future internet

Article

Towards Incidence Management in 5G Based on Situational Awareness

Lorena Isabel Barona López [†], Ángel Leonardo Valdivieso Caraguay [†], Jorge Maestre Vidal [†], Marco Antonio Sotelo Monge [†] and Luis Javier García Villalba [*,†]

Group of Analysis, Security and Systems (GASS), Department of Software Engineering and Artificial Intelligence (DISIA), Faculty of Computer Science and Engineering, Office 431, Universidad Complutense de Madrid (UCM), Calle Profesor José García Santesmases, 9, Ciudad Universitaria, 28040 Madrid, Spain; lorebaro@ucm.es (L.I.B.L.); angevald@ucm.es (Á.L.V.C.); jmaestre@ucm.es (J.M.V.); masotelo@ucm.es (M.A.S.M.)

* Correspondence: javiergv@fdi.ucm.es; Tel.: +34-91-394-7638

† These authors contributed equally to this work.

Academic Editor: Dino Giuli

Received: 11 September 2016; Accepted: 5 January 2017 ; Published: 17 January 2017

Abstract: The fifth generation mobile network, or 5G, moves towards bringing solutions to deploying faster networks, with hundreds of thousands of simultaneous connections and massive data transfer. For this purpose, several emerging technologies are implemented, resulting in virtualization and self-organization of most of their components, which raises important challenges related to safety. In order to contribute to their resolution, this paper proposes a novel architecture for incident management on 5G. The approach combines the conventional risk management schemes with the Endsley Situational Awareness model, thus improving effectiveness in different aspects, among them the ability to adapt to complex and dynamical monitoring environments, and countermeasure tracking or the role of context when decision-making. The proposal takes into account all layers for information processing in 5G mobile networks, ranging from infrastructure to the actuators responsible for deploying corrective measures.

Keywords: 5G; incidence management; information security; SDN/NFV; Situational Awareness

1. Introduction

The rapid proliferation of the use of mobile devices has revealed the lack of ability of the current networks to accommodate the vast amount of information that they will have to manage [1–3]. This situation has given rise to the development of a brand new generation of mobile networks not only to provide solutions to such problems, but also to improve many features of their predecessors. Enhanced capabilities, related to transfer massive data, interoperability or reduction in energy consumption, allow a better Quality of Experience (QoE) to the users [4]. Achieving these goals requires great capacity for innovation, such as high speed data transfers or better information management methods [5]. The last part has significant impact on business models based on services and real-time applications (e-health, e-security, Voice over IP, streaming, etc.), where emerging technologies, such as Software-Defined Networking (SDN) or Network Function Virtualization (NFV), facilitate pattern customization and management of the mobile network traffic. However, the development of these services is limited by the poor performance in the management and decision-making strategies [6], which additionally entails difficulty when deploying information security measures, the principal objective of this research. Nowadays, information security management plays a major role towards achieving the objectives and goals of companies and organizations. Traditionally, it has been carried out by implementing guidelines, standards and platforms that aim to protect their resources and assets (ISO/IEC 27000 [7], NIST-SP 800 [8], CVSS-SIG-First [9], MAGERIT [10], ITIL and COBIT [11], etc.).

However, these proposals have shown shortcomings when they are implemented in dynamic scenarios, where the context plays a very important role in decision-making [12]. This is the case of network-based monitoring environments, and more specifically, those that implement 5G technology, where the assets and events are considered highly dependent on the environment. As a solution to this problem, some authors have adopted incident management methodologies capable of handling information in a much more cognitive way, and, therefore, facilitating their understanding through contextual analysis. Worthy of special mention are those based on constructing Situational Awareness (SA) of the protected environment by applying the Endsley's model, where the perception, comprehension and projection of the system status are kept in mind [13]. The adaptation of this paradigm to the management of information security in networks has led to the coining of the term Network Security Situational Awareness (NSSA) [14]. Despite, however, its effectiveness having been proven in existing networks, it has not yet been considered to meet the challenges posed by 5G technologies.

To the best of our knowledge, there are few studies that survey Security and Risk Management in 5G Networks. In [15], a context aware framework for the next generation of Mobile Cloud Network (MCN) is proposed. This work introduces a "Context Generation and Handling Function" to provide enriched processing information from radio and core elements, taking into account two key-enabled 5G technologies (SDN and NFV concepts). Meanwhile, a recently published threat report has been conducted by the European Union Agency for Network and Information Security (ENISA) [16]. This work reviews the potential security in SDN/5G networks, considering not only SDN but also NFV and Radio fields. This report identifies the network assets and the security threats, their related challenges and risks. It also describes the existing security methods and provides good practices for 5G systems. These works could be considered part of the initial research of 5G Security Management. However, these are limited in scope. On one hand, the ENISA Report [16] identifies only the assets and threats to SDN/5G environments (no architecture proposal has been done). On the other hand, Marquezan et al. [15] propose a single network function that monitors radio and access elements but doesn't take into account other 5G components such as virtualization or application layers. Meanwhile, the 5G-Ensure Project is intended to cover security requirements in 5G Networks. The proposed architecture will provide a trustworthy 5G system, offering reliable security services to customers by means of the development of a set of non-intrusive security enablers such as privacy, security network management, and trust, among others [17]. As part of its proposal, 5G-Ensure defines a Risk Assessment and Mitigation methodology in order to evaluate security concerns in 5G systems, based on NIST-SP-800-30 and ISO 27005 standards [18]. Although 5G-Ensure covers a wide range of security issues on 5G Networks, this project is still at an early stage and does not keep in mind the concept of actuators, which have been introduced in our proposal in order to mitigate possible risks and deploy corrective measures. This article introduces a novel architecture for incident management on 5G Mobile networks, which combines the foundations of the traditional risk management guidelines with the Situational Awareness model published by Endsley. It covers all layers of information processing in 5G networks, from the infrastructure to the actuators responsible for implementing mitigation actions. The basis for the identification, monitoring, analysis, decision-making, prediction and countermeasure tracking are also introduced. The paper is divided into six sections, the first section being this introduction. The risk management systems, Situational Awareness and the related work are described in Section 2. The challenges posed by 5G networking related to risk management are explained in Section 3. An architecture that combines traditional risk management and Situational Awareness for 5G is detailed in Section 4. The componets to carry out analysis and decision-making processes are described in Section 5. Finally, conclusions and future work are presented in Section 6.

