The network topology of connecting Things: Defence of IoT graph in the smart city

Marta Chinnici[1], Vincenzo Fioriti[2], Andrea Arbore[3]

[1] ENEA-ICT Division, C.R Casaccia Via Anguillarese 301, ROMA 00123, Italy
marta.chinnici@enea.it
[2] ENEA-ISER Division, C.R. Casaccia Via Anguillarese 301, ROMA 00123, Italy
vincenzo.fioriti@enea.it
[3] SiliconDev SpA, ROMA 00131, Italy
arborean@hotmail.com

Abstract. The Internet of Things (IoT) is a novel paradigm based on the connectivity among different entities or "things". IoT environment in the form of interconnected smart "things" represents a great potential in terms of effective and efficient solutions related to urban context (e.g., system architecture, design and development, human involvement, data management and applications). On the other hand, with the introduction of the IoT environment, devices and network security have become a fundamental and challenging issue. Moreover, growing number of users connected via IoT system necessitates focusing on the vulnerability of complex networks and defence challenges at the topological level. This paper addresses these challenges from the perspective of graph theory. In this work, the authors introduce a novel AV11 algorithm to identify the most critical and influential IoT nodes in a Social IoT (SIoT) network in a smart city context using ENEA Portici CRESCO infrastructure.

Keywords: IoT, Malware, Complex Networks, Graph Theory, Infrastructure, Smart City, Social Internet of Things (SIoT) network, Risks, Big Data.

1 Introduction

In a smart city context, the introduction of the Internet of Things (IoT) paradigm has become a fundamental concept: devices become pervasive and blend with human beings. It is the state wherein there is no distinguishable difference between the operation of devices surrounding us and our actions. Consequently, devices play an interactive role in the IoT systems and enhance the human experience. There is a seamless integration between us and the things around us. Various devices communicate intelligently with one another with minimal human intervention. Thus, devices of the IoT system are interconnected; they communicate with one another, transfer and retrieve data, intelligently respond to requests and trigger actions [1].
Hence, the introduction of the IoT in smart cities context involves the consideration of a vast number of aspects. These include system architecture, design and development,

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

use of embedded devices, communication technology, human involvement, data management and applications, security and privacy concerns. According to the reports by Cisco [2], Gartner [4] and Ericsson [3], 50 billion of heterogeneous devices will be connected to the Internet by 2020. These devices are getting increasingly smarter, connected to the global networks and among themselves, giving value to the IoT paradigm that is generating an unprecedented volume and variety of data. In [2] and [5], authors have estimated that the data caused by physical objects would reach 507.5 Zettabytes (ZB) per year (42.3 ZB per month) by 2019, which is 269 times more than the amount of data transmitted to Data Centers (DCs) from end-user devices and 49 times higher than total DCs traffic [13]. This brings up crucial discussion regarding all the data generated, stored or transmitted by IoT devices as well as its security and how this relates to the privacy of the users. Every approach of IoT system must have a secure network and provide a necessary level of control and privacy to the users. To accomplish these goals and then the success of the IoT systems' implementation, a baseline to build secure IoT network is one of the central aspects achievable with IoT graph topology.

Motivated by such challenges and inspired by graph theory, we aim to identify the most critical and influential IoT nodes in a Social IoT (SIoT) network [6] to address the way towards building a secure IoT environment for smart city context. This paper discusses security issues at the baseline level of IoT system and proposes topology of a graph, to target security challenges and vulnerabilities of different IoT systems. In detail, in this work the authors utilize a revised version of the AV11 algorithm [15] in a real SIoT network [21] to identify crucial infected nodes in the graph that corresponds to a set of key IoT systems (e.g., smartphone, laptop, computer, tablet, home sensors, etc). The procedure allows extracting information from the graph topology regarding the best k nodes (namely the "budget") to immunise or remove; thus, the remaining network is more robust to attacks. In IoT networks, the concept of attack handling can be translated to the identification of the IoT nodes that become "infected" in a specific configuration and hence, to defend the graph discovering these infected nodes become a crucial issue. Besides the defence concerns, the procedure also allows controlling virality of the network, identifying the most influential nodes (the influencers).

