Cyber Security of Smart Grids Modeled Through Epidemic Models in Cellular Automata

Giulia Cisotto and Leonardo Badia
Dept. of Information Engineering, University of Padova, via Gradenigo 6B, 35131 Padova, Italy
email: {cisotto, badia}@dei.unipd.it

***Abstract*—Due to their distributed management, smart grids can be vulnerable to malicious attacks that undermine their cyber security. An adversary can take control of few nodes in the network and spread digital attacks like an infection, whose diffusion is facilitated by the lack of centralized supervision within the smart grid. In this paper, we propose to investigate these phenomena by means of epidemic models applied to cellular automata. We show that the common key parameters of epidemic models, such as the basic reproductive ratio, are also useful in this context to understand the extent of the grid portion that can be compromised. At the same time, the lack of mobility of individuals limits the spreading of the infection. In particular, we evaluate the role of the grid connectivity degree in both containing the epidemics and avoiding its spreading on the entire network, and also increasing the number of nodes that do not get any contact with the cyber attacks.**

***Index Terms*—Smart grid; cyber security; graph theory; cellular automata; epidemic models; Internet of Everything.**

I. Introduction

THE KEY to the success of smart grids, i.e., their ability of distributed and autonomous control, is also a big vulnerability in terms of cyber security [1]. Smart metering, wireless connectivity, and integration with other infrastructures for communication and control offer an unprecedented level of flexibility and easy management for the power grid. Since electricity provisioning represents a key requirement of contemporary life, changing it from an isolated subsystem to a networked service is certainly welcome [2]. At the same time, it also opens the door to several cyber security threats. Among the many reasons why cyber security of smart grids should be a sensitive issue, we mention two serious problems that may occur when these systems are attacked by an adversary.

First, smart grids are a critical infrastructure for our society and an appealing target for terrorism or any similar attack that has the intent of creating havoc [3], [4]. Increasing their automation and cyber inclusion makes them also easier to hack and control remotely, thus reducing the effort and cost for malicious operations, in the same way as it happens for legitimate network management.

Second, the integration of smart grids with the overarching Internet of Everything [5] may be the backdoor to the diffusion of attacks from the smart grid to the entire Internet, and vice versa. Every security weakness of the smart grid may be exploited in this sense; especially, any cyber intrusion of Trojan-horse kind for the Internet can find its gate of Troy in the smart grid.

978-1-5090-2185-7/16/$31.00 ©2016

These problems are exacerbated by smart grid access points being generally low-cost devices, such as sensors or meters with power-line or wireless connectivity [6], which are relatively easier to hack and take control of. There have been proposals to increase their inherent security based on distributed approach, e.g., by utilizing network coding [7], but still a fundamental problem remains, that is, due to their decentralized nature and high penetration rate, even in buildings with low level of access security, smart grids are inherently vulnerable to malicious tampering.

In this paper, we propose a contribution that may help understanding and designing countermeasures against cyber attacks to smart grids. Generally speaking, the dissemination of a digital threat over a network can be compared, as proposed by certain contributions, to an epidemic spread [8]. Also, note that this is not limited to malicious content: the "viral" diffusion of useful information can be modeled in this way, too [9].

Epidemiologists have developed some widely applied models to characterize these phenomena [10]. Often, *compartmental models* are employed, where the individuals are divided into different groups. For example, the famous "Susceptible, Infectious, Recovered" (SIR) model, developed by Kermack and McKendrick in 1927 [11], assigns each member of the population to one of these three groups and determines the evolution of the disease through the transitions of the individuals through the three states. Depending on the kind of disease that the model aims at capturing, further states can be added and the transitions can be made more complex. This kind of studies is deemed to be very valuable to study the evolution of epidemics as well as preliminarily assess the effectiveness of countermeasures such as quarantines or vaccines.

However, most of the times compartmental models are applied over simplified assumptions, especially considering a closed population in an extreme small-world context, that is, every node is in direct contact with (and therefore can spread the contagion to) every other node in the network. To overcome this point, compartmental models can be superimposed to an underlying network structure as done in [12]. These models often refer to scale-free networks and similar structures, which many authors [13] argued to be suitable models for smart grid topologies. However, cellular automata [14] can be employed to this purpose too, and we claim that the description offered can be even more powerful.