2. Background

The following describes the main characteristics of Information Security Risk Management (ISRM), Situational Awareness and the related works.

2.1. Information Security Incidence Management

The problems inherent to incidence assessment and management have captured the attention of the research community over the recent four decades. Consequently, several studies have been published in order to collect the most relevant contributions, as well as to identify the causes that have given way to their evolution, as it is described in [19,20]. The bibliography covers a very large collection of topics that range from the definition of risk and its scientific approach [21] to discussions about their development by different governments and organizations [22]. On the other hand, the need to protect the information technology has also led to the publication of standards [7–9] and guidelines [9,11] for their proper implementation. Most of these proposals agree that the incident management process must be carried out in the following steps: framing, assessing, monitoring and responding [20]. Risk framing determines the context and a common perspective on how organizations manage risk, which include their goals, policies, constraints, risk tolerance, priorities, trade-offs, and principles of action [7]. Incidence assessment identifies potential risks, organizational assets and vulnerabilities. Then, it evaluates the risks according to different criteria, such as likelihood of occurrence, capacity to inflict harm or dimensions (confidentiality, integrity, availability, authenticity, etc.) [9,10]. Because of its complexity [23], this is the step with the largest presence in the literature, which has motivated the development of specific systems for Information Security Risk Assessment (ISRA). In the monitoring step, the ISRM maintains awareness of the incidences being incurred, which implies looking for events in the monitoring environment that allow the detection of the previously determined threats. If any of them is identified, the response tasks decide and apply the appropriate countermeasures.

Due to the large differences between monitoring scenarios, the success of decision-making depends directly on the previously described processes and their ability to adapt to each use case. The following are examples of methodologies to facilitate their integration into more specific monitoring environments: Cloud Environments [24], industrial control [25], embedded systems [26] and Supervisory Control And Data Acquisition (SCADA) [27]. Given the nature of 5G devices and layers, it is important to track suspicious events in order to provide more intelligence to 5G security and monitoring systems [28,29]. Forensics are intended to collect, analyze and interpret digital data connected to a security incident in order to track an evidence trail (how an attack was carried out or how an event occurred). In the context of 5G mobile networks, these incidents might be related to physical and virtual devices as well as sensors, SDN/NFV functions and cloud elements [30].

2.2. Situational Awareness and Information Security

As defined by Endsley, the term Situational Awareness (SA) refers to "the perception of the elements in the environment within a volume of time and space, comprehension of their meaning and the projection of their status in the near future" [31]. Usually, this definition is simplified as "knowing what's going on so you can figure what to do" [32]. Thus, it is clear that its aim is to facilitate decision-making based on what is happening and its projection [13]. In order to acquire Situational Awareness, Endsley proposes three stages of information processing: perception, comprehension and projection; the first conducts the tasks of monitoring and identification of incidences, the second their analysis and association, and the last predicts the evolution of the state of the system. As shown in Figure 1, once relevant situations are detected, the countermeasures to be applied are decided and executed. It is important to highlight that there is feedback between action/decision levels and the Situational Awareness; in this way, the countermeasures and their impact on the system are tracked. The observed results have implications on future decisions and facilitate the use of advanced diagnostic methods [14].

Incident management based on Situational Awareness has been implemented in very different areas, among them smart grids [33], power generation [34] or vehicular collision avoidance systems [35]. In [36], a method for defining the critical information and the relevant information quality elements that are required to build the Shared Situational Awareness (SSA) in disaster response is suggested. The adaptation of the Endsley has proved particularly effective in complex and dynamic environments [37], where the diagnosis is highly dependent on the context in which incidents are reported, reaching to play an essential role in the fight against cybercrime. Many of these contributions are collected in [38], where the predominance of issues related to risk management in emergency situations, industrial systems and networks is observed. As discussed in [12], they improve the three most repeated deficiencies of the Information Security Risk Management: (1) Information security risk identification is commonly perfunctory; (2) Information security risks are commonly estimated with little reference to the current situation; and (3) Information security risk assessment is commonly performed on an intermittent, non-historical basis (a conventional security risk assessment scheme can only give a "snapshot" of the risks of the information systems at a particular time [39]). In order to bring solutions to these problems, but without losing focus on the ISRM/ISRA basis, several publications approach the combination of both paradigms. This is the case of [12,40], where the Situational Awareness is acquired, taking into account the definition of risks, assets and their impact posed by the different standards and platforms for ISRA implementation [7–11].

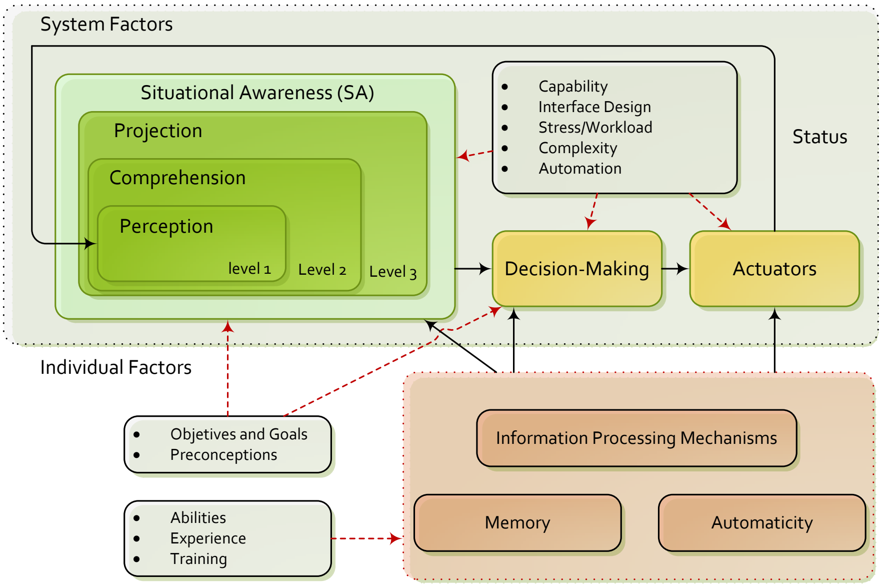

Figure 1. Endsley model for Situational Awareness.