In summary, this work aims to investigate the network risk security based on the rapid deployment of IoT systems around the digital world. For IoT network, risk assessment is complex due to its vast deployment and diversity in terms of devices. Thus, traditional risk assessment frameworks do not adequately address the risk related to the topology of the network and then the risk assessment of IoT to be completed needs also to include a risk framework at a graph level.

The following objectives will support this aim:

a) Apply the algorithm AV11 for real IoT network [21] and provide the assessment risk framework;
b) Analyse topology structure of the network in terms of infective IoT nodes;
c) Perform data analysis to calculate statistics associated with the infective IoT nodes and hence, the graph topology in terms of devices;
d) Evaluate stability of the IoT graph with IoT devices configuration;
e) Assess the risk based on (a-d) in a real IoT network in a smart city context;

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

f) *Versus* risk assessment and mitigation of IoT dynamic network and future association of energy consumption of IoT device in the configuration network.

The paper is organized as follows: Section I – Introduction; Section II – Background: Related Works and AV11 Algorithm presentation; Section III – Methodology; Section IV – Assessment of an IoT graph; Section V – Conclusions and Future Works.

2 Background: Related Work & AV11 Algorithm

In recent years, significant research efforts and technological developments have been devoted to IoT paradigm [8] targeting energy efficiency of IoT systems. Indeed, these "things" enable new computing applications and represent the base of the vision of a global infrastructure composed of complex networked physical objects. According to [7], IoT systems represent the principal source of big data and, consequently, are the drivers of the plethora of applications, e.g. in smart cities [14]. Due to the inherently diverse nature of IoT paradigm, it attracts lots of risks in various forms. Therefore, understanding the processes and mechanisms involved in the evolution of complex networks for the IoT is a significant challenge.

Undeniably, in the IoT paradigm in smart cities context, mathematics plays an essential role in understanding complex networks. To address the networks with mathematical models, one is naturally led to dynamical systems, in which the graph describing the network is also a dynamical variable. The graph's dynamics is coupled with that of other variables not explicitly considered in the model. Analysis of such dynamics requires development of some new tools inspired by the graph theory [16, 17, 18]. Historically, the study of networks has been mainly a branch of discrete mathematics known as graph theory [9] that proves useful in understanding complex networks. The network structure is irregular, complex and dynamically evolving in time, with the main focus moving from the analysis of small networks to that of systems with thousands or millions of nodes, and with renewed attention to the properties of networks with dynamical units.

The complexity of the network structure poses significant challenges of capturing risks associated with the topological structure of the graph and risk assessment. In [10, 11, 12] a summary of the current literature related to fundament, kernel, methods, environment for IoT and associated risks is provided. Even if many efforts are addressed to IoT paradigm architecture, no investigation into the security aspects associated with the IoT graph in terms of complex network topology is present. Nowadays, IoT is missing security and in particular at the topologic level; for this reason, the security has emerged as a significant challenge for the IoT. Therefore, in this paper, the authors investigate topological and functional structures of an IoT network - where IoT system is represented by the nodes - to analyse the system and the specific infection nodes and malicious propagation attack. This study is based on the application of the algorithm AV11 [15, 22, 23] which intends to immunise or remove chosen nodes and make the rest of the network more robust and resilient to

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

attacks. With this analysis, we are also able to figure out intelligent and robust characters of IoT.