The advantages of exploiting epidemic models over cellular automata to characterize the spread of security threats in a smart grid relate to the direct mapping of the locality principle that is very strong in this kind of systems [15]. Indeed, electric networks have special topological characteristics, with a small-world topology yet strongly localized with many connections among physically neighboring nodes [16]. Moreover, the structure is often regular; therefore, we can assume that cellular automata fit the network pattern better than other structures.

Up to our knowledge, this paper is the first to propose such a connection, and even more so for the specific case study of security threats in smart grids. More specifically, the present paper makes the following contributions. First of all, we review compartmental epidemic models, both from a general standpoint and more specifically applied to smart grids. For this latter point, we propose the application of these epidemic models to cellular automata, since we envision their suitability to represent the topological characteristics of smart grids. Moreover, we present several numerical evaluations related to the key parameters of our model. We show how the epidemic strength, modeled via the *basic reproductive ratio* R_0, is a key parameter. At the same time, the degree of the topology is also relevant in influencing the infection spreading. Finally, we propose to evaluate a subclass of the susceptible set, which we call the *Untouched* nodes, which are those nodes that are neither infected nor have any infected neighbor through the entire duration of the epidemic process. This class has an important physical meaning associated with the awareness of the cyber attack and the potential counteractions against it. We show that the trend related to this class is even more strongly dependent on the aforementioned topological and epidemic parameters.

The rest of this paper is organized as follows. In Section II we outline the background about epidemic models and cellular automata, and we discuss their applicability to represent a cyber attack to a smart grid. Section III presents the adapted model to the smart grid scenario. We discuss some numerical results in Section IV and finally we conclude in Section V.

II. Epidemic Models and Cellular Automata

Standard epidemic models, such as the SIR model proposed first by [11], assume that the population subject to the epidemic outbreak can be subdivided into three groups: the susceptible (S) individuals, that are healthy but can contract the infection, the ones that are already infected (I) and can further transmit the disease, and the recovered (R) individuals that have ended the infection cycle, and therefore have gained immunity (this can include the case where they died from the disease).

Such a model can be transferred to information technology contexts [9] by seeing the infected individuals as those who actively participate in the dissemination process of the viral content (regardless of its intent being malicious or not) over a network. The nodes belonging to the S class are therefore those that have not been contacted yet, but still can become active carriers of the content in the future, while recovered individuals are those that are outside the spreading process. For example, if we track the diffusion of a worm [8] capable of destroying smart grid operational capabilities, recovered nodes can either be those smart meters that have been compromised and no longer work, or conversely grid nodes that have been replaced or where countermeasures have been taken by their owners to eliminate the threat.

Thus, the SIR model considers three classes, whose cardinalities are denoted as $S(t)$, $I(t)$, and $R(t)$, as they are actually functions of the time index t. If the population consists of N individuals, then $S(t) + I(t) + R(t) = N$ at any time. Moreover, the following equations are introduced to determine the temporal evolution of the states [10]:

$$\begin{aligned} \frac{\mathrm{d}S(t)}{\mathrm{d}t} &= -\beta\, I(t)\, S(t) \\ \frac{\mathrm{d}I(t)}{\mathrm{d}t} &= \beta\, I(t)\, S(t) - \gamma I(t) \\ \frac{\mathrm{d}R(t)}{\mathrm{d}t} &= \gamma\, I(t) \end{aligned} \tag{1}$$

where β and γ are parameters whose setup is discussed in the following.

The model describes a general transition of the individuals contracting the disease from state S going through state I and eventually entering state R. Thus, β is the contagion rate, which in a homogenous population can be seen as depending on the probability of contact among the individuals and the conditional probability of contagion in case of contact. The model includes a term giving a marginal increase of I (and correspondingly, a marginal decrease of S) proportional to both S and I, since the higher the number of infected, the more likely for a susceptible individual to become infected, and, conversely, the higher S, the more likely for an infected individual to spread the disease. On the other hand, I marginally decreases proportionally to its value (and R increases of the same amount) with a recovery rate γ, which represents the reciprocal of the average infection duration.

As a side note, the entire model, and the system of equations (1), can be rewritten in a normalized version by dividing all variables by N. Also, since the goal is to describe an epidemics starting from a limited number of infections and spreading across the population, the initial condition for a normalized problem is often taken as $S(0) = 1-I_0$, $I(0) = I_0$, and $R(0) = 0$, i.e., by setting an initial fraction of infected individuals I_0 that is generally small. Thus, the key parameters are β, γ, and I_0, as well as N to evaluate the normalization.