3. Incidence Management in 5G

The new 5G design principles are intended to support an exponential increase of connected devices and, consequently, the data traffic moving through the network. In contrast to traditional mobile architectures, 5G requests a clear separation between data and control planes, a global vision of the network and a dynamic/customizable control of the mobile network operations. For this purpose, innovative technologies, such as SDN and NFV, have been extended to wireless and mobile platforms. In this way, the operators are not limited by the use of Command Line Interface (CLI) for individual and remote access. Instead, the administrator can create software or "network applications" to dynamically control the network behavior. However, the use of autonomous incident management systems that take advantage of these new paradigms is limited. In this context, the main challenge is the coordination between the virtual monitoring elements, allocated in different nodes in the infrastructure, and the response or mitigation procedures through the execution of actions in virtual functions. Similarly, mobile SDN/NFV-enabled architectures are limited by the lack of integrated schemes capable of analyzing large volumes of data, detecting potential risks and diagnosing their causes. Furthermore, the management systems should enable the definition, organization and handling of the different risks, assets and priorities without compromise the security and quality of service.

4. Information Security Architecture for 5G

The proposed architecture is mainly focused on autonomous risk management of 5G mobile infrastructures based on SDN/NFV architectures. In order to establish the coverage and limits of this approach, the following addresses the assumptions and requirements of the following design:

- The elements responsible for monitoring and executing mitigation actions (e.g., virtual functions) are compatible with the SDN/NFV paradigm. If the elements follow the traditional architectures, a compatibility layer is assumed. This additional layer can use the available configuration options to emulate a SDN/NFV enabled element.
- The communication between the different modules of the framework must be performed through secure channels.
- The information provided by the monitoring elements (low level metrics, alerts) are considered reliable.
- The Risk Analysis and the corresponding Situation Awareness procedures are strongly isolated from the data plane forwarding. In other words, the resources (network, storage and computing) used for the operation of the framework belong to administrative domain and, consequently, do not modify the capabilities of the 5G forwarding elements.
- The functional modules are extensible and can be implemented using distributed architectures in function of the available management resources and the size of the managed infrastructure.

The proposed architecture presents the synergy between 5G risk analysis and the Endsley model, and is depicted in Figure 2. The model describes four functional layers: Virtual Infrastructure and Sensors, Monitoring and Correlation, Analysis, and Decision-Making and Actuators. The Virtual Infrastructure executes the data forwarding engine and Sensors monitors the different metrics of the network. For its part, the perception, comprehension and projection principles of the Situational Awareness are applied in the Monitoring, Correlation and Analysis modules. The Decision-Making and Actuators complete the circle with the execution of proactive and reactive actions to optimize and solve problems located in the virtual infrastructure. The following sections of this chapter focus on the description of the Virtual Infrastructure/Sensors and Monitoring/Correlation.

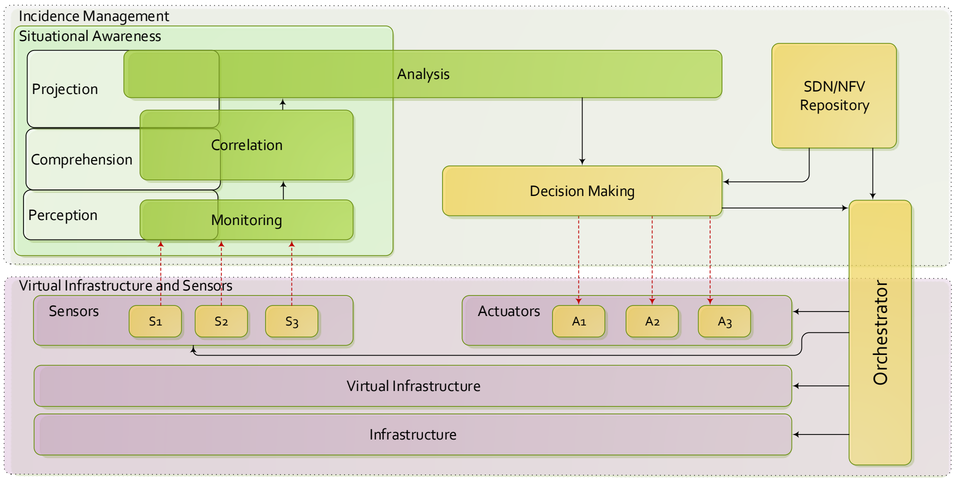

Figure 2. Endsley model for Situational Awareness.

4.1. Virtual Infrastructure and Sensors

The main purpose of this layer is the abstraction of the different hardware/software elements running in the mobile infrastructure and enabling the monitoring of low-level metrics related to the network behavior/status. Its developments includes the innovative designs principles of 5G networks: decoupling of data and control planes, virtualization of mobile functions, and a complete integration with cloud computing environments. In this way, the SDN architecture promotes the separation between data and control planes in mobile infrastructure (base stations, links, servers, gateways, Deep Packet Inspection (DPI), among others). The network administrator is not limited by the traditional private/closed hardware/software system and, consequently, the data forwarding engine can be customized. Similarly, the virtualization layer enables the dynamic allocation of virtual resources based on the user requirements. For its part, the NFV approach proposes the implementation of the different services (e.g., firewall, DPI, Quality of Service optimizer, load balancer) as virtual software functions that can be instantiated in different points of the virtualized infrastructure. As a result, the architecture considers two software applications types: SDN-Apps and NFV-Apps. SDN-Apps is executed in software programs to control the data plane in network devices and the NFV-Apps are virtual functions that can be instantiated in virtualized elements to develop a particular service. In the proposed architecture, the sensors are specialized NFV-Apps capable of monitoring different metrics on the system. Traffic analyzers, QoS analyzers, and anomalies/botnet/Distributed Denial of Service (DDoS) attack detectors are examples of sensors. These sensors (NFV-Apps) can be instantiated in different locations of the virtual infrastructure and reconfigured depending on the requirements of upper layers. Consequently, the system is able to increase the surveillance in suspected hazardous areas and establish quarantine regions.

