Quantifying the Impact of External Attacks on a Distributed Automatic Track Warning System

Leonardo Montecchi, Paolo Lollini, Andrea Bondavalli

Dipartimento di Matematica e Informatica, University of Firenze
Viale Morgagni, 65 – I-50134 Firenze, Italy
{lmontecchi,lollini,bondavalli}@unifi.it

***Abstract*—For several years, the vulnerability of Critical Infrastructures (CIs) to cyber-threats has been limited, since they were mostly isolated systems, using proprietary protocols. Nowadays, CIs are increasingly threatened by external attacks: the use of off-the-shelf components is common, they have become interconnected, and sometimes also connected to the Internet. This problem is exacerbated by the recent trend towards the adoption of wireless connectivity and mobile devices, which is gaining interest also in this domain. One of the main challenges is to quantify the impact that external attacks may have on the infrastructure, and ensure that its dependability and safety requirements can still be fulfilled. In this paper we focus on the ALARP system, which protects workers on the railway infrastructure using distributed mobile terminals, and evaluate the impact of two attacks to the communication infrastructure. In performing such analysis, we experiment with a new method, which combines a stochastic model of the system with a model of the attacker, and quantifies the impact of specific attacks on precise safety and availability metrics.**

Keywords*—railway, security, quantitative evaluation, vulnerabilities, 802.11

I. Introduction

For several years, the vulnerability of Critical Infrastructures (CIs) to cyber-threats has been limited, since they were mostly disconnected from the outside world and using proprietary components and protocols. This has slowly but continuously changed in the last decades, to the point that it is not uncommon anymore for CIs to use off-the-shelf components or to be (at least partially) connected to the Internet. Such trend has however increased the threat of external attacks, and cyberattacks are now one of the major concerns in Critical Infrastructures Protection. Recent data point to a 17-fold increase in the number of cyberattacks on U.S. infrastructures between 2009 and 2011 [26], and a 20-fold increase in the number of incidents in the same period [4].

Future critical systems need thus to devise mechanisms that are able to cope with security threats (e.g., identity verification mechanisms [7]), aiming at systems that are able to fulfill its dependability requirements even in presence of external attacks. In this perspective, one of the major challenges is to quantify the impact that attacks may have on a system, and understand if its dependability requirements can still be fulfilled in spite of that.

In this paper we evaluate the impact that attacks on the communication architecture of the ALARP[1] system produce on its dependability properties. The analysis applies the ADVISE method introduced in [14] for modeling the behavior of the attacker, combining it with a Stochastic Activity Networks (SAN) [25] model of the system behavior.

The paper is organized as follows. Related work is discussed in Section II, while Section III introduces the ALARP system. The models that have been used for the analysis are described in Section IV, while evaluations and results are reported in Section V. Finally, conclusions are drawn in Section VI.

II. Related Work

Model-based assessment has been applied for several decades for the purpose of analyzing properties of systems. One of the first formal models specifically tailored to security analysis is the Dolev-Yao model [9], which is commonly used to verify properties of cryptographic protocols through semi-automatic tools.

Attack trees [29] are a popular formalism for security analysis, and they are mainly used to qualitatively describe the possible ways in which an attacker can compromise the system, as well as the adopted countermeasures. Attack graphs [28] extend attack trees by introducing the notion of state, thus allowing more complex interactions between events and attacks to be described. More recently, methods and concepts that originated from the reliability domain have started to be applied to security analysis as well [20]. For example, some works employ the classical formalisms used for reliability analysis (e.g., Stochastic Petri Nets or Markov Chains) to quantify security-related system properties [8], [12].

