# Poster: Knowledge Inference Analysis Framework for Incidence Management in 5G Networks

Marco Antonio Sotelo Monge, Jorge Maestre Vidal, 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 s/n, Ciudad Universitaria, 28040 Madrid, Spain
E-mail: {masotelo, jmaestre}@ucm.es, javiergv@fdi.ucm.es

***Abstract*—This paper proposes a knowledge inference analysis framework for incidence management, in the context of the SELFNET project. This framework is intended to infer the current network status of a 5G network and detect, either proactive or reactively, the presence of security incidents that represent possible security threats to mitigate, so that, allowing a better decision making process. The proposed framework provides also prediction, pattern recognition, and adaptive thresholding capabilities, enhancing the generation of context-aware facts to produce knowledge about suspicious behaviours, so that, enabling other system components the deployment of mitigation actions over the identified scenario. In addition, this framework proposes an easily configurable use-case driven methodology, following the 5G simplicity and scalability design principles.**

***Index Terms*—5G, Analysis, Framework, Incidence Management, Knowledge Inference, NFV, SDN.**

## 1. Introduction

5G networks have the main goal to provide a secure and high-performance operational environment, suitable to ensure the efficient delivery of network services, with the agreed service levels. To fulfill these goals, 5G makes a seamless integration of emerging technologies such as Software Defined Networking (SDN), Network Functions Virtualization (NFV), Artificial Intelligence (AI), among others. 5G networks are expected not only to automatically identify and mitigate security threats, but also to expose a simplified, unified and heterogeneous management scheme. Nowadays, the 5G-PPP consortium promotes the development of 5G research projects, being SELFNET (Self-Organized Network Management in Virtualized and Software Defined Networks) [1] part of them. One of the SELFNET priorities is the autonomic security management through an exhaustive data analysis process, thus, allowing the system to infer possible security incidents. To this end, this paper proposes a novel knowledge inference based framework to deal with the aforementioned 5G incidence management objectives.

## 2. The SELFNET Project

SELFNET project aims to develop an autonomic network management framework in order to provide self-organization capabilities in 5G networks. SELFNET relies on the principles of SDN and NFV to make a smart autonomic management of different network functions intended to detect and automatically mitigate a range of common network problems. With this aim, SELFNET firstly identifies the 5G network behavior, over which will decide the best mitigation actions under a use-case driven approach. SELFNET provides Self-protection capabilities as one of the core framework functionalities, leading to the deployment of timely response actions, either proactive or reactively, against cyber attacks, virus, malware, among other security threats. To accomplish this, a set of sensors and actuators (IDS, DPI, anti-malware, etc.) are deployed along the network. SELFNET provides a three step schema (Monitoring, Aggregation and Correlation, and Analysis) in order to facilitate the operational context comprehension based on the Endsley situational awareness model [2]. Monitoring is intended to gather network infrastructure low-level metrics and network events, to allow their processing in upper layers. In the Aggregation and Correlation layer, low-level metrics are inputs to perform aggregation operations, in order to obtain higher level metrics and, at the same time, to reduce the high volume of monitored data. On the other hand, events are correlated not only for filtering purposes (i.e by deleting redundand alerts), but also for a better global understanding of the network context. Finally, at Analysis level, the identification of potencial security incidents is achieved.

## 3. Knowledge-based Analysis Framework

The analysis framework is intended to infer knowledge based on the information processed in the lower layers (Monitoring and Aggregation/Correlation), thus allowing the identification of security threats over which mitigation actions are needed. Those actions are selected as a result