4.2. Monitoring and Correlation

The monitoring module collects the information provided by lower layers (Virtualized Infrastructure and Sensors) and applies aggregation/correlation techniques to simplify the further analysis tasks:

- *Monitoring (Data Collection)*. The main objectives are the gathering and management of the information from all data sources, and facilitating their access to upper layers. Monitoring tasks would be able to actively poll different sources to collect real-time statistics, providing highly accurate and low overhead traffic measurement [41]. This module also controls the registration and access process of new sensors. The collected information is organized in efficient data structures, taking into account the large amount of data to be processed. In this regard, two scenarios were considered. In the first scenario, the sensor sends a report to the monitor when it detects relevant information (alerts, link failures, memory or CPU overload). In the second scenario, the monitor requests information (whenever necessary) to the sensors in order to facilitate the aggregation and analysis tasks (virtual topology, available links, among others).
- *Correlation*. It is responsible for the first abstraction level of information processing, in which, in order to have a global view of the network status, correlation and aggregation processes are executed. Information considered as redundant or non-sensitive is discarded. As an example, in case of multiple alerts received from each device belonging to the same affected area, a single alert is displayed with the affected topology. Due to the dynamism offered by virtual environments, in contrast to the rigidity of the physical elements, network topology is expressed as an extended or increased graph ($G_a(V_a, E_a)$), which models virtual nodes (V_a) and links (E_a) located in the physical infrastructure [42,43]. Likewise, as a result of correlation and aggregation operations, the received low-level metrics can be expressed or translated into high-level metrics, also known as Health of Network (HoN). For example, transmission data rate (Mbps), delay (ms) and jitter (ms) of data in streaming video, collected by the sensors at different points in the network, can be expressed as an overall perception of quality of service QoS/QoE, quantified by the measurement of the Mean Opinion Score (MOS).

5. Analysis and Decision-Making

This section describes the principal characteristics of the components related to analyzing the gathered information, decision of countermeasures and their deployment.

5.1. Analysis

The analysis component performs identification of network situations from metrics provided by the aggregation module and reaches diagnoses that contribute in decision-making tasks. In general terms, the analysis studies any aspect related with the incidences reported by the 5G use cases and the risks that could compromise the system requirements. In this context, situations are divided into two main groups: events and risks. Events are defined as situations that occur within 5G mobile networks which a priori do not display harmful features but are useful in diagnosis. The events are grouped into four categories: discovery, removal, modification and notification, which are described as follows:

- *Discovery events*—include all situations related to incorporation of new assets to the system. For example, this occurs when incorporating new nodes into the network, establishment of new connections between previously existing resources, or deployment of new virtualization layers. Each time a discovery event is communicated, the asset inventory is updated.
- *Removal events*. Unlike discovery events, removal events indicate situations related to the elimination of 5G resources. These are the cases of deletion of assets, removal of connections between nodes, or elimination of virtualization resources. As in discovery events, each time a removal event is communicated, the asset inventory is upgraded.
- *Modification events*. They include every situation related with the modification (not removal) of an existing resource. For example, this occurs when varying the location of the asset (i.e., changes to IP address, MAC address, etc.), and changes between communication protocols or software updates. As in the previous cases, modification events involve changes to the asset inventory.
- *Notification events*. They report specific situations in the network that are not related to changes in the assets inventory, such as periodic reviews of the bandwidth status, presence of unused resources or requests for special configurations.

On the other hand, risks are inherently damaging, and they may be inferred from network mapping or directly reported by the use case agents. An example of the first case is the identification of bottlenecks, congested regions or resources depletion. In the other case, a striking example relates to defensive use cases, where security NFV-Apps (Intrusion Detection Systems, honeypots, etc.) directly reports intrusions such as malware spreading or denial of service threats. The bases of 5G situation analysis are shown in Figure 3. They include: detection, risk assessment, asset inventory management, risk map, prediction, diagnosis and countermeasure tracking. The following briefly describes the most important features of each of them.

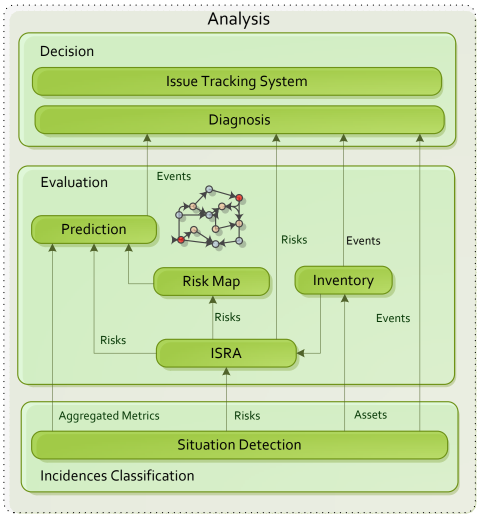

Figure 3. Situation analysis on 5G.

5.1.1. Detection

The detection module is the connection between monitoring/aggregation tasks and the functions for understanding the information. Its inputs are aggregated high-level metrics built from correlated data and reports of situations directly issued by the sensors. After processing this information, the detection module builds the primitive situations (events or risks) to be analyzed. The rules to infer situations from the perceived data are provided by security operators and determined after the risks/events identification. Note that the same combination of metrics could trigger different situations; because of this, the proper management of the detection component implies adaptation of expert systems, especially those based on rules.