The ADVISE formalism that we use in this paper has been introduced in [14]. The approach of ADVISE is to create executable security models combining information about the system, the adversary, and the desired security metrics to produce quantitative metrics data. The specification of an ADVISE model is composed of two parts: an Attack Execution Graph (AEG), describing how the adversary can attack the system, and an adversary profile, describing the characteristics of the attacker. An AEG differs from attack graphs in that it contains timing, cost, probabilistic outcomes and other information about each attack step. The *adversary profile* captures skills, preferences, goals and other characteristics of the attacker,

[1] ALARP: *A railway automatic track warning system based on distributed personal mobile terminals* [3].

which are used to determine, in the evaluation, which attack steps are executed. Further details on the ADVISE formalism can be found in [14],

The evaluation of critical infrastructures is addressed in several ways in literature, either by focusing on the overall workflow [15], on modeling formalisms [6], [10], on interdependencies [23], or on ad-hoc simulation frameworks [21]. Tradeoffs between performance and security have been evaluated using a model-based approach in [19]. In this paper we introduce an approach to quantify the impact of attacks on system dependability properties.

Concerning the ALARP system, a detailed description of the system architecture is provided in [27], while challenges faced in its design and evaluation are discussed in [17]. Starting from the models that have been used for safety and availability evaluation of the system [2], in this paper we extend the previous models and build new models in order to also consider the impact of two specific external attacks on the communication system.

III. The ALARP System

Safety of workers is a serious concern in the most industrialized countries. Surface transport workers are facing very high risks, since they often have to operate without service interruptions. In railway transportation the situation is even more peculiar, since vehicles are constrained to tracks and drivers have much less margins to react in case of emergencies, therefore exposing workers to higher risks of injuries and fatalities.

ALARP ("*A railway automatic track warning system based on distributed personal mobile terminals*" [3]) is a research project funded within the Seventh Framework Programme (FP7). Its objective was to design and develop an innovative Automatic Track Warning System (ATWS), to improve the safety of railway trackside workers. The ALARP ATWS is able to inform the trackside workers about dangerous events within the worksite, e.g., approaching trains on the track, maintenance events on power lines and/or safety equipment that may put at risk workers' safety.

The ALARP system is based on the following main components: i) one or more trackside Train Presence Alert Devices (TPADs), able to sense an approaching train on the interested track without interfering with the signalling system; ii) a set of distributed, low-cost, wearable, wireless Mobile Terminals (MTs), to inform the workers about possible approaching trains and/or other events that could put at risk their safety, and iii) infrastructure for wireless communication. Railway regulations require a Controller Of Site Safety (COSS) to supervise the workers team and take care of safety concerns. The ALARP system supports the COSS by providing additional functionalities to its MT.

The overall communication architecture follows a centralized approach, mainly based on a fixed coordinator (Access Point) located at the worksite, and all MTs communicating through it. The Real-time Group Communication Protocol [16] forms the basis of the worksite communication protocol. RGCP is based on IEEE 802.11, and relies on the coordinator for realizing a polling scheme of the MTs in a round-based fashion, allocating node slots via time multiplexing.

When a train approaches the worksite, it is detected by the TPAD, which sends a broadcast message, called "RISK_EVENT", to all the MTs in the worksite. Each MT, using its localization mechanism, determines if the worker is in a "red" (i.e., dangerous) zone, or in a "green" (i.e., safe) zone. The red zone is defined as a zone in the worksite that is not protected from rolling stock movements, or that is nearer to the track than the safe working limit prescribed by regulations. Green zone is the safe area outside of the limits of the red zone. When a MT receives a RISK_EVENT it generates an "Alert" or a "Warning" message to the user (i.e., the worker), depending on whether (s)he is located in the red zone or in the green zone.

While no trains are detected, each TPAD periodically sends an "I_AM_ALIVE" message to all the MTs in the worksite, in order to give evidence of its proper functioning. When a train is detected, the TPAD temporarily interrupts the transmission of I_AM_ALIVE messages, substituting them with RISK_EVENT ones. When a MT detects a malfunction (e.g. missing I_AM_ALIVE messages), it moves to a *safe state*: the MT signals to the worker that it is not able to properly function and halts its services. As a consequence, the worker should move to the nearest green zone. While this mechanism guarantees the system safety, it may have a strong impact on its availability, especially in presence of external attacks as it will be shown in Section V.