Furthermore, it is usual to introduce the basic reproductive ratio R_0 as β/γ. Its physical meaning is the expected number of infections caused by an individual belonging to the *initial* share of the infected population (that is, I_0). This parameter is descriptively powerful: it is easy to prove that the infection propagates if and only if $R_0 > 1$, and the higher R_0, the stronger the ability to spread [10].

Remarkably, this elementary model is based on many underlying assumptions. First, the infection process is memoryless, since transitions only depend on the state at time t and the resulting differential equations only involve first-order derivatives. Moreover, there is no preferred direction of contagion within the population. Any infected individual can pass the disease to any susceptible one. In other words, the model brings to the extreme the assumption of *small world* [12].

For what concerns the population dynamics and the absence of memory, several extensions have been proposed in the literature [10], [17]. For example, it is possible to insert additional transient states in the epidemic evolution, such as the *exposed* state, which represents an incubation period before the infection proper. At the same time, births and deaths (from other causes than the disease) can be included as well. This is generally done for epidemics that can have a long timespan, so that the population dynamics becomes relevant. For our smart grid analysis, this is likely not needed; however, nothing forbids to include these extensions in our model as well.

Instead, our main contribution in the present paper is relaxing the modeling assumption that dictates all the nodes to be virtually capable of contacting each other. In reality, smart grids are strongly localized [15] and most communications involve neighboring nodes. Moreover, the topology is generally regular. Therefore, we propose the application of epidemic model for cellular automata [14] to this specific scenario.

Cellular automata [18] are discrete dynamical systems made of a lattice of identical elements, which can have a state chosen from a finite set of values. A common formulation is that of a grid where each element (cell) can be occupied by a living being. The evolutive behavior of the automaton is determined by local interactions of its cells. Cellular automata exhibit self-organizing behavior: very often they deterministically evolve toward an attracting state.

The application of the SIR model (or any other compartmental epidemic model) to cellular automata was first proposed by [14] and can be outlined as follows. Nodes are located in a fixed position of the automaton lattice and have known relationships of neighborhood with others. Instead of considering a single variable describing the state of the node related to the disease, the cellular automaton epidemic model takes into account the states of all the neighbors and defines an evolution through the steps of the disease that depends on local contagion and individual recovery rates.

We remark that such an extension was proposed by [14] with an entirely different purpose than what done here for the specific case of smart grid cyber security. Indeed, the goal of that paper was mostly to *recreate* the classic model evolution without resorting to differential equations; thus, the different approach is due to complexity reasons. Our claim is instead that cellular automata are more suitable to represent the spatial distribution of infected nodes throughout the network, as well as account for the localized nature of cyber attacks.

III. Epidemic Models applied to Cellular Automata for Smart Grid Cyber Security

We first outline the changes that we applied to the basic SIR model in order to make it better suitable for computer simulation and the application of the cellular automaton rationale. First, the SIR model is inherently deterministic. Its differential equations express the exact value of individuals changing state, not just average values. Instead, we took a randomized approach, in which contagion and recovery rates are just probabilities. Thus, our analysis returns the same results of the SIR model with a first order approximation. At the same time, we consider a discretized time, as discussed by [17]. This way, first-order derivatives can be rewritten as incremental ratios and the time increment can be set to $\Delta t = 1$.

Another relevant parameter is the *topological degree* that we denote as d. This is the number of neighbors that each node has got in the automaton lattice. As the cellular automata is homogeneous, the probability to transmit the disease over a specific link is set to β/d, in order to have a contagion rate equal to β. Hence, the SIR model can be empirically replaced by the algorithm whose pseudo-code is reported in Fig. 1.

```
while ($t < T_{\max}$)
 for $i \in$ set of infected users
  for $n \in$ neighbors($i$)
   if status($n$) $\neq$ susceptible, continue
   if rand() $< \beta/d$, status($n$)=infected
  endfor
 if rand() $< \gamma$, status($i$)=recovered
 endfor
$t++$; endwhile
```

Fig. 1. Pseudo-code of the SIR model implementation.