5.1.2. Risk Assessment

Risk assessment combines some of the most widely spread strategies approved by the research community for Information Security Risk Assessment (ISRA), among them the guidelines ISO/IEC 27000 [7], NIST-SP 800 [8], CVSS-SIG-First [9] or MAGERIT [10]. The approach to identify risk factors assumes the basis on ISO/IEC 2700 series and NIST-SP800. However, since these are mainly aimed at general purpose risk assessment, they lack specificity; in particular, they do not take into account the 5G design principles, infrastructure or requirements. Because of this, they must be adapted to the 5G mobile networks circumstances. Another obstacle is that they are based on metrics that are too simple. In order to improve the ability to understand the impact and facilitate decision-making, as well as consider a more current model, a group of advanced measures similar to those proposed in CVSS-SIG-First should be adapted. Thereby, a larger amount of characteristics on the potential vulnerabilities should be studied, thus assuming the union of three metric sets that contain intrinsic (base), temporal and specific (environmental) features. On the other hand, approaches like MAGERIT provide alternative ways to calculate risks, which may be particularly useful in certain use cases. In general terms, the risk assessment component may be integrated as part of the detection module or could be deployed completely independently. Bearing in mind the taxonomy of ISRA approaches [20], it is recommended that its development considers qualitative assessment criteria, service-based perspectives, vertical valuation and propagated measurement.

5.1.3. Asset Inventory

The asset inventory builds and manages a list of resources or assets to be considered at the risk valuation step. Due to the ability of the 5G mobile networks to automate the deployment of new services and network devices depending on their status, this component plays a critical role in the analysis of the gathered information. The new assets are detected at the monitoring layer and are reported by discovery events. When the existing events are updated, the monitor layer emits modification or removal events. For the proper functioning of the proposed architecture, it is very important to ensure coherence between the list of assets and the real network resources.

5.1.4. Risk Map

This component builds and manages a risk map of the network incidences considering aggregated high-level metrics, events and the inferred risks. The risk map is mainly considered in the following situations: prediction of threats spreading, the establishment of quarantine regions, identification of the best spots to deploy mitigation actions, and recognition of the source of the attacks. As in the case of the asset inventory, there must be coherence between the list of assets and the current network resources. The risk map is built considering the network map, so its proper development implies upgrades in real-time of the network connectivity and its status (throughput, congestion, transmission delays, availability, etc.)

5.1.5. Prediction

Prediction facilitates the anticipation of future complications, such as congestion of certain network regions, inclusion of large amounts of new assets or spreading of cyberattacks. The general scheme for forecasting SA studies variations on their contents by modeling the sequence of observations as time series, as it is shown in Figure 4. Each observation includes information about every SA feature, such as the network map, risk levels or recent incidents monitored over a period of time. Because of this, the prediction module is not only capable of anticipating particular situations, but also the whole future SA, thus providing general and particular overviews about everything that occurs in the system. Note that the observations are delimited by a fixed period of time. A common alternative to this fixed value is to consider more specific features, such as workload or number of situations reported. Both cases imply advantages and disadvantages, but the delimitation by time periods poses a more intuitive method. In order to avoid overloading of storage systems, after a reasonable period, the oldest observations are discarded to make way for the new ones. In this way, a sliding window of size N that gathers the observations is applied. This boundedness is important for ensuring that the implemented algorithms are computable, avoiding the case $N \rightarrow \infty$ (i.e., the worst case), which leads to holding an infinite amount of information.

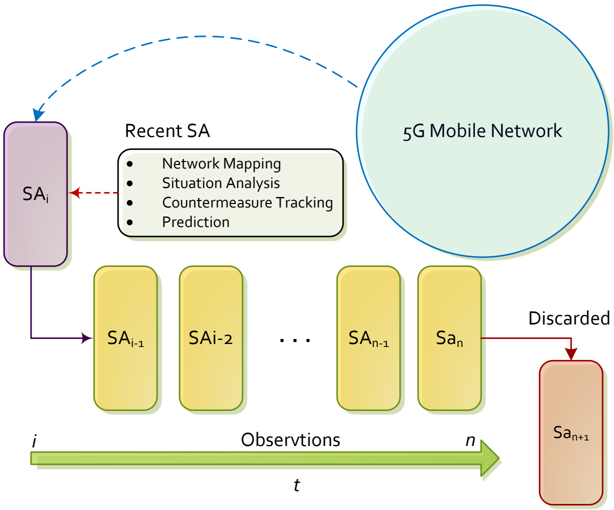

Figure 4. Situational Awareness prediction.

5.1.6. Diagnosis

Diagnosis performs advanced analysis of risks and their assessment, impact, projection and network status. This allows for identifying complex situations that can be difficult to detect from the lower levels of data processing. For example, the diagnosis component should be able to recognize botnets by analyzing the relationships between the risk in network devices compromised by malware and the discovery of surrounding traffic anomalies. Given that the proposed architecture assumes a service-driven vertical risk analysis model that considers propagation, it is important to determine two diagnosis criteria: particular threat level and propagated threat level. The particular threat level related with a risk is its severity. This value is useful to manage isolated situations, but it does not take into account what happens in the surrounding area. On the other hand, the propagated threat level considers all the risks detected in a region and their relationships. There are several publications that address the calculation of propagated risks, where the Bayesian Networks (BN) are the most widespread solutions [44,45]. An example of this methodology is shown in Figure 5, where several particular threat levels related to each other are normalized and pooled, thus allowing for inferring the propagated risk in the lower situations.

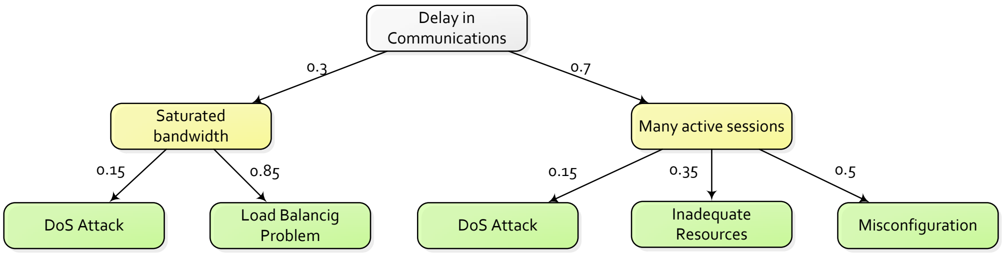

Figure 5. Example of Bayesian Network (Decision Tree) in network diagnosis.