A. ALARP Vulnerabilities

In order to quantify the impact of external attacks, we first analyzed the main vulnerabilities of the system. Due to its complexity, the ALARP system is exposed to different classes of vulnerabilities. For example, an attacker could try to physically access the MTs or the TPADs in order to inject malicious software; (s)he could try to degrade the hardware of the components themselves; (s)he could try to manipulate the preloaded maps in the MTs in order to invert red zones and green zones, or (s)he could try to exploit some common vulnerabilities of the GPS system (used by the localization mechanism). In this paper we focus on vulnerabilities of the communication architecture. In particular, we consider two common vulnerabilities of the IEEE 802.11 standard [13], described in the following.

1) Deauthentication attack [5]: The 802.11 MAC layer provides functionalities designed to address problems specific to wireless networks. In particular, these includes the ability to discover networks, join and leave networks, and coordinate the access to the radio medium. Identity vulnerabilities arise from the implicit trust that 802.11 networks place in a speaker's source address. Nodes are identified at the MAC layer with globally unique 12 byte addresses. A field in the MAC frames holds both the sender's and the receiver's addresses, as reported by the sender of the frame. For most management and control messages, standard 802.11 networks do not include any mechanism for verifying the correctness of the self-reported identity. This is the case also of the *deauthentication* message, which is discussed in the following.

According to 802.11, after a client has selected an access point (AP) to be used for communication, it must first authenticate itself to the AP before further communication may take place. The authentication protocol includes a message that allows clients and APs to explicitly request deauthentication from each other. This message is not authenticated using any keying material. An attacker may thus spoof this message, either pretending to be the access point or the client, and direct it to the other part. In response, the recipient of the message will exit the authenticated state and will refuse all further packets until authentication is reestablished. By continuously repeating such attack a client may be indefinitely prevented from transmitting or receiving data.

2) Jamming attack [22]: The shared nature of the medium in wireless networks makes it easy for an adversary to perform a wireless Denial of Service (DoS) attack. Such attack can be very easily accomplished using off-the-shelf equipment. To give a simple example, a malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called *jamming* and the malicious nodes are referred to as *jammers*. Therefore, we define a jammer as an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. There are different techniques of jamming: from the “constant jammer” that continually emits radio signals on the wireless medium in order to corrupt packets, to the “reactive jammer” in which the attacker constantly senses the channel and upon sensing a packet transmission it immediately transmits a radio signal in order to cause a collision. For power efficiency reasons, a jammer may alternate active periods, in which he actively performs jamming, to sleeping periods. Note that current standards for wireless data communications do not prevent jamming. For example, the physical layer of IEEE 802.11 does not support error correction. As a result, the jammer can release just enough power to corrupt a single bit in order to cause a whole packet to fail the CRC check. The reason for this protocol specification is that wireless systems have been designed only to be resilient to non-malicious interference and to noise. A jammer can exploit this and efficiently use low power in order to disrupt the entire communication.

IV. Analysis Model

In this section we provide an overview of the models that have been used to quantify the impact of attacks on the ALARP system. The models combine i) a *system model* in the Stochastic Activity Networks (SAN) formalism [25], and ii) an *attacker model* in the ADVISE formalism [14]. The modeling process that was adopted is based on a model composition approach [18], in which the model of the system is built composing sub-models, each one capturing a specific part of the system; models are then composed using the Join/Replicate formalism [24]. The work described in this paper considers a scenario with 20 MTs (including the COSS MT) and 2 TPADs.

A. System Models

Within the project, a modeling framework for the quantitative evaluation of the system-level ALARP dependability properties has been defined [2], [17]. The ALARP evaluation framework includes a stochastic model of the system, realized using the SAN formalism.

The model, which is fully described in [2], allows different measures related to the safety and availability of the overall ALARP system to be evaluated. The two main supported measures of interest are the following:

- $P_{catastrophic}(0,t)$: probability that a catastrophic failure occurs in the time interval $[0,t]$. A catastrophic failure occurs when i) workers are not notified within the time bounds imposed by ALARP safety requirements [1], or ii) workers are incorrectly notified with a “Warning” instead of an “Alert”.
- $A_N(0,t)$: portion of time in which at least N MTs are in operational state within the interval of time $[0,t]$. This metric is of primary importance to the owner of the railway infrastructure, as it provides an indication of the amount of time the workers are not able to work due to the unavailability of safety measures.

