inside the places *com_queue*, *poll_queue* and *fake_queue* represent the command copies, the poll requests and the fake command copies, respectively, waiting to be transmitted on the available communication network. The places *com_queue* and *poll_queue* appear also in the SAN model of the control centre (Fig. 2), while the place *fake_queue* appear also in the SAN model of the intrusions (Fig. 4). The tokens inside the places *ack_queue* and *sig_queue* represent acknowledgments and signals respectively, waiting to be transmitted. Such places appear also in the SAN model of the substation (Fig. 3). In this way, besides representing the transmission of packets, the SAN model in Fig. 4 acts as a "bridge" to join the previous SAN models, in order to build the model of the scenarios. The failure and the repair of the communication network $NET1$ or $NET2$ is represented by the SAN model in Fig. 6. If the places *net1_ko* (*net2_ko*) is marked, then $NET1$ ($NET2$) is currently failed. The places *net1_ko* and *net2_ko* appear also in the SAN model of the packets transmission (Fig. 4) in order to disable the communication on $NET1$ or $NET2$ in case of failure.

The models of the scenarios defined at the end of Sec. 2, are obtained by replicating and joining the SAN models described so far, by means of the *Rep* and *Join* operators (Sec. 3). The composed model for the Scenario 3 is shown in Fig. 7 where the SAN model of the substation is replicated 10 times in order to obtain the set of substations which is in turn joined with the

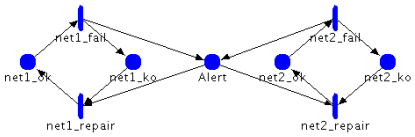

Figure 6: The SAN model of the communication networks failure and repair.

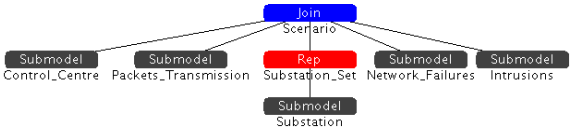

Figure 7: The composed model of the Case 3.

SAN models represening the control centre, the packets transmission, the network failures, and the intrusions. The composed model for the Scenario 1 is obtained from the one in Fig. 7 by omitting to join the model of the network failures, while the composed model for the Scenario 3 by omitting to join the model of the intrusions.

5 Simulation results

The composed models of the scenarios, described in the previous section, have been object of simulation. For each scenario, 10000 simulation batches have been performed by means of *Möbius*, setting a confidence level of 0.95, and a relative confidence interval of 0.1. The measures computed as a function of the time are: **1)** the probability that at least one command session has failed ($Pr_{com}(t)$); **2)** the probability that at least one signal session has failed ($Pr_{sig}(t)$); **3)** the mean number of failed command sessions ($Num_{com}(t)$); **4)** the mean number of failed signal sessions ($Num_{sig}(t)$). All measures are computed for a mission time varying between 0 and 10000 h. The functions expressing these measures in terms of place markings are reported in [9].

The values returned by the simulation are depicted in Fig. 8 and are provided in numerical form in [9]. Both Fig. 8.a and Fig. 8.b show that according to the event occurrence times specified in Table 2 and the SAN models described in Sec. 4, the intrusions (Scenario 1) determine a higher probability of command or signal session failure, with respect to the communication network failures (Scenario 2). In the Scenario 1, a command or signal session fails if at least two substations are unavailable at the same time due to execution of fake commands. In the Scenario 2 instead, some packets are lost causing the session failure, if a communication network ($NET1$ or $NET2$) is failed and a command session is running in parallel with a signal session (Sec. 2). In this situation, it may happen that the available communication network is not enough to transmit all the packets (command copies, acknowledgments, poll requests, signals). Still in the Scenario 2, if both communication networks are failed at the same time, this will lead to the loss of packets. Given the simulation results obtained for the Scenario 1 and the Scenario 2, we can conclude that the intrusions have a higher negative influence to the communication reliability, with respect to the network failures. This is confirmed in terms of number of failed session, by the results obtained for the measures $Num_{com}(t)$ (Fig. 8.c) and $Num_{sig}(t)$ (Fig. 8.d).

In the Scenario 3, both threats to the communication are present. For instance, a command session may fail because one acknowledgment is missing due to the current unavailability of one substation as a consequence of the execution of a fake command, and another acknowledgment is missing due to a failure affecting one of the communication networks. Actually, observing both Fig. 8.a and Fig. 8.b, we notice that the probability of failure of a command (signal) session at a certain time in the Scenario 3, is always higher than the corresponding probabilities in the Scenario 1 and in the Scenario 2. Also the mean number of failed command sessions (Fig. 8.c) and the mean number of failed signal sessions (Fig. 8.d) are increased in Scenario 3, with respect to the Scenarios 1 and 2. This is due to the occurrence of both causes of command and signal session failure.