The application of our AV11 algorithm at the topological structure level of the graph is the baseline for the dynamic network analysis. In the paper, the authors also explore those intrinsic structures that are independent of data and methodology. The AV11 algorithm is a topological vulnerability tool, meaning that the vulnerability is taken into consideration according to a particular position of a node in a graph representing a technological network, such as an IoT network. In straightforward cases, such as the star, it is clear that the node in the centre is the most important/critical/influential one, but usually, for more complex topologies, the problem is not that trivial. The spreading of dangerous malware (malicious software) in networks of electronics devices has raised deep grave concern because infections may propagate from the ICT networks to other Critical Infrastructures producing a well-known domino effect. There are two diffusion strategies: targeted intrusion and cooperative search. The first strategy foresees a direct conventional approach to the actual target, while the second one demands a distributed control system, a sophisticated communication scheme and a consensus-like decision-making process. As a side effect of the cooperative search, the malware will spread in the network like a disease (the "epidemic" spreading). Actually, any worm follows the epidemic spreading, but a standard worm will attempt to invade the maximum number of machines as quickly as possible. In contrast, a sophisticated malware adopting a cooperative search strategy or even a simpler network aware approach will infect (relatively) few machines during an extended period. In any case, both seem to propagate following the epidemic spreading model, at least during the initial phase of the attack. Understanding this model may help to counteract the spreading at its very beginning when the cost of defence is more affordable. Researchers are attempting to develop a high-level analysis of malware propagation, discarding software details, to generalise to the maximum extent the defensive strategies. Since the maximum eigenvalue of the adjacency matrix of the network acts as a threshold for the malware's spreading [15], spectral analysis of the graph's adjacency matrix has a relevant role.

In this section, a brief description of the AV11 algorithm development by the authors is presented; the application of the algorithm to a specific IoT network will be shown in the next paragraph.

2.1 Description of AV11 Algorithm

The problem to be faced is: find k best nodes (the "budget") of an IoT network to immunise/remove them with the intention to make the whole network more resilient to malware attacks. Malware is malicious software designed to damage an ICT (Information and Communications Technology) network, often called viruses. Today viruses are net-aware in the sense that they can exploit vulnerabilities of the network, carefully selecting the critical nodes. Something similar could describe the spreading of faults, a well-known domino effect or cascade failure.

A defensive strategy should protect the most critical or influential nodes. Since, unfortunately, available resources are limited, to safeguard at most only k nodes of the network we should select them to maximise the probability to stop or reduce the

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

spread of the malware or the fault in the network. This is what we mean by "find the best k nodes". This task is not trivial since it is not clear what nodes are the most important in a network, because the interdependencies among them are often counter-intuitive. Thus, to identify these k nodes many algorithms have been used in the past years: degree, closeness, betweenness, Estrada indices, most infected, k-core, dynamical importance, and other [15, 19, 22, 23]. Standard topological centrality indicators such as degree, closeness, clustering, etc., are relevant quantities for assessing useful information. These parameters can also be employed to provide the first, non-trivial understanding of the network's dependencies, but are insufficient to unveil more subtle relations among the nodes, and as a matter of fact, spectral methods usually perform better. Even worse is the performance of the "most infected" strategy. According to this procedure, influential nodes that provide significant support to the epidemic spreading are the nodes that get infected more frequently during simulations. Our experiments demonstrate the weak points of this strategy. In the complex environment of the IoT, relying on such an approach could be extremely dangerous.

In this paper, we propose to solve the issue related to finding the best k nodes with our AV11 algorithm, which follows a combinatorial spectral paradigm [19] and has proved to be the most effective [15]. We use standard notation and terminology of graph theory and refer to the *network* as a *graph*, the *node* as a *vertex* and the *link* as an *edge* hereafter. Let G be the graph for it. It is well known that the largest eigenvalue λ_1 of a graph is related to a threshold for the epidemic propagation of a fault or a malware in the network [22]. If the ratio probability of infection, i.e. probability to cure is under this threshold, the spreading does not take place and vice versa [22]. Here, to "cure" means to provide an antivirus or some other kind of protection to the node/device. In practice, AV11 removes a set of k nodes and finds a sub-optimal decrease of the largest eigenvalue of the graph G as indicated in the pseudocode below. A brute-force strategy would be impossible to use even for small graphs, because of the vast number of combinations given that the problem is NP-complete [22]. Nevertheless, our suboptimal algorithm AV11 reduces the algorithmic complexity to $O(k \cdot n^3 \cdot \log n)$. However, it should be noted that even such a complexity is by far too cumbersome for a PC. Therefore, we have used the ENEA' infrastructure (CRESCO) to determine the most critical nodes from the adjacency matrix representing an IoT network [21]. Out of 16216 devices (nodes), 3300 were identified as the most critical ones. These 3300 nodes are those to be immunized somehow, since they guarantee to provide the maximum protection. It has to be considered that immunizing a node involves a non-negligible cost and that the available resources are scarce. In our case-study, the number of 3300 was chosen large enough to test the CRESCO potential, but actually, to determine the number of nodes to be immunized it would be necessary to run some Monte Carlo simulations to know the minimum number of nodes able to stop the spreading of the malware. Therefore 3300 it is crucial to refer only to verify the CRESCO calculation capabilities.