The model takes into account the main aspects of the ALARP architecture, and it supports the interaction with more detailed analysis techniques [17]. For example, the model is able to represent: i) train approaching the worksite, ii) different layouts of railway tracks within the worksite, iii) detection of trains by TPADs, iv) transmission of messages between TPADs and MTs, v) transition of MTs to safe state and recovery, vi) the COSS MT functionalities.

Within the project, the framework has been used to evaluate safety and availability metrics under nominal working conditions, i.e., without external attacks. Such results are reported in [2]. In this work we based on such existing models, adapting them in order to be able to integrate them with attack models in the ADVISE formalism. In particular, we inserted some hooks in the model of network communication in order to represent the effect of attacks (e.g., the corruption of messages due to successful jamming).

B. Attack Models

The attacks described in Section III-A have been modeled using ADVISE. In this section we detail the model for a jamming attack following the “reactive jammer” scheme; the model for the deauthentication attack follows a similar approach and it is not described here due to lack of space.

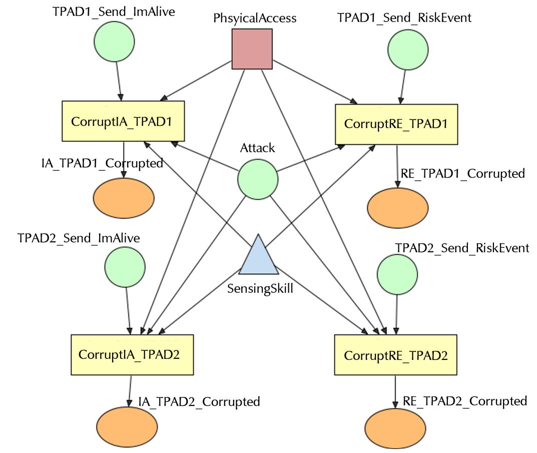

Fig. 1: ADVISE AEG for the jamming attack.

The Attack Execution Graph for the jamming attack in an environment composed of two TPADs is shown in Figure 1.

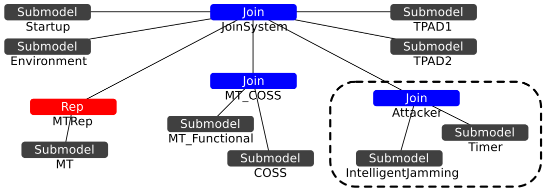

Fig. 2: Composed model for the ALARP system under jamming attack. In the dashed region the models that have been added to represent the behavior of the attacker.

The knowledge item `Attack` is shared with a place in the SAN model Timer, which is used to represents an attacker who alternates a silent period to an attack period. The knowledge items `TPAD1_Send_ImAlive`, `TPAD2_Send_ImAlive`, `TPAD1_Send_RiskEvent` and `TPAD2_Send_RiskEvent` are shared with the corresponding places in the SAN models that represent the behavior of the two TPADs in the considered scenario. When these places contain a number of tokens greater than zero, the corresponding TPAD is sending a message on the network (I_AM_ALIVE or RISK_EVENT).

One of the four attack steps presented in the AEG is executed according to the detected message. If the attack step terminates with a success the corresponding attack goal is reached. All the attack steps require physical access to the network and a specific level of skills to sense the channel.

These conditions are described by the following code, that represents the precondition for the attack step `CorruptIA_TPAD1` (others attack steps have similar preconditions):

```
return (!IA_TPAD1_Corrupted−>Mark() && PhysicalAccess−>Mark()
        && Attack−>Mark() && TPAD1_Send_ImAlive−>Mark() > 0
        && SensingSkill−>Mark() > skill );
```

The attack steps execution time is exponentially distributed with rate equal to the inverse of `execTime` parameter. Each attack step has two possible outcomes: *success*, which occurs with probability $(1 - fp)$, and *failure* which occurs with probability fp. To each of possible outcomes is associated a detection probability.

ADVISE permits to define different adversary profiles. To evaluate the measures of interest considering different adversary profiles, the parameters related to the adversary profile are set using global variables, which assume different values in the various experiments.