5.1.7. Countermeasure Tracking

The countermeasure tracking component conducts comprehensive monitoring of the actions proposed by the decision-making modules for dealing with situations. This allows for identifying ineffective countermeasures that may lead to new diagnosis or prevention of counterproductive situations. On the other hand, the countermeasure tracking stage allows for the development of an immune memory. Therein, all situations that have been resolved or are being processed are stored. This allows knowing how a problem was previously solved, offering added value to the decision-making. In addition, it provides information about all similar problems that are being processed, which may facilitate the correlation of incidences. In order to enhance the countermeasure tracking tasks, the proposed architecture implements an Issue Tracking System (ITS). The ITS assigns a ticket to every situation tracked in the protected environment. Tickets are running reports on a particular problem, which contains their nature, history and other relevant data. They are continuously analyzed to provide real-time status of the situation, and they record all the countermeasures implemented over time, as well as their effectiveness. The ITS is illustrated in Figure 6, where the original situation to be treated is provided by a use case, or it is detected from the network map. Then, the incident is analyzed, and a token with the results is sent to the decision stages. If countermeasures should not be applied, the ticket is close; in this case, it is assumed that the problem is fixed, and the solution is stored in the immune memory. Otherwise, countermeasures are applied. Then, the evolution and effectiveness of such actions are studied and added to the ticket history field; as in the previous case, the progress is also stored in the memory. The resulting ticket is sent back to the decision-making module, and this process is repeated until the problem is fixed.

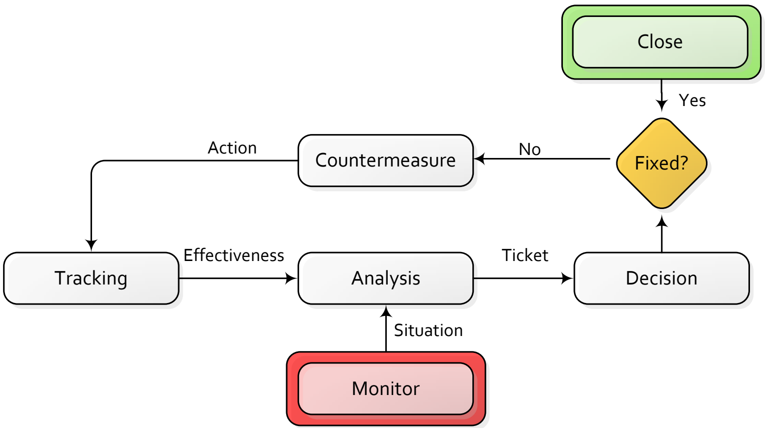

Figure 6. Issue tracking algorithm.

5.2. Decision-Making and Actuators

The decision-making component addresses the problem of mitigating the network situations that may disrupt the normal operation of the network elements and the services provided. In particular cases, it can take also part in the performance optimization process of the services offered by the mobile network, thereby playing an active role in tasks such as load balancing or management of traffic with multimedia content. To this end, the decision-making processes receive information from the analysis stage (mainly from diagnosis and countermeasures tracking) and then select a set of responses to be executed. According to ISO/IEC 7498-2 [46], such correctives are referred as security safeguards, and they are involved in prevention, mitigation and source identification. The strategy for selecting optimal countermeasures must balance the cost of implementation of the safeguard and the achieved reduction of the incidence impact [47]. The available actions are distributed as NFV-Apps, so that these constitute a large repository of potential countermeasures. The network components that execute the safeguards are known as actuators. An example of their implementation is the mitigation of distributed denial of service attacks: when the analysis component performs a diagnosis related to this category of incidences, the report includes information about the compromised assets, impact, prediction and the attack vector. In the example, the first step of decision-making is to prevent the spreading of the threat by deploying firewall NFV-Apps (specific actuators), thus taking into account the predictions of their distribution. The second step is to mitigate the threat by implementing honeypot NFV-Apps and the malicious traffic redirection towards sinkholes. Once the impact of the attack is minimized, the last step is identifying the sources by applying IP traceback algorithms [48], from which they could be blocked or alerted. The deployment of the various actions is coordinated by an orchestrator agent, which ensures that the virtual resources that implement the countermeasures are available and do not affect the system performance.

6. Conclusions

The conventional schemes for Information Security Risk Management have demonstrated significant shortcomings in the deployment in dynamic monitoring environments, as is the case of 5G mobile networks. In order to contribute to their development, this article has presented a novel architecture for incidence management in 5G based on the combination of the cognitive model for Situational Awareness proposed by Endsley, and the guidelines, platforms and more frequent regulations on the identification and assessment of threats. In this way, the automation of proactive/reactive deployment of countermeasures is facilitated.

Additionally, other important aspects are enhanced such as taking advantage of every information source, the quality of the context to be considered in the decision-making and the projection of the system status. Our design significantly reduces capital and operational expenditures, and it also allows for processing information gathered from 5G mobile networks, expressed as high-level metrics (HoN). The proposed architecture is possible thanks to the capabilities offered by innovative technologies such as SDN, NFV or virtualization. However, in order to not add additional complexity to this first approach, several aspects (to bear in mind before its implementation) have not been explained in detail. This is the case of the characteristics of sensors/actuators and their relationship with the repositories of NFV-Apps from which they can be instantiated.

The paper has not delved into the advanced diagnostic methods to be considered in order to take advantage of the issue tracking system, nor in their feedback with decision-making. The same happened with the specification of the interfaces that connect the different components, and the tactical language for information exchange. All of these aspects will be covered in future work. From the presented work, different lines of research have been encouraged. The most obvious is focused on the implementation of the approach in recent monitoring environments, as occurs with the European project that is funding this investigation.