The AV11 pseudocode (see [15] for more details) is:

Input: the adjacency matrix A and an integer $0 < k < n$

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

Output: a set S with k nodes
Algorithm:
1. Calculate eigenvalues of the adjacency matrix A; let λ_1 be the largest eigenvalue;
2. Initialize: S to empty; $Z = I_n$; $D = \left(1 - \min_{i\in[1,n]} \mathbb{R}\mathrm{e}(\lambda_i)\right) I_n$; $node = 0$;
3. **for** $i = 0$ to k **do**
4. $P = (Z * A * Z + D)^p$;
5. $node = index\ of \max\left(\mathrm{diag}\,(P)\right)$;
6. Add $node$ to S;
7. Set $Z\,[node, node] = 0$;
8. **end for**;
9. **return** S.

Where, I_n is the identity matrix of order n and $0 < p \leq n$ is a parameter based on the longest cycle of the graph.

3 Methodology

This work focuses on IoT network graph assessment through a topology structure analysis using the AV11 algorithm [15, 22], particularly, on the evaluation of infected IoT-nodes [21]. To address this challenge, in this paper, we analyse real data of the IoT network consisted of 16216 IoT devices (nodes) provided by the authors in [21]. In detail, real IoT devices are available in the city of Santander and categorized in [6, 21] with respect to typologies and data model for objects introduced in the FIWARE data models [24]. As we have already mentioned, an experimental campaign which consists of the application of the AV11 algorithm to this real network is conducted by the ENEA infrastructure, on the Cluster named CRESCO4 (hosted by ENEA R.C. Portici). The principal goal is to calculate critical nodes of IoT devices and explore their characteristics. In this work, improvements have been made to previous studies conducted on the IoT environment concerning the topology and graph control. In particular, the authors provide an assessment of dynamical properties of the network through spectral eigenvalue analysis and also more in-depth knowledge of the IoT devices. Results are also expressed in terms of statistical data that could be generalized and applied in a real smart city context.
Briefly, the cluster CRESCO4 consists of 38 Supermicro F617R3-FT chassis, each hosting 8 dual CPU nodes. Each CPU, specifically an Intel E5-2670, hosts in its turn 8 cores, for a total number of 4864 cores. These CPUs operate at a clock frequency of 2.6 GHz. Moreover, the system is provided with a RAM memory of 4 GB per core. Computing nodes access a DDN storage system, for a total storage amount of 1 Pbyte. The connection between computing nodes is realized via an Infiniband 4xQDR QLogic/Intel12800-180 switch (432 ports, 40Gbps).

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

3.1 IoT graph in the smart city

As aforementioned, the authors consider as IoT network the case-study provided by the Santander testbed [21] of real IoT objects.

The Santander testbed considered in this current work as IoT network is composed of several thousand devices that comply with IEEE 802.15.4 standard (10-meter communications range with a transfer rate of 250 kbit/s), 200 GPRS modules and 2000 joint RFID, positioned at static locations (e.g., streetlights, bus stops) or mobile location such as on-board of vehicles (e.g., buses, taxis), in order to provide environmental monitoring, outdoor parking area management, mobile environmental monitoring, traffic intensity monitoring, guidance to free parking lots, parks and gardens irrigation, and participatory sensing. The general idea is to develop an architecture to support the smart city concept.