C. Composition

SAN models (that represents the functionalities of the system and its components) and ADVISE models (that represents the behavior of the attacker) are then composed using the Join/Replicate state-sharing formalism [24], which allows composing models using the *join* and *replicate* operators.

The composed model represents the system in presence of an attacker and it is shown in Figure 2 (for the case of a jamming attack). It is important to note that, using this approach, the system model and the attacker model can be developed (or refined) in isolation, which leads to obvious advantages. For example, the task of building the model can be split between two different teams of experts.

V. Evaluations and Results

In this section we discuss the evaluations that have been performed on the model, and the obtained results. The measures of interest have been evaluated by discrete events simulation using the Möbius-ADVISE tool [11]. Starting from the models described in previous section, the metrics described in Section IV-A have been studied considering different adversary profiles, in order to verify the impact of the attacks on the system.

Different profiles are considered varying `cost weight`, `detection weight` and `payoff weight` of the attacker, i.e., the importance (s)he gives to reducing costs, avoiding being detected, and maximizing profit [14]. Furthermore, other studies have been conducted varying the `detection probability`, the `failure probability` and the time required for the attacker to complete each attack step (`execTime` parameter). The measures of interest defined in Section IV-A have been evaluated considering a mission length of 8 hours (i.e., $t = 28800$ seconds), corresponding to a typical working day.

The experiments conducted on existing models of the system, which did not consider external attacks, evaluated the probability of catastrophic failure ($P_{catastrophic}(0,t)$) under different system conditions [2]. The results described the main relations between system parameters and the target measures. In the experiments we conducted on the modified models we did not observe any increase in this metric due to the introduction of external attacks due to deauthentication or jamming attacks.

This is of course the expected behavior of the system, and it is the main purpose of introducing the "safe state" mechanism of the MTs. When a MT does not receive I_AM_ALIVE messages from TPADs for a certain period of time (e.g. due to a jamming attack), it moves to the safe state and the worker is alerted of the failure of the system. Similarly, if the attacker is able to prevent the reception of RISK_EVENT messages (e.g. due to a deauthentication attack), the MT moves to the safe state because TPAD stops sending I_AM_ALIVE messages when it detects a train on its controlled track. In both cases the safety of workers is not affected.

While the considered attacks don't impact on the safety of the system, they affect the system availability. To quantify such impact, we evaluated the measure of interest $A_N(0,t)$ for $N = \{20, 10, 1\}$, corresponding respectively to the fraction of time in which: i) *all MTs are available*, ii) *at least* 50% *of all MTs are available*, and iii) *at least one MT is available*.

Figure 3 shows the results obtained for the availability at varying of the execution time for each attack step, in the case of jamming attack.

The results show that the availability of the system is heavily affected by the amount of time required to the attacker to perform a jamming. The objective of the attacker is to send an impulse on the communication channel when it detects messages in transit. These messages require a certain period of time to reach the destination, therefore the attack must be fast

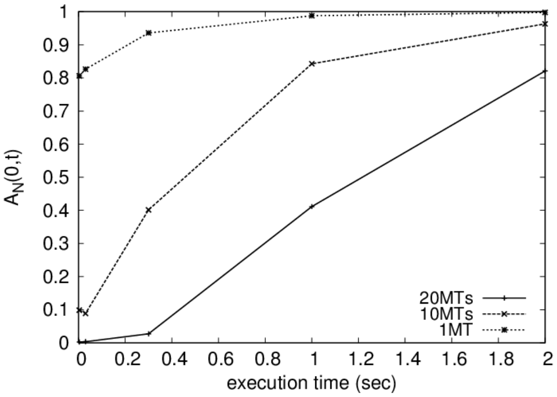

Fig. 3: $A_N(0,t)$ at varying the execution time of attack steps.