One can see that this implementation preserves the correctness of the equations of (1), only with a discretized time, as discussed previously. An example of realization for a network with 900 nodes disposed over a 30×30 grid in two dimensions, with topological degree $d = 4$ (i.e., the neighbors are those in the four orthogonal adjacent cells, also called the von Neumann neighborhood [19]) is shown in Fig. 2. Initially, 5% of the nodes are infected, with their individual positions randomly chosen in the lattice with uniform distribution. We show the network evolution during the infection propagation and subsequent recovery. The "temperature" values in the plots represent the recovered nodes with 2, the infected individuals with 1, and the susceptible nodes with 0 (or less, see later).

From the figure, it appears that an important separation

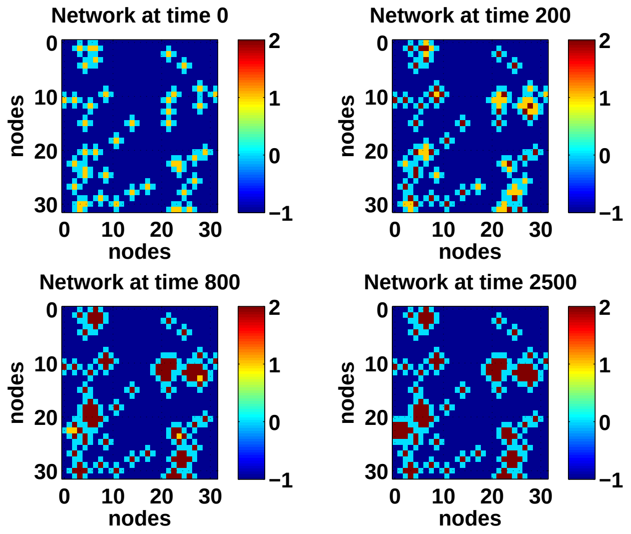

Fig. 2. An example of network with degree $d = 4$, with 5% initial infected nodes in a distributed attack scenario.

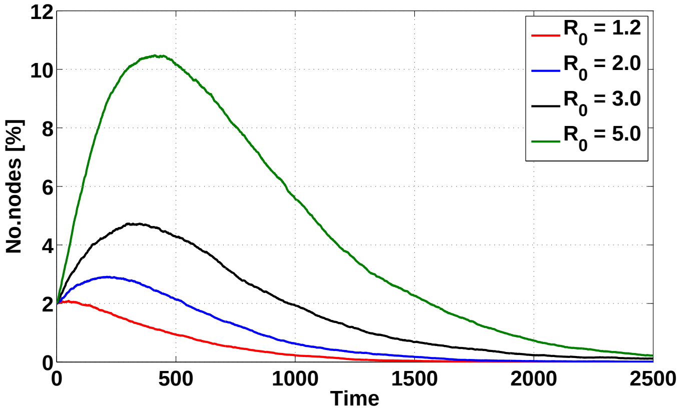

Fig. 3. Infected individuals over time, degree $d = 3$.

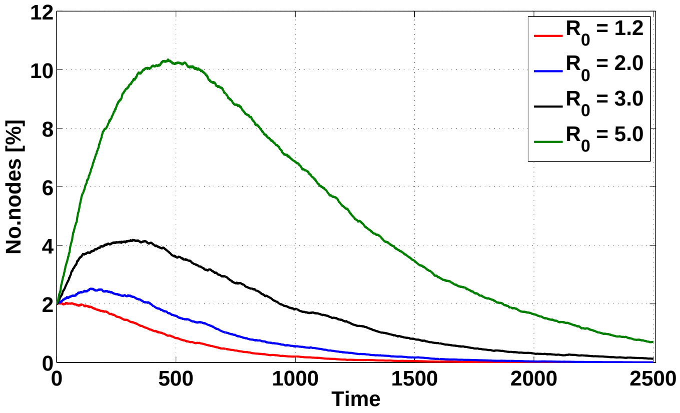

Fig. 4. Infected individuals over time, degree $d = 8$.

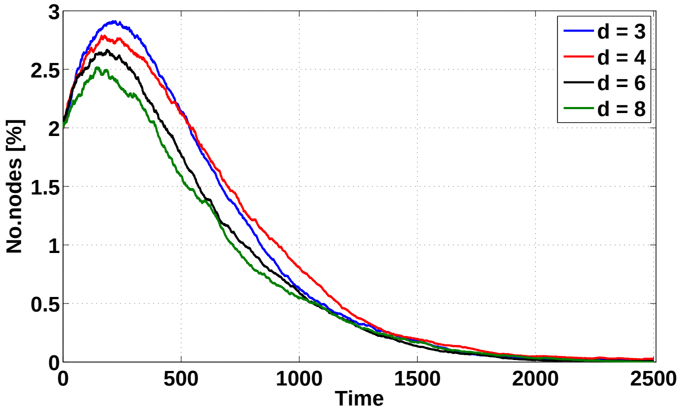

Fig. 5. Infected individuals over time, for different degrees, $R_0 = 2.0$.