As described in Sec. 2, we consider a session as failed if more than one acknowledgment or signal is missing when the time out expires. We now define the **Scenarios 1***, **2*** and **3***, characterized by the same threats occurring in the Scenarios 1, 2 and 3 respectively, but assuming that a session is failed when all the acknowledgments or signals are missing when the time out expires. Still by means of SAN simulation, we compute the same measures defined at the begin of this section, in the new scenarios. In the Scenario 1^*, the value of all measures is equal to 0 for any time between 0 and 10000 h: according to the rates about intrusions in Table 2 and the 0.01 probability to not discard a fake command (Sec. 2), this one may be executed by a subset of

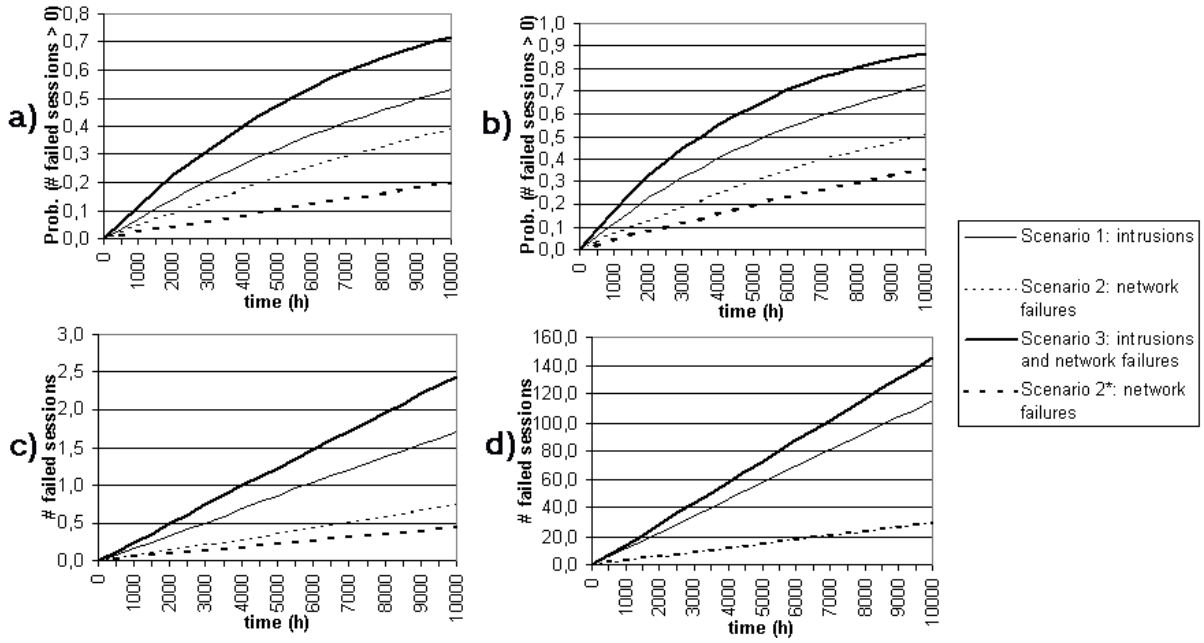

Figure 8: The simulation results: a) $Pr_{com}(t)$. b) $Pr_{sig}(t)$. c) $Num_{com}(t)$. d) $Num_{sig}(t)$. During 10000 h, the mean number of command sessions is about 1665, while the number of signal session is about 112500.

substations causing their temporary failure, but not by all the substations. Therefore the number of missing acknoledgments (signals) will never be equal to $N = 10$, and a command (signal) session will never fail. In the Scenario 2^* instead, a complete set of acknowledgments or signals is missing only if both $NET1$ and $NET2$ are failed; if only one communication network is available, a session can not fail because the network bandwidth is enough to avoid the loss of all the packets. Finally, in the Scenario 3^*, the occurrence of both threaths does not significantly increase the measure values, with respect to the Scenario 2^*. Therefore in Fig. 5, we show only the results obtained in the Scenario 2^*. For all the measures of interest, the values obtained in such scenario are lower than those in the Scenarios 1, 2 and 3. This depends on the fact the complete loss of a set of acknowledgments or signals is significantly less probable than the loss of at least two of them.