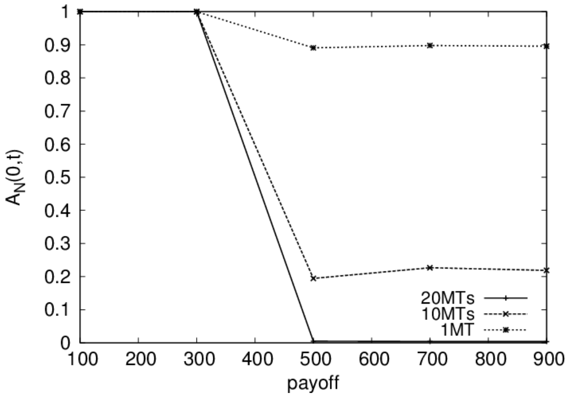

Fig. 5: $A_N(0,t)$ at varying the payoff of each attack goal.

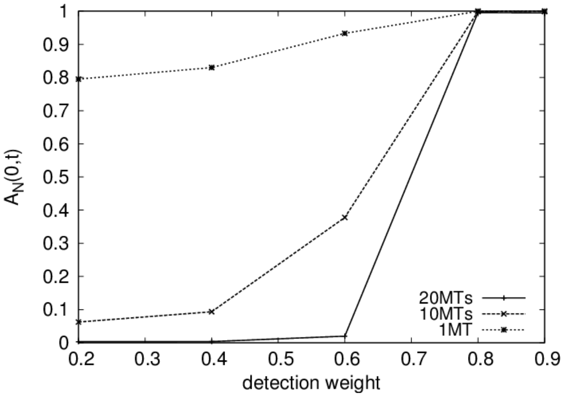

Fig. 4: $A_N(0,t)$ at varying the detection weight in the adversary profile.

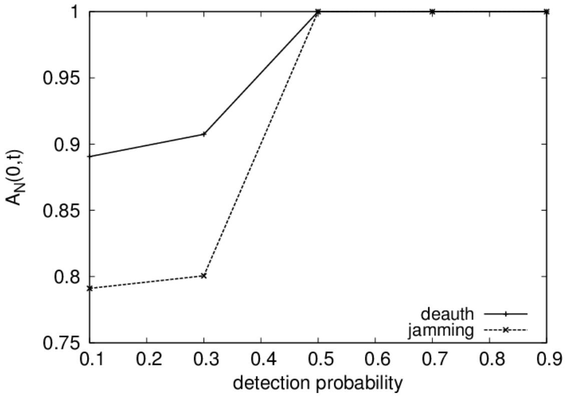

Fig. 6: $A_1(0,t)$ at varying the detection probability in the two attacks

enough to achieve its goal. For this reason, the availability of the system increases at the increasing of the execution time. In particular, when the execution time is equal to 2 sec, $A_1(0,t)$ reaches the maximum value, $A_{10}(0,t)$ is around to 95% and $A_{20}(0,t)$ is greater than 80%.

Another important parameter is represented by the detection weight. This quantity represents the importance that the attacker associates with the risk of being detected while trying to attack. Figure 4 shows the results for the availability at varying of this parameter. As expected, the results show that the availability of the system increases with the increasing of detection weight. In particular, when the detection weight is greater than or equal to 0.8, the attacker considers the *donothing* attack step more attractive than any other attack step. In this case $A_N(0,t)$ assumes the maximum value for all considered values of N, since in this case the system is not attacked. Attack appears however to be effective for values of the detection weight less than 0.8. For example, the probability that all of the MTs are available during the whole mission is less than 2% for values of detection weight less than or equal to 0.6.

Figure 5 shows the results for the availability at varying the payoff that the attacker associates to each of the attack goals (the payoff is the same for all the attack goals). The objective of this experiment is to identify the limit below which the attacker pays more attention on the risk of being detected, with respect to the gain that would get completing the attack with success. Results show that for values of payoff up to 300, the attacker considers the *donothing* attack step more attractive than any other attack step. In these cases the availability reaches the maximum value; for values of payoff greater than 300 the availability is instead drastically reduced.

Similar results for availability are obtained in the case of deauthentication attack with some differences between the case in which the objective of the attacker is to disconnect MTs from the network, and the case in which the attack is made against the TPADs. Finally, in Figure 6, we present a comparison between jamming attack and deauthentication attack against the MTs at varying the detection probability. The jamming attack is more efficient than the deauthentication attack. This is because in the former case it is sufficient for the attacker to corrupt a certain number of consecutive I_AM_ALIVE messages in order to rend unavailable all of the MTs; in the latter case the attacker is required to disconnect each MT one by one through a sequence of malicious deauthentication requests.