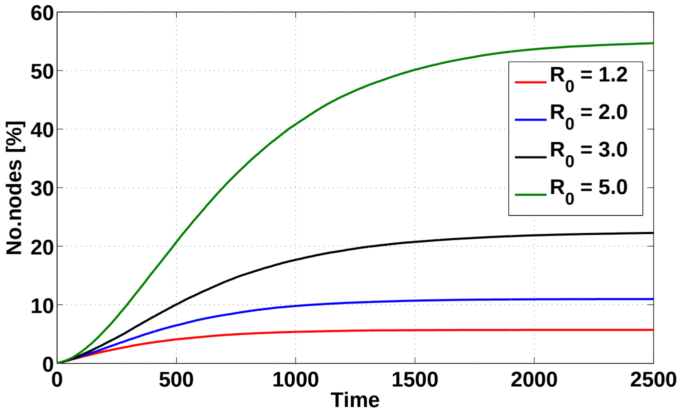

Fig. 6. Recovered individuals over time, degree $d = 3$.

can be made within the class S. Indeed, there are susceptible nodes that are fully surrounded by non-infected neighbors and therefore cannot contract the epidemics in the next round. Such nodes are not even aware that there is an ongoing infection spreading throughout the network. Thus, we split class S into two subclasses, denoted as S_0 and S_1. The former consists of all the “untouched” nodes, namely, those that have no infected neighbors, while the latter contains nodes with at least one infected neighbor. Fig. 2 represents untouched nodes with negative values. Cardinality-wise, it must hold that $S_0(t)+S_1(t) = S(t)$. In the following, we will discuss the role of these users in the network and their quantitative evaluation.

IV. Results

We considered a smart grid network represented as a cellular automata with 30×30 elements on a 2-dimensional plane. We simulated four different connectivity scenarios, namely, $d \in \{3, 4, 6, 8\}$. Values 4 and 8 were obtained by considering a square lattice, while degrees 3 and 6 were obtained translating the grid into a hexagonal lattice. The results are averaged over 150 simulation runs.

To simulate attacks of different strengths, we considered several values of R_0. Actually, the value of γ has been kept fixed to 0.005 (indeed, we tried other values and the results were found to be still consistent). Therefore, R_0 was simply tuned by setting a different value of β. Also, in all the results shown, the initial fraction of compromised nodes I_0 was set to 2%. Other values have been investigated but are not reported here due to space constraints. Nevertheless, their results are in full agreement with the ones shown. Finally, we considered two different configurations for the positions of the infected nodes at time 0. In most of the plots, we investigated a *distributed attack* scenario where these positions are randomly selected with uniform distribution over the lattice. However, we also considered a *compact attack* case, where the infected nodes at the beginning are all grouped at the center of the grid.

Figs. 3 and 4 report the evolution over time of the fraction of infected individuals, for two different degree, $d = 3$ and $d = 8$, respectively. Infections of different strengths have been considered. The trend is both quantitatively and qualitatively similar for both figures: the higher the basic reproductive ratio R_0, the higher the strength of the infection. The shape of the function is aligned with the result of a classic SIR model [9], [10], [17]. However, comparing the two figures, it is visible that the peak is slightly higher and narrower for the case with lower degree.

To better understand this trend and its implications, one can consider Fig. 5 where the evolution of the number of infected nodes over time is shown for different values of the topological degree, with $R_0 = 2.0$. Also, Fig. 6 considers the number of recovered individuals for the case of a topology with degree

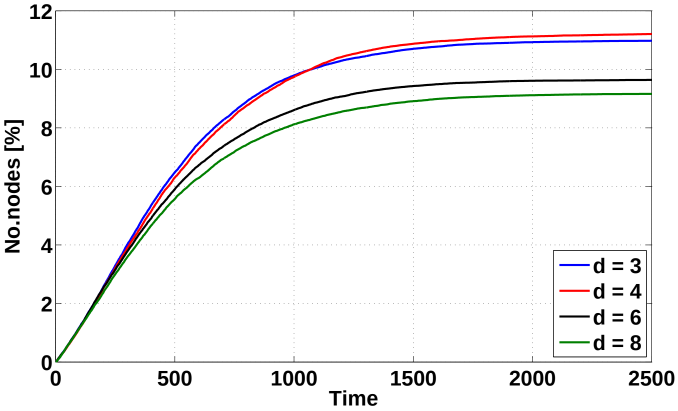

Fig. 7. Recovered individuals over time, for different degrees, $R_0 = 2.0$.