6 Conclusions and future work

This paper has taken in exam several communication scenarios between one control centre and a set of substations exchanging commands and signals inside an area of a distribution grid, where the communication reliability may be affected by intrusions, network failures, or both. The scenarios have been modelled, simulated and evaluated by means of SAN, quantifying the effect of the threats, in terms of probability and quantity of lost data.

The case study can be extended by taking into account several countermeasures to the threats affecting the communication: **1.)** we may consider that each time a substation is recovered from the failure due to the execution of a fake command, the substation protection is improved, so the probability to execute a fake command is decreased. **2.)** We may deal with the possibility that more than two networks are available, and the same packet is trasmitted on a subset of them in order to increase the probability of delivery, still considering the possibility to replace the networks under failure, with the available ones. This would require to model some kind of routing protocol. **3.)** We may suppose that if too many acknowledgments are missing at the end of a command session, we could repeat the session one or more times. So the session would be considered as failed if all the attempts have no success.

Other scenarios can be evaluated by means of SAN, for instance the communication inside the larger transmission grid where commands are transmitted from the transmission grid control centres to the control centres into the distribution grids. We may consider the effects of the communication failures on the regulations functions perfomed by the physical infrastructure, such as the voltage regulation and the teleoperation [3]. Other threats to the communication can be considered, such as denial of service (DoS) attacks [3] or the unavailability of substations or control centres, caused by the failure of its internal components. In this case, we may consider the possibility of a backup control centre.

Acknowledgments. This work has been partially supported by the Project CRUTIAL IST-2004-27513.

References

[1] CRUTIAL project's web page. http://crutial.cesiricerca.it.

[2] D. Cerotti, D. Codetta-Raiteri, S. Donatelli, C. Brasca, G. Dondossola, and F. Garrone. UML diagrams supporting domain specification inside the CRUTIAL project. *Lecture Notes in Computer Science*, 5141:106–123, 2008.

[3] F. Garrone(editor), C. Brasca, D. Cerotti, D. Codetta-Raiteri, A. Daidone, G. Deconinck, S. Donatelli, G. Dondossola, F. Grandoni, M. Kaaniche, and T. Rigole. *Deliverable D2: Analysis of new control applications*. CRUTIAL project, http://crutial.cesiricerca.it, January 2007.

[4] C. L. DeMarco and Y. Braden. Threats to electric power grid security through hacking of networked generation control. In *Int. Conf. on Critical Infrastructures (CRIS)*, Alexandria, VA USA, 2006.

[5] G. Dondossola, J. Szanto, M. Masera, and I. Nai-Fovino. Evaluation of the effects of intentional threats to power substation control systems. In *Int. Workshop on Complex Network and Infrastructure Protection (CNIP)*, Rome, Italy, 2006.

[6] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelley. Identifying, understanding, and analyzing critical infrastructure interdependencies. *IEEE Control Systems Magazine*, 21(6):11–25, 2001.

[7] W. H. Sanders and J. F. Meyer. Stochastic activity networks: Formal definitions and concepts. *Lecture Notes in Computer Science*, 2090:315–343, 2001.

[8] D. Deavours, G. Clark, T. Courtney, D. Daly, S. Derisavi, J. Doyle, W. Sanders, and P. G. Webster. The Möbius Framework and its Implementation. *IEEE Transactions on Software Engineering*, 28(10):956–969, 2002.

[9] D. Codetta-Raiteri and R. Nai. SAN models of communication scenarios inside the Electrical Power System. Technical Report TR-INF-2009-07-05-UNIPMN, Dip. di Informatica, Univ. del Piemonte Orientale, August 2009. http://www.di.unipmn.it.

Daniele Codetta-Raiteri received the Ph.D. in Computer Science from the University of Torino, Italy, in Feb. 2006. From June 2006 to Dec. 2007, he was a research assistant at CNIT, Italy. In 2008 and 2009, he has been a research associate at the University of Piemonte Orientale, Italy. His research focuses on stochastic modelling oriented to the dependability evaluation. Most of his work has regarded extensions to the Fault Tree formalism, the analysis of dynamic reliability cases, and multi-formalism modelling. He is the (co-)author of more than twenty papers published in proceedings or journals.

Roberto Nai received the M.Sc. in Computer Science from the University of Piemonte Orientale, Italy, in April 2008. His thesis concerned the modelling of communication scenarios inside the electrical power grid. Previously, he was involved in the dependability evaluation of communication systems for transportation vehicles. Now he works as a consultant and a high school teacher.