The effectiveness of the two considered attacks on the availability of the system is a side effect of the safe state mechanism of the MTs: if the attacker is able to prevent the correct delivery of messages, the MT detects a malfunction and halts its services, thus decreasing the system's availability. While this behavior was expected, and due to the fail-safe design of the system, it has a strong impact on the availability of the system. Depending on the expertise of the attacker, the probability that at least one MT is available may drop below 80%, and the probability that *all* MTs are available is near to zero, i.e., in that case the attacker is always able to put at least one MT into the safe-state.

VI. Concluding Remarks

In this paper we have used a model-based approach to quantify the impact of external attacks on the dependability of the ALARP Automatic Track Warning System (ATWS). The analysis has been performed by combining a SAN model of the system, with an ADVISE model of the attacker.

The obtained results highlight that, thanks to the safe-state mechanism of the MT, deauthentication and jamming attacks have no impact on the probability of occurrence of a catastrophic failure (i.e., potential loss of workers' lives) occurs. However, the same mechanism has a strong impact on the system availability: in certain conditions the attacker is always able to put at least one MT into a safe-state. While such tradeoffs are a typical aspect of critical systems, being able to quantify such dependencies is a valuable tool in the design of safety-critical systems and infrastructures. Furthermore, this kind of analysis has permitted a comparison of the impact potentially caused by the two different attacks.

The analysis we performed in this paper has also been the opportunity to apply a new analysis method for security assessment of complex systems, in which security models in the ADVISE formalism have been combined with existing models of the system, built using the SAN formalism. Future work will be devoted to apply the presented approach to security analysis of national critical infrastructures.

Acknowledgments

This work has been partially supported by the TENACE PRIN project (n. 20103P34XC) funded by the Italian Ministry of Education, University and Research, and by the DEVASSES project, funded by European Union's seventh framework programme under grant agreement PIRSES-GA-2013-612569.

References

[1] ALARP: D1.2 "Requirements Specifications" (June 2010)

[2] ALARP: D6.1 "Quantitative Modelling of ALARP Solutions" (January 2012)

[3] ALARP: "A railway automatic track warning system based on distributed personal mobile terminals" – FP7-IST-2010-234088, http://www.alarp.eu/

[4] Alcaraz, C., Zeadally, S.: Critical control system protection in the 21st century: Threats and solutions. IEEE Computer (2013)

[5] Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: Proc. 12th USENIX Security Symposium (2003)

[6] Bondavalli, A., Lollini, P., Montecchi, L.: Graphical formalisms for modeling critical infrastructures. In: Flammini, F. (ed.) Critical Infrastructure Security: Assessment, Prevention, Detection, Response, pp. 57–73. WIT Press (2012)

[7] Ceccarelli, A., Montecchi, L., Brancati, F., Lollini, P., Marguglio, A., Bondavalli, A.: Continuous and Transparent User Identity Verification for Secure Internet Services. IEEE Transactions on Dependable and Secure Computing (To Appear) (2015)

[8] Chiaradonna, S., Lollini, P., Di Giandomenico, F.: On a modeling framework for the analysis of interdependencies in electric power systems. In: 37th Dependable Systems and Networks (DSN'07). pp. 185–195 (June 2007)

[9] Dolev, D., Yao, A.C.: On the security of public key protocols. Information Theory, IEEE Transactions on 29(2), 198–208 (1983)

[10] Flammini, F., Vittorini, V., Mazzocca, N., Pragliola, C.: Critical Information Infrastructure Security, Lecture Notes in Computer Science (LNCS), vol. 5508, chap. A Study on Multiformalism Modeling of Critical Infrastructures, pp. 336–343. Springer (2009)

[11] Ford, M.D., Keefe, K., LeMay, E., Sanders, W.H., Muehrcke, C.: Implementing the ADVISE Security Modeling Formalism in Möbius. In: Proc. of the 43rd International Conference on Dependable Systems and Networks (DSN'13). Budapest, Hungary (June 24-27 2013)