Briefly, we present characteristics of Santander IoT network used in this manuscript to apply the AV11 algorithm. The IoT objects are categorized with typologies and data model for objectives introduced by FIWARE Data Model and comprehend a total of 16216 devices, of which 14600 from private users and 1616 from public services. The following form has been used to describe network objects: id_device, id_user (owner id of device), device_type (category associated with a device in the form of code to differentiate between public and private devices from 1 to 16), device_brand (each device is assigned with a number from 1 to 12 encoding a brand), device model (it is associated with each device, a number from 1 to 24). The device_type code is provided to every object by the global Web Index 2017 [27] that identifies both the status (*static:* home sensors, PC, etc., or *mobile*: smartphone, car, etc.) and the type of device being private or public (Table 1).

Besides, the adjacency matrix is compiled by notions of Social Internet of Things (SIoT): social relationships between the nodes are established by a disjunction (OR) of five elementary relationships [6]. Mobile devices are carried with the users during their movements, while static objects are left in the users' home.

To simulate the user's movements, authors in [6] rely on a mobility model called Small World in Motion (SWIM). In this way, the authors of [6] obtained the estimate of the relationships between the devices on a given day, producing the 16216 × 16216 adjacency matrix of the Santander case study. In Figure 1 a Gephi [26] visualization of this network is showed. These datasets are freely downloadable from [21]; they are among very few ones available for IoT offering a valuable estimation of real-life phenomena.

Table 1 summarizes a legend of groups of devices: a code number identifies each group, also classified as public or private and static or mobile.

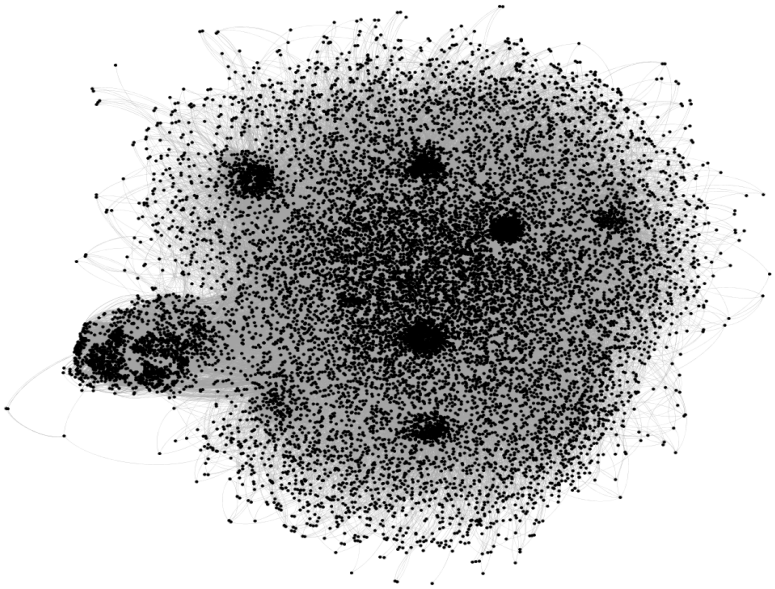
ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

Table 1. The first column is the code number defined by the device type and mobility characteristic provided in the second and third columns respectively.

Device Type	IoT-Device	Kind
1	Smartphone	Mobile
2	Car	Mobile
3	Tablet	Mobile
4	Smart Fitness	Mobile
5	Smartwatch	Mobile
6	PC	Static
7	Printer	Static
8	Home Sensors	Static
9	Point of Interest (specific point location that a user may find useful or interesting)	Static
10	Environment Weather	Static
11	Transportation (Vehicles, taxis or buses)	Mobile
12	Indicator (Digital signage to display information)	Static
13	Garbage Truck	Mobile
14	Street Light	Static
15	Parking (Location designed for parking)	Static
16	Alarms (Security supervisor or traffic monitoring)	Static

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

Figure 1. Gephi visualization of the graph representing the network of the Santander case study with all 16216 nodes.