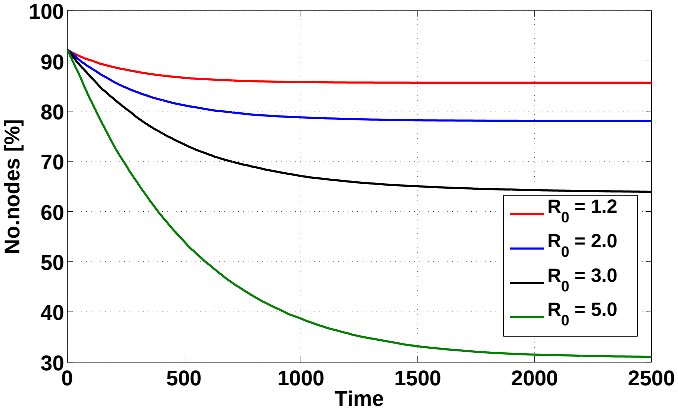

Fig. 8. Untouched individuals over time, degree $d = 3$.

$d = 3$ and various values of R_0. Since the equations start from $R(0) = 0$ and the model guarantees recovery of all nodes after a sufficiently long time, the asymptotic trend of the recovered individuals is also a measure of the nodes that were infected at any time of the simulation. From this figure, it is further emphasized that R_0 highly influences the number of nodes influenced by the attack: the case with $R_0 = 1.2$ leads to the contagion of very few nodes, while $R_0 = 5.0$ causes more than half the network to be directly compromised.

Similar to the previous discussion, the influence of the degree on $R(t)$ is shown in Fig. 7, focusing again on the specific case $R_0 = 2.0$. From this figure, as well as Fig. 5, it can be argued that a lower degree allow the attack to concentrate its diffusion towards fewer neighbors. In this way, the infection is slightly more effective. This may lead to considering the classic SIR model, and similar compartmental schemes, as not fully suitable for environments such as a smart grid. Indeed, classic models can be compared to a mesh topology with very high degree. Thus, this leads to slightly underestimate the extent of the attack.

Figs. 8 and 9 show instead the *untouched* individuals over time, for $d = 3$ and variable R_0, and $R_0 = 2.0$ and variable d, respectively. Our proposal in Section III was to split the susceptible class into subclasses S_0 (the untouched) and S_1. While the number of susceptible nodes can be simply derived by complementing the previous plots of $I(t)$ and $R(t)$, the behavior of $S_0(t)$ is more interesting. Indeed, these nodes have no contact whatsoever with the infection. This evaluation is therefore important to understand how many nodes actually use the protection against a security threat, so as to possibly assess an evaluation of costs versus benefits. It is possible that if the contagion model applied to the cellular automaton predicts that many individuals will not have an infected neighbor for the entire outbreak of the epidemics, there will be little interest for the owners of the network nodes to apply some local security protections. This kind of interactions can be better modeled via game theory [20], also involving multiple choices for the strategy of the attackers; indeed, this can enable the exploitation of the common roots of cellular automata and game theory. This kind of approach may be worth investigating as a future work.

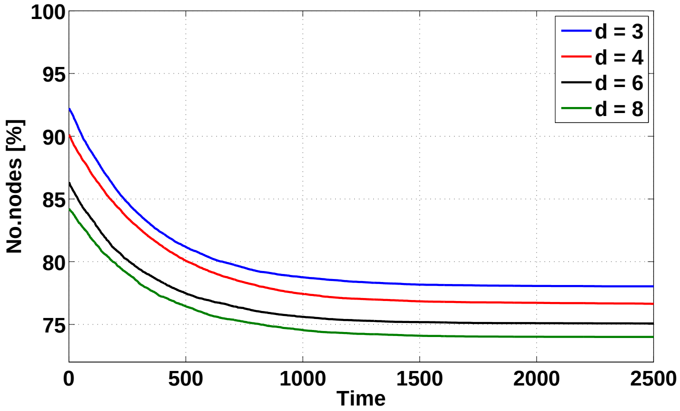

Fig. 9. Untouched individuals over time, for different degrees, $R_0 = 2.0$.