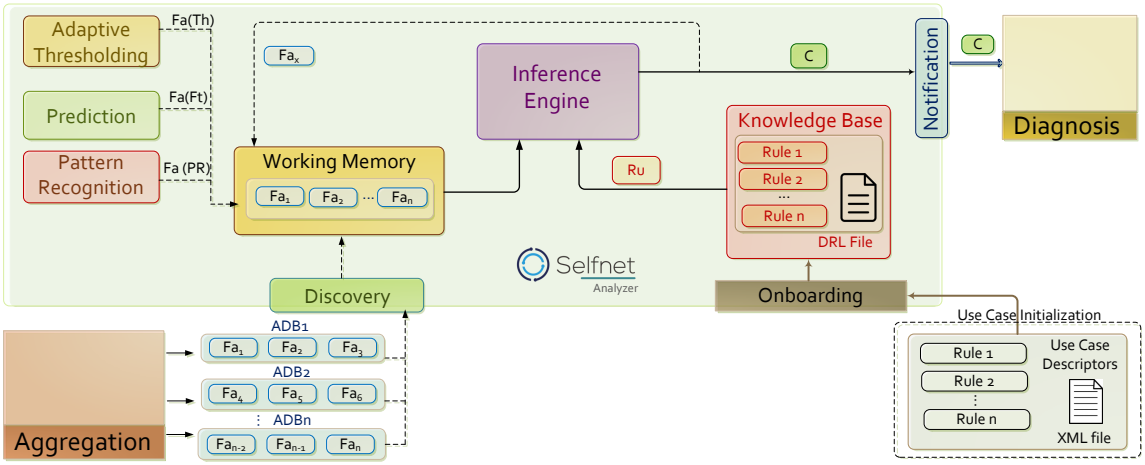


Figure 1. Knowledge Inference Analysis Framework for Incidence Management in 5G

of complex diagnosis and decision making processes in the Intelligence component of SELFNET. Under this context, network events representing security alerts (i.e IDMEF [3]) to trigger also more sophisticated analysis techniques; for example, flow traffic analysis and packet inspection for botnet generated attacks [4].

The internal architecture of the framework is shown in Fig. 1. Facts are the information units of analysis for rule-based systems, and are stored in the Working Memory. In Selfnet Analyzer, facts can be originated from external or internal sources. External facts (i.e. Fa1) are loaded into the system from the Aggregation and Correlation module, through Discovery procedures, in the form of Aggregated Data Bundles (ADBs). Internal facts are also originated either by the Patter recognition, Prediction or Adaptive Thresholding components; or by the Inference engine itself through the insertion of new facts into the Working Memory (forward chaining). Procedural knowledge is represented as rule sets (Ru), along with other descriptors (Objects, Facts, and so on), which are onboarded in the initialization phase. In addition, the Inference engine considers separation rules (*modus ponens*) driven by propositional logic.

Patter Recognition generates new facts (Fa(PR)) identified through the analysis of the most accurate pattern recognition strategy, regression model, etc. applied in the current network scenario. The Prediction component calculates forecasting metrics expresed as facts (Fa(Ft)) as a result of the evaluation of historical data, the selection of the most appropriate algorithm, and the results assessment to enhance future forecasts. Likewise, Adaptive Thresholding sets approximation methods to apply when prediction errors must be taken into account with the aim to reduce false positives, generating new facts (Fa(Th)) from such calculus. With all these information in the working memory, Knowledge Inference can infer conclusions (C), making them available to the SELFNET Intelligence component.

At the time of this writing, the framework is still under development with a formal data specification defined, and an inference engine already implemented. Current efforts are in the implementation of the Prediction, and the subsequent components are also on the development path. All of them expected to be delivered in the short-term.

## 4. Conclusion

The presented knowledge-based framework analysis contributes to the deployment of network intelligence in 5G networks, providing the inferred knowledge about possible context-aware security threats in the network. The proposed framework offers a generic architecture to enable security incidence management based on the Endsley situational awareness model. Input aggregated metrics and events are also useful for the identification of threats and security alerts over a specific network domain. In this way, the acquired knowledge facilitates the consequent deployment of mitigation countermeasures.

## Acknowledgments

This work was funded by the European Commission Horizon 2020 Programme under Grant Agreement number H2020-ICT-2014-2/ 671672 SELFNET (A Framework for Self-Organized Network Management in Virtualized and Software Defined Networks).

## References

[1] EU SELFNET Project "Self-Organized Network Management in Virtualized and Software Defined Networks". Project reference: H2020-ICT-2014-2/671672. Funded under: H2020. http://www.selfnet-5g.eu

[2] M.R. Endsley, "Design and Evaluation for Situation Awareness Enhancement", Proc. *32nd Annual Meeting on Human Factors Society*, pp. 97-101, 1988.

[3] H. Debar, D. Curry, B. Feinstein. "The Intrusion Detection Message Exchange Format (IDMEF)". IETF RFC 4765, 2007.

[4] D. Zhao, I. Traore, B. Sayed, W. Lu, S. Saad, A. Ghorbani, D. Garant, "Botnet detection based on traffic behavior analysis and flow intervals", In *Computers Security*, 39, pp. 2-16, 2013.