Another aim could be to analyze their different use cases in order to adapt the incidence concept to common problems related to the Quality of Experience, such as the prevention of internal network errors, collisions or the optimization of multimedia content transmissions. Finally, this architecture is proposed as an alternative to the current collaborative defensive strategies due its great potential for synchronizing the efforts of prevention, detection, mitigation and source identification.

Acknowledgments: This work is supported by the European Commission Horizon 2020 Programme under grant agreement number H2020-ICT-2014-2/671672—SELFNET (Framework for Self-Organized Network Management in Virtualized and Software Defined Networks). Lorena Isabel Barona López and Ángel Leonardo Valdivieso Caraguay are supported by the Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación SENESCYT (Quito, Ecuador) under the Convocatoria Abierta 2012 and 2013 Scholarship Program.

Author Contributions: The authors contributed equally to this research.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Andrews, J.G.; Buzzi, S.; Choi, W.; Hanly, S.V.; Lozano, A.; Soong, A.C.K.; Zhang, J.C. What Will 5G Be? *IEEE J. Sel. Areas Commun.* **2014**, *32*, 1065–1082.
2. Agyapong, P.K.; Iwamura, M.; Staehle, D.; Kiess, W.; Benjebbour, A. Design Considerations for a 5G Network Architecture. *IEEE Commun. Mag.* **2014**, *52*, 65–75.
3. NGMN Alliance. NMGN 5G White Paper. 2015. Available online: https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf (accessed on 19 December 2016).
4. Panwar, N.; Sharma, S.; Singh, A.K. A Survey on 5G: The Next Generation of Mobile Communication. *Phys. Commun.* **2016**, *18*, 64–84.
5. Boccardi, F.; Heath, R.W.; Lozano, A.; Marzetta, T.; Popovski, P. Five Disruptive Technology Directions for 5G. *IEEE Commun. Mag.* **2014**, *52*, 74–80.
6. Imran, A.; Zoha, A. Challenges in 5G: How to Empower SON with Big Data for Enabling 5G. *IEEE Netw.* **2014**, *28*, 27–33.
7. International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 27002: Information Technology, Security Techniques, Code of Practice for Information Security Management. 2005. Available online: http://www.iso.org/iso/catalogue_detail?csnumber=54533 (accessed on 19 December 2016).
8. National Institute of Standards and Technology. NIST-SP800 Series Special Publications on Computer Security. Available online: http://csrc.nist.gov/publications/PubsSPs.html#SP800 (accessed on 19 December 2016).
9. Forum of Incident Response and Security Teams. CVSS: Common Vulnerability Scoring System. Available online: https://www.first.org/cvss/specification-document (accessed on 19 December 2016).
10. MAGERIT: Risk Analysis and Management Methodology for Information Systems. Available online: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/ (accessed on 19 December 2016).
11. Parvizi, R.; Oghbaei, F.; Khayami, S.R. Using COBIT and ITIL Frameworks to Establish the Alignment of Business and IT Organizations as One of the Critical Success Factors in ERP Implementation. In Proceedings of the 5th IEEE Conference on Information and Knowledge Technology (IKT), Shiraz, Iran, 28–30 May 2013; pp. 274–278.
12. Webb, J.; Ahmad, A.; Maynard, S.B.; Shanks, G.; Popovski, P. A Situation Awareness Model for Information Security Risk Management. *Comput. Secur.* **2014**, *44*, 1–15.
13. Endsley, N.R. Design and Evaluation for Situation Awareness Enhancement. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Anaheim, CA, USA, 24–28 October 1988; Volume 32, pp. 97–101.
14. Leau, Y.B.; Ahmad, A.; Manickam, S. Network Security Situation Prediction: A Review and Discussion. In Proceedings of the 4th International Conference on Soft Computing, Intelligent Systems, and Information Technology (ICSIIT), Bali, Indonesia, 11–14 March 2015; pp. 424–435.
15. Marquezan, C.C.; Mahmood, K.; Zafeiropoulos, A.; Krishna, R.; Huang, X.; An, X; Corujo, D; Leitão, F.; Rosas, M.L.; Einsiedler, H. Context Awareness in Next Generation of Mobile Core Networks. *arXiv* **2016**, arXiv:1611.05353.
16. Belmonte Martin, A.; Marinos, L.; Rekleitis, E.; Spanoudakis, G.; Petroulakis, N.E. *Threat Landscape and Good Practice Guide for Software Defined Networks/5G*; European Union Agency for Network and Information Security (ENISA): Heraklion, Greece, 2015. Available online: http://openaccess.city.ac.uk/15504/7/SDN%20Threat%20Landscape.pdf (accessed on 19 December 2016).