4 Assessment of an IoT graph

As we have already mentioned, among topological analytical tools, the spectral description of networks deserves special attention. By its means, it is possible to infer insights on dynamical properties based on "static" parameters. Following Restrepo, Ott and Hunt [19] the authors focus on the largest eigenvalue of the graph adjacency matrix. This parameter (under a set of commonly accepted hypotheses) is closely related to the epidemic spreading of viruses or failures. The dynamical importance of a node (or an edge) [19] is defined as a normalised amount by which the maximum eigenvalue of the graph decreases if the node is removed. Therefore, if we remove a node, we can infer a measure of its "dynamical dependence" for all the other nodes employing the variation of the maximum eigenvector (the eigenvector of the maximum eigenvalue). Thus, if we consider a node (link), its dynamical importance will define its "importance" for the graph. The purpose of a network defence technique is to intervene in certain elements (the "budget") of the network to limit the impact of an attack or the spread of a virus or information.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

Our algorithm AV11 selects a subset of k nodes all at once according to spectral combinatorial methods, to immunize or remove them to make the remaining network more robust to attacks. In particular, AV11 classifies all the nodes of a graph according to a spectral parameter that describes dynamical properties of the graph's nodes in terms of the node influence on the network. A selected subset may be optimal or suboptimal, as a result of the brute-force method, and is not unique.
In [15] it is shown that the AV11 algorithm performs better than other selection techniques such as k-core in different topological scenarios. Note that although it might seem counterintuitive, the degree of centrality is not the best choice. In contrast, it often gives the wrong results. The same supposedly holds for the most important degree-like parameters, like k-core presented by the articles [15] [23] where the percentage of infected nodes is presented after the application of techniques to identify the immunizations nodes. Even more critical is the inferior performance of the "most infected" strategy. According to this procedure, influential nodes, i.e. those nodes that provide significant support to the epidemic spreading or the cascade effect, are those that get infected more frequently during simulations. Our experiments demonstrate how deceiving this idea is [22] [23]. In the complex environment of the IoT, relying on such a strategy could be extremely dangerous.

4.1 Data Analysis: Results & Discussion

In this paper, the authors have used the spectral algorithm AV11 to determine the first 3300 critical nodes on the IoT network created by the authors in [6] composed in total by 16216 nodes. Table 2 presents the first "best" ten nodes of 3300 classified by the algorithm to be protected from malware.

Table 2. The first ten nodes/devices of the IoT graphs from the AV11 analysis; they are all type 1 device, i.e. smartphones. The AV11 algorithm provides the value that is used to rank the importance of the node (third column); thus, these nodes are recognized as the most influential and need to be protected in the first place.

Classification	Node	Max_Eingevalue
1	247	364.837169
2	1407	363.841058
3	1521	362.846303
4	593	361.856203
5	728	360.910795
6	274	359.966537
7	240	359.021899
8	3631	358.075309
9	3322	357.135808
10	2314	356.211899

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

The algorithm goes like this: choosing a set of k nodes (in our case study $k = 3300$) simultaneously and removing them from the graph G, we obtain a new graph, and therefore we can calculate a new λ_1, smaller with respect to the old λ_1. Since the infection threshold depends on the inverse of λ_1 , the lower λ_1 the stronger the resilience to the infection spreading. Thus, we are interested in choosing k nodes that will provide the minimum possible λ_1. Moreover, AV11 provides an individual ranking for each of the k selected nodes (Table 2, third column AV11 value).
Then we analyse the major device groups (see Table 2) in order to provide some group statistics (Table 3).
For each type of group device, parameters taken into consideration are the number of devices in the group, the percentage of the total number of devices, mean and variance of the eigenvalues per group, eigenvalue sum per group and the percentage related to the total sum of the 3300 eigenvalues.
Therefore, within the subset of the 3300 nodes, the relevance of each device group concerning the transmission of any interaction to the whole network is represented by the sum per group of the eigenvalues of the group. For example, as shown in Table 3, the sum of the 375 eigenvalues of the type 2 devices accounts for 12.50% of the 3300 eigenvalues sum. Then the type 2 group is placed among the most influential of the network. In other words, since any physical action in the real world somehow finds a counterpart in the graph spectral analysis, the of contribution of each group type to the eigenvalue sum (see Table 3, last column) may be read as the relative relevance in the virtual world of the graph produced by real phenomena in the physical world.
The most relevant effect on the total eigenvalue sum is caused by smartphones, accounting for 27% of the total number of devices and 31.50% of the total eigenvalue sum. The second massive contribution comes from the PCs (25.70%), the third one from cars (12,50%). Smartphones, cars, tablets, printers and PCs represent 86% of the total sum of the eigenvalues, therefore are by far the most critical part of the network. However, it is immediately evident that some devices, namely 6, 7, 12, 13 (PCs, printers, indicators, trucks) even if not the most numerous, have high eigenvalue mean values, meaning that their impact on the network is important, despite the total number of devices.
It is particularly interesting to note the importance of indicators and printers since at present they are the favourite targets of hackers. Moreover, if we associate a cost to a device, it would be possible to produce a cost function describing the trade-off between the risk reduction provided by a security measure applied to a specific group of devices and the economic cost of the measure itself. Not surprisingly in this sense, it may be more affordable to spend more on the security of PCs, printers, indicators and trucks than on smartphones.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