It is again shown by Fig. 8 that the stronger the infectivity, the lower the number of untouched nodes. However, Fig. 9 shows an interesting behavior in that the number of untouched nodes is slightly *increasing* with the degree. Clearly this is due in part to the definition of untouched node, since a higher number of neighbors leads to a lower probability that none of them is infected. Still, this result suggests that controlling the network topology might have contrasting results, since a lower degree increases the number of infected nodes, but also raises the number of nodes that do not perceive any attack.

Finally, Figs. 10 and 11 consider the case of compact attack. In all the previous results, a distributed attack was considered, while here we investigate a case with fixed $R_0 = 2.0$ and different degrees, and we plot the trend over time of $I(t)$ and $S_1(t)$, respectively. In this case, the extent of the attack is generally more limited. Fig. 10 shows that the trend of $I(t)$ is always monotonically decreasing; compare with Fig. 5, where a higher peak was reached in the case o a distributed attack. Fig. 11 shows that, for a compact attack, an increased number of nodes remain untouched, as they do not ever have any infected neighbor: while Fig. 9 showed an untouched rate between 70% and 80%, for a compact attack this value becomes around 90%. To sum up, since the network attacks start in a concentrated area, they are less effective. The differences in d are also less relevant, that is, all the values of the topological degree lead to similar curves. These results

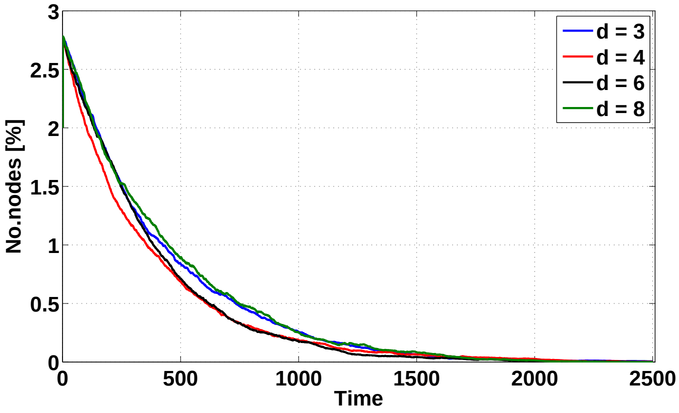

Fig. 10. Infected individuals over time for a compact attack, $R_0 = 2.0$.

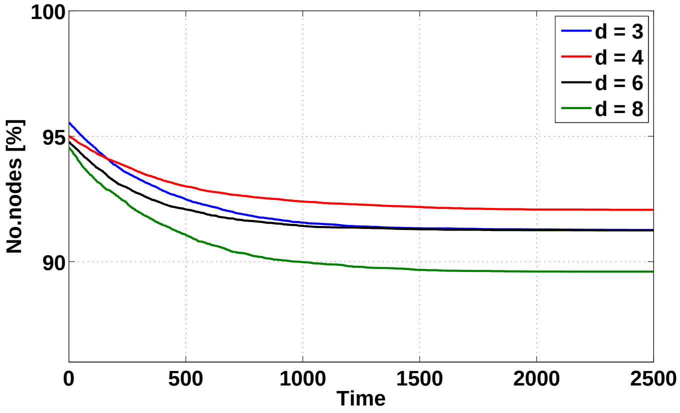

Fig. 11. Untouched individuals over time, for a compact attack, $R_0 = 2.0$.

prove that, in order to better exploit the decentralized nature of the smart grid, the adversary should disperse the injection of attacks. Conversely, a massive yet strongly localized attack to the smart grid would be less effective. Incidentally, this kind of conclusion is another point supporting the better descriptive effectiveness of cellular automata.

V. Conclusions and Future Developments

We presented an original quantitative approach to analyze security in smart grids based on epidemic models and cellular automata. As far as nodes in a smart grid can be looked at as individuals in a population susceptible to an epidemic infection, compartmental models can be exploited to predict the outbreak of a malicious attack and/or take effective countermeasures. To our knowledge, this represents an original contribution for future developments of security solutions for smart grids, which is an important yet overlooked aspect.