17. 5G-Ensure Project. Enablers for Network and System Security and Resilience. Project Reference: 671562. Funded under: H2020-ICT-2014-2. Available online: http://www.5gensure.eu/ (accessed on 19 December 2016).
18. 5G Ensure. Deliverable D 2.3, Risk Assessment, Mitigation and Requirements (Draft), August 2016. Available online: http://www.5gensure.eu/deliverables (accessed on 19 December 2016).
19. Aven, T. Risk Assessment and Risk Management: Review of Recent Advances on their Foundation. *Eur. J. Oper. Res.* **2016**, *256*, 1–13.
20. Shameli-Sendi, A.; Aghababaei-Barzegar, R.; Cheriet, M. Taxonomy of Information Security Risk Assessment (ISRA). *Comput. Secur.* **2016**, *57*, 14–30.
21. Hansson, S.O.; Aven, T. Is Risk Analysis Scientific? *Risk Anal.* **2014**, *34*, 1173–1183.
22. Doty, P. US Homeland Security and Risk Assessment. *Gov. Inf. Q.* **2015**, *32*, 342–352.
23. Yang, M.; Khan, F.; Lye, L.; Amyotte, P. Risk Assessment of Rare Events. *Process Saf. Environ. Prot.* **2015**, *98*, 102–108.
24. Ab Rahman, N.H.; Choo, K.K.R. A Survey of Information Security Incident Handling in the Cloud. *Comput. Secur.* **2015**, *49*, 45–69.
25. Knowles, W.; Prince, D.; Hutchison, D.; Disso, J.; Ferdinand, P.J.; Jones, K. A Survey of Cyber Security Management in Industrial Control Systems. *Int. J. Crit. Infrastruct. Prot.* **2015**, *9*, 52–80.
26. Ni, S.; Zhuang, Y.; Gu, J.; Huo, Y. A Formal Model and Risk Assessment Method for Security-critical Real-time Embedded Systems. *Comput. Secur.* **2016**, *58*, 199–215.
27. Cherdantseva, Y.; Burnap, P.; Blyth, A.; Eden, P.; Jones, K.; Soulsby, H.; Stoddart, K. A Review of Cyber Security Risk Assessment Methods for SCADA Systems. *Comput. Secur.* **2016**, *56*, 1–27.
28. Quick, D; Martini, B; Choo, K.K.R. Cloud Storage Forensics. In *Syngress*; Elsevier: Amsterdam, The Netherlands, 2013; pp. 1–208, ISBN: 978-0-12-419970-5. Available online: http://www.sciencedirect.com/science/book/9780124199705 (accessed on 19 December 2016).
29. Ab Rahman, N.H.; Glisson, W.B.; Yang, Y.; Choo, K.K.R. Forensic-by-Design Framework for Cyber-Physical Cloud Systems. *IEEE Cloud Comput.* **2016**, *3*, 50–59.
30. Ab Rahman, N.H.; Cahyani, N.D.W.; Choo, K.K.R. Cloud incident handling and Forensic-by-Design: Cloud Storage as a Case Study. *Concurr. Comput. Pract. Exp.* **2016**, 1–16, doi:10.1002/cpe.3868.
31. Endsley, M.R.; Selcon, S.J.; Hardiman, T.D.; Croft, D.G. A Comparative Analysis of SAGAT and SART for Evaluations of Situation Awareness. In Proceedings of the Human Factors and Ergonomics Society Annual Meeting, Chicago, IL, USA, 5–9 October 1998; Volume 1, pp. 82–86.
32. Adam, E.C. Fighter Cockpits of the Future. In Proceedings of the 12th IEEE Digital Avionics Systems Conference (DASC), Fort Worth, TX, USA, 25–28 October 1993; pp. 318–323.
33. Dahal, N.; Abuomar, O.; King, R.; Madani, V. Event Stream Processing for Improved Situational Awareness in the Smart Grid. *Expert Syst. Appl.* **2015**, *42*, 6853–6863.
34. Naderpour, M.; Nazir, S.; Lu, J. The Role of Situation Awareness in Accidents of Large-scale Technological Systems. *Process Saf. Environ. Prot.* **2015**, *97*, 13–24.
35. Moradi-Pari, E.; Tahmasbi-Sarvestani, A.; Fallah, Y.P. A Hybrid Systems Approach to Modeling Real-time Situation-Awareness Component of Networked Crash Avoidance Systems. *IEEE Syst. J.* **2016**, *10*, 169–178.
36. Seppänen, H.; Virrantaus, K. Shared Situational Awareness and Information Quality in Disaster Management. *Saf. Sci.* **2015**, *77*, 112–122.
37. Chatzimichailidou, M.K.; Stanton, N.A.; Dokas, I.M. The Concept of Risk Situation Awareness Provision: Towards a New Approach for Assessing the DSA about the Threats and Vulnerabilities of Complex Socio-technical Systems. *Saf. Sci.* **2015**, *79*, 126–138.
38. Franke, U.; Brynielsson, J. Cyber Situational Awareness—A Systematic Review of the Literature. *Comput. Secur.* **2014**, *46*, 18–31.
39. Schmittling, R.; Munns, A. Performing a Security Risk Assessment. *ISACA J.* **2010**, *1*, 10–18.
40. Naderpour, M.; Lu, J.; Zhang, G. A Situation Risk Awareness Approach for Process Systems Safety. *Saf. Sci.* **2014**, *64*, 173–189.
41. Tahaei, H.; Salleh, R.; Khan, S.; Izard, R.; Choo, K.K.R.; Anuar, N.B. A multi-objective Software Defined Network Traffic Measurement. *Measurement* **2016**, *95*, 317–327.
42. Shanbhag, S.; Kandoor, A.R.; Wang, C.; Mettu, R.; Wolf, T. VHub: Single-stage Virtual Network Mapping Through Hub Location. *Comput. Netw.* **2015**, *77*, 169–180.

43. Chowdhury, N.M.K.; Rahman, M.R.; Boutaba, R. Virtual Network Embedding with Coordinated Node and Link Mapping. In Proceedings of the 28th IEEE Conference on Computer Communications (INFOCOM), Rio de Janeiro, Brasil, 19–25 April 2009; pp. 783–791.
44. Awan, M.S.K.; Burnap, P.; Rana, O. Identifying Cyber Risk Hotspots: A Framework for Measuring Temporal Variance in Computer Network Risk. *Comput. Secur.* **2016**, *57*, 31–46.
45. Shin, J.; Son, H.; Ur, R.K.; Heo, G. Development of a Cyber Security Risk Model Using Bayesian Networks. *Reliab. Eng. Syst. Saf.* **2015**, *134*, 208–217.
46. International Organization for Standardization and the International Electrotechnical Commission. ISO/IEC 7498-2, Information Processing Systems—Open Systems Interconnection—Basic Reference Model Part 2: Security Architecture. Available online: http://www.iso.org/iso/catalogue_detail.htm?csnumber=14256 (accessed on 19 December 2016).
47. Gonzalez-Granadillo, G.; Garcia-Alfaro, J.; Alvarez, E.; El-Barbori, M.; Debar, H. Selecting Optimal Countermeasures for Attacks against Critical Systems Using the Attack Volume Model and the RORI Index. *Comput. Electr. Eng.* **2015**, *47*, 13–34.
48. Alenezi, M.N.; Reed, M.J. Uniform DoS Traceback. *Comput. Secur.* **2014**, *45*, 17–26.