Table 3. In the first column codes of devices are indicated, then for each type of device the following statistics are shown: the absolute number of that type of device present in the network, percentage of the device type related to the total number of devices, the average and the variance of the AV11 values per type, and finally the percentage of the eigenvalues of a type_device related to all the AV11 values.

Type_device	Nodes	%Nodes	AV11 value Mean	AV11 value Var	%AV11 Total
1	887	27	114	11399	31.50
6	535	16	155	9432	25.70
2	375	11.30	107	4654	12.50
15	361	10.90	33	208	3.80
7	317	9.60	99	3644	9.80
3	252	7.60	85	2519	6.60
14	141	4.30	54	1003	2.39
11	128	3.90	69	944	2.80
4	127	3.80	52	661	2.00
8	68	2.10	35	168	0.75
9	50	1.50	39	1136	0.61
10	27	0.82	93	9775	0.79
5	15	0.45	21	9	0.10
12	10	0.30	98	1799	0.31
13	7	0.21	138	15	0.30

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

In essence, the IoT environment will continue to increase in size and complexity. Therefore, a domino effect due to net-aware malware has to be considered probable and not only possible. Inherent vulnerability of IoT devices and structures exacerbate the problem to the point that does not allow an ex-post reaction of the attack, and it is not even viable to trust the enhancement of the IoT resilience. Thus, it is mandatory to rely on a formal ex-ante defence analysis, able to provide cost-effective countermeasures.

5. Conclusion and Future Works

In this paper, we proposed the AV11 algorithm and shown its applicability on a real IoT network example with the goal to provide an assessment framework based on the graph theory for the IoT network in a smart city context. The IoT network has been modelled as an undirected graph, and the nodes/devices have been classified according to a spectral technique able to identify the most influential nodes, i.e. the nodes that can propagate malware through the network. Since it was demonstrated [22, 25] that immunizing a small set of properly selected nodes can prevent or at least reduce the spreading, it is mandatory to identify these nodes in advance. Meanwhile, it is not a viable solution to immunise a large part of an IoT network, because of the vast number of devices. The economic advantages of the proposed algorithm are thus clear. For example, instead of concentrating the defence efforts on smartphones, it could be equally efficient but more economical to protect static assets such as computers, printers, indicators. Further, as part of future work, we aim to approach an IoT network dynamic risk assessment and mitigation and the association of the energy consumption of each device in the configuration network. Since limited research is devoted to topological structures of other complex networks for IoT in comparison with the investigation of IoT software technology and also to the ongoing investigation on the energy efficiency of the IoT devices, the authors aim to address in the future works these results on dynamic IoT network in smart cities context.

Acknowledgments. The authors would like to express their gratitude to the HPC research group at ENEA R.C. Portici to using ENEA Infrastructure for calculations.