To support our approach, we presented results from simulations of different smart grid topologies. Three critical parameters were taken into account: the degree of the network, the infectious impact of the attack, and the locations of infected nodes in the network, that is, their proximity or distance from the source of contamination.

We have shown interesting trade-offs between connectivity and cyber infection diffusion. If the same infection strength is applied to different topologies, the networks with lower degree show an earlier and higher peak of the infection. The number of nodes involved in the attack is also larger. This implies that traditional compartmental models, where all nodes are in direct contact with each other (albeit with a smaller probability) can underestimate the extent of a cyber attack.

Moreover, we have also found that some nodes can remain untouched from the infection, thanks to their strategic location in the network. Importantly, the influencing parameters are the same as before (degree and infection strength) but the degree has the opposite behavior. This aspect can be further investigated in the future, when distribution of key elements of the smart grids, that can be access points or electricity sources, have to be carefully designed in order to lower down the probability of a cyber attack.

References

[1] W. Wang and Z. Lu, "Cyber security in the smart grid: Survey and challenges," *Comput. Netw.*, vol. 57, no. 5, pp. 1344-1371, 2013.

[2] G. Ericsson, "Cyber security and power system communication – essential parts of a smart grid infrastructure," *IEEE Trans. Pow. Deliv.*, vol. 25, no. 3, pp. 1501-1507, 2010.

[3] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645-658, 2011.

[4] A. Sargolzaei, K. Yen, and M. N. Abdelghani, '"Delayed inputs attack on load frequency control in smart grid," *Proceedings IEEE ISGT*, pp. 1–5, 2014.

[5] E. Spanò, L. Niccolini, S. Di Pascoli and G. Iannaccone, "Last-meter smart grid embedded in an Internet-of-things platform," *IEEE Trans. Smart Grid*, vol. 6, no. 1, pp. 468-476, 2015.

[6] V. C. Gungor, B. Lu, and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Trans. Ind. Elec.,* vol. 57, no. 10, pp. 3557-3564, 2010.

[7] R. Prior, D. E. Lucani, Y. Phulpin, M. Nistor, J. Barros, "Network coding protocols for smart grid communications," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1523-1531, May 2014.

[8] M. Nekovee, "Worm epidemics in wireless ad hoc networks," *New J. Phys.*, vol. 9, no. 189, 2007.

[9] A. Khelil, C. Becker, J. Tian, K. Rothermel, "An epidemic model for information diffusion in MANETs," *Proc. ACM MSWiM*, pp. 54-60, 2002.

[10] M. J. Keeling and P. Rohani, "Modeling infectious diseases in humans and animals", Princeton Univ. Press, 2007.

[11] W. O. Kermack and A. G. McKendrick, "A Contribution to the mathematical theory of epidemics," *Proc. Roy. Soc. A*, vol. 115, no. 772, pp. 700721, 1927.

[12] R. Pastor-Satorras, C. Castellano, P. van Mieghem, and A. Vespignani, "Epidemic processes in complex networks," *Mod. Phys.*, vol. 87, no. 925, 2015.

[13] G. A. Pagani, M. Aiello, "Power grid complex network evolutions for the smart grid," *Physica A*, vol. 396, pp. 248-266, 2014.

[14] M. A. Fuentes, and M. N. Kuperman, "Cellular automata and epidemiological models with spatial dependence," *Physica A*, vol. 267, pp. 471–486, 1999.

[15] S. F. Bush, "Network theory and smart grid distribution automation," *IEEE J. Sel. Ar. Commun.*, vol. 32, no. 7, pp. 1451-1459, 2014.

[16] Z. Wang, A. Scaglione, R. J. Thomas, "Generating statistically correct random topologies for testing smart grid communication and control networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 28-39, 2010.

[17] J. Satsuma, R. Willox, A. Ramani, B. Grammaticos, and A. S. Carstea, "Extending the SIR epidemic model," *Physica A*, vol. 336, no. 3-4, pp. 369375, 2004.

[18] S. Wolfram, "Universality and complexity in cellular automata," *Physica D*, vol. 10, no. 1-2, pp. 1-35, 1984.

[19] J. von Neumann. *Theory of Self-Reproducing Automata.* University of Illinois Press, Champaign, IL, USA, 1966.

[20] E. D. Demaine, "Playing games with algorithms: algorithmic combinatorial game theory," *Lect. Notes Comp. Sc.*, vol. 2136, pp. 18-33, 2001.