[12] Houmb, S.H., Sallhammar, K.: Modelling System Integrity of a Security Critical System Using Colored Petri Nets. In: Proceeding of Safety and Security Engineering (SAFE 2005). pp. 3–12. WIT Press, Rome, Italy (2005)

[13] IEEE Standard for Local and Metropolitan Area Networks, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007 (June 12 2007)

[14] LeMay, E., Ford, M., Keefe, K., Sanders, W., Muehrcke, C.: Model-based security metrics using adversary view security evaluation (advise). In: 8th International Conference on Quantitative Evaluation of Systems (QEST 2011). pp. 191–200 (September 2011)

[15] Leszczyna, R., Fovino, I., Masera, M.: Approach to security assessment of critical infrastructures' information systems. Information Security, IET 5(3), 135–144 (2011)

[16] Mock, M., Nett, E., Schemmer, S.: Efficient reliable real-time group communication for wireless local area networks. In: EDCC (1999)

[17] Montecchi, L., Ceccarelli, A., Lollini, P., Bondavalli, A.: Meeting the challenges in the design and evaluation of a trackside real-time safety-critical system. In: 4th IEEE Workshop on Self-Organizing Real-Time Systems (SORT 2013). Paderborn, Germany (2013)

[18] Montecchi, L., Lollini, P., Bondavalli, A.: A DSL-Supported Workflow for the Automated Assembly of Large Performability Models. In: Proc. European Depend. Comput. Conf. (EDCC). pp. 82–93 (2014)

[19] Montecchi, L., Nostro, N., Ceccarelli, A., Vella, G., Caruso, A., Bondavalli, A.: Model-based Evaluation of Scalability and Security Tradeoffs: a Case Study on a Multi-Service Platform. Electronic Notes in Theoretical Computer Science 310(5), 113–133 (January 2015)

[20] Nicol, D.M., Sanders, W.H., Trivedi, K.S.: Model-based evaluation: from dependability to security. IEEE Transactions on Dependable and Secure Computing 1(1), 48–65 (Jan-March 2004)

[21] Pederson, P., Dudenhoeffer, D., Hartley, S., Permann, M.: Critical Infrastructures Interdependency Modeling: A Survey of U.S. and International Research. Tech. rep., Idaho National Laboratory (INL) (August 2006)

[22] Pelechrinis, K., Iliofotou, M.: Denial of service attacks in wireless networks: The case of jammers. Communications Surveys & Tutorials, IEEE 13, 245–257 (2011)

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

[24] Sanders, W.H., Meyer, J.: Reduced base model construction methods for stochastic activity networks. IEEE Journal on Selected Areas in Communications 9(1), 25–36 (1991)

[25] Sanders, W.H., Meyer, J.F.: Stochastic activity networks: formal definitions and concepts. In: Lectures on formal methods and performance analysis, pp. 315–343. Springer-Verlag, New York, NY, USA (2002)

[26] Sanger, D.E., Schmitt, E.: Rise Is Seen in Cyberattacks Targeting U.S. Infrastructure. New York Times (July 26 2012), http://www.nytimes.com/2012/07/27/us/cyberattacks-are-up-national-security-chief-says.html, last accessed April 21, 2015.

[27] Seminatore, A., Ghelardoni, L., Ceccarelli, A., Falai, L., Schultheis, M., Malinowsky, B.: ALARP (A Railway Automatic Track Warning System Based on Distributed Personal Mobile Terminals). In: TRA 2012. p. 10. Elsevier Ltd (2012)

[28] Sheyner, O., Haines, J., Jha, S., Lippmann, R., Wing, J.: Automated generation and analysis of attack graphs. In: Security and Privacy, 2002. Proceedings. 2002 IEEE Symposium on. pp. 273–284 (2002)

[29] Ten, C.W., Liu, C.C., Govindarasu, M.: Vulnerability assessment of cybersecurity for scada systems using attack trees. In: Power Engineering Society General Meeting, 2007. IEEE. pp. 1–8 (24-28 2007)