References

1. D. M. Mendez, I. Papapanagiotou, B. Yang: Internet of things: Survey on security. Information Security Journal: A Global Perspective, 27(3), DOI:10.1080/19393555.2018.1458258, 2018.
2. E. Dave: The Internet of Things How the Next Evolution of the Internet Is Changing Everything. White Paper, Cisco, April 2011.
3. V. Hans: CEO to Shareholders: 50 Billion Connections 2020. White Paper, Ericsson, April 2010.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

4. Gartner: Gartner says 6.4 billion connected "things" will be in use in 2016, up 30 percent from 2015. http://www.gartner.com/newsroom/id/3165317. [Online; accessed 06-December-2016].
5. Forbes: 152,000 smart devices every minute in 2025: Idc outlines the future of smart things. http://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/#34bf983369a7. [Online; accessed 06-December-2016].
6. L. Atzori, A. Iera, G. Morabito, M. Nitti: The Social Internet of Things (SIoT) - When Social Networks meet the Internet of Things: Concept, Architecture and Network Characterization. Computer Networks, 56(16), Elsevier, 2012.
7. M. Chen, et al.: Big Data: Related Technologies Challenges and Future Prospects. Springer, 2014.
8. M. Chinnici, S. De Vito: IoT Meets Opportunities and Challenges: Edge Computing in Deep Urban Environment. In Dependable IoT for Human and Industry, Chapter 11, pp. 241-272, Ed. River Publishers, 2018.
9. R. V. Kranenburg, et al.: The Internet of Things. Paper Prepared for the 1st Berlin Symposium on Internet and Society October 25-27, 2011.
10. B. Yao, et al.: Applying Graph Theory To The Internet of Things. Proceedings of IEEE International Conference on High Performance Computing and Communications & IEEE International Conference on Embedded and Ubiquitous Computing, 2013.
11. V. L. Shivraj: A Graph theory based Generic Risk Assessment framework for Internet of Things (IoT). IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS), 2017.
12. D. Mendez, et al.: Internet of Things: Survey on Security and Privacy. In Information Security Journal A Global perspective, 2017.
13. M. Chinnici, A. Capozzoli, and G. Serale: Measuring energy efficiency in data centers. In Pervasive Computing Next Generation Platforms for Intelligent Data Collection, Chapter 10, pp. 299-351, 2016.
14. N. Dey, et al.: Internet of Things and Big Data Analytics. Springer, 2018.
15. A. Arbore, V. Fioriti, M. Chinnici: The topological defense in SIS epidemic models. Chaos Solitons and Fractals, 86, 16-22, ISSN: 0960-0779, 2016.
16. V. Fioriti, M. Chinnici, J. Palomo: Predicting the Sources of an Outbreak with a Spectral Technique. Applied Mathematical Sciences, 8(135), 6775-6782. HIKARI Ltd, ISSN: 1312885X, 2014.
17. V. Fioriti, M. Chinnici: Identifying sparse and dense sub-graphs in large graphs with a fast Algorithm. Euro Physics Letters, 108(5), ISSN: 0295-5075, 2014.
18. V. Fioriti, M. Chinnici: Node Seniority Ranking in Networks. Studies in Informatics and Control, ISSN 1220-1766, vol. 26(4), pp. 397-402, 2017.
19. J. Restrepo, E. Ott and B. Hunt: Characterizing the dynamical importance of network nodes and links: Phy. Rev. Lett 97, 094102, 2006.
20. Available at: http://www.smartsantander.eu/index.php/testbeds/item/132-santander-summary
21. Available at: http://www.social-iot.org/index.php?p=downloads
22. A. Arbore, V. Fioriti, "Topological Protection from the Next Generation Malware: a Survey", IJCIS 9(1/2): 52-73, 2013.
23. A. Arbore, V. Fioriti, "Sub-optimal Topological Protection Strategy from Advanced Malware", CRITIS 2011: 81-92, 2011.
24. Available at: https://www.fiware.org/developers/data-models/
25. D. Chakrabarti, Y. Wang, C. Wang, J. Leskovec, and C. Faloutsos: Epidemic thresholds in real networks. ACM Transactions on Information and System Security, 10(4), 1-26, 2008.

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7

26. M. Bastian, S. Heymann, M. Jacomy: Gephi: an open source software for exploring and manipulating networks. International AAAI Conference on Weblogs and Social Media, 2009.
27. Available at: https://cdn2.hubspot.net/hubfs/304927/Downloads/Trends-17.pdf

ICCS Camera Ready Version 2019
To cite this paper please use the final published version:
DOI: 10.1007/978-3-030-22750-0_7