Multi-level Resilience in Networked Environments: Concepts & Principles

Muhammad Azizi Mohd Ariffin*, Angelos K. Marnerides*†, Andreas U. Mauthe*
* InfoLab21, School of Computing & Communications, Lancaster University, UK
a.mohdariffin, a.mauthe@lancaster.ac.uk
†Department of Computer Science, Liverpool John Moores University, UK
a.marnerides@ljmu.ac.uk

***Abstract*—Resilience is an essential property for critical networked environments such as utility networks (e.g. gas, water and electricity grids), industrial control systems, and communication networks. Due to the complexity of such networked environments achieving resilience is multi-dimensional since it involves a range of factors such as *redundancy* and *connectivity* of different system components as well as *availability, security, dependability* and *fault tolerance*. Hence, it is of importance to address resilience within a unified framework that considers such factors and further enables the practical composition of resilience mechanisms. In this paper we firstly introduce the concepts and principles of Multi-Level Resilience (MLR) and then demonstrate its applicability in a particular cloud-based scenario.**

***Index Terms*—Resilience, cloud security, multi-level resilience**

I. Introduction

In recent years resilience has received considerable attention by industry, governmental bodies as well as research. This is motivated by the need for resilient mechanisms that can manage and control complex, mission-critical networked environments (e.g. industrial control systems, utility networks) and further guarantee their continued operations. A number of recent incidents have shown that the interruption of normal operations of critical systems can lead to major disruptions within society and business, i.e. the socio-economic backbone in today's society.

In the past resilience has been mainly achieved through structural means (e.g. through redundancy and distribution) [1], which has proven a viable strategy, (e.g. during the 2011 Tohoku earthquake and tsunami in Japan the fixed line telephone networks and fibre based data networks were by enlarge still operational due to sufficient redundancy being in place [1]). However, providing resilience solely through structural means is in itself no longer sufficient since specifically cyber challenges target service operations and system management directly. An example is one of the largest ever reported DDoS attack against a French Web site in February 2014 reaching 400Gb/s [2]. More profane reasons for a service disruption can be something simple such as a misconfiguration, which was the suspected cause of an eight hour outage that left 618 million Chinese Internet users without a service in January 2014 [3]. Thus, resilience has to be an active property that is supported through appropriate mechanisms (such as anomaly detection and remediation) as well as a structural characteristic achieved through passive, architectural means.

The provisioning of resilience also needs to consider different system layers of interconnected systems. Research activities such as [5] [6] have developed evaluation metrics for the resilience of communication infrastructures. These help to analyse and subsequently improve structural resilience. However, approaches that aim to coordinate operational resilience via joint detection and remediation processes has received less attention. Anomalous events (malicious or legitimate, e.g. in the case of DDoS and Flash Crowds) can propagate and affect a number of subsystems within a given networked environment. Further, in some cases the attribution of an anomaly needs additional information from another system level (e.g. a sys log) to fully establish the root cause. Hence, it is critical to design solutions that combine the various information levels on both the network and system stack in both a vertical (i.e. on a given subsystem) and horizontal fashion (i.e. across multiple subsystems) in order to detect and identify the cause and source of an anomaly, and the location where remediation actions should be triggered.

Despite the fact that in some areas resilience indicators from different levels are jointly considered a systematic approach towards the area of *multilevel resilience* is so far lacking. In this paper, we structure the approach-to-design space by introducing a *multi-level resilience* (MLR) taxonomy and by outlining principles and concepts. Furthermore, this paper briefly discusses different aspects related to structural and operational MLR. Subsequently we use an example based on anomaly detection within the scope of cloud management to demonstrate the applicability of the major concepts within a specific scenario. We argue, that the work-in-progress reported herein will establish the basis for the future design and development of resilient mechanisms in the context of evolving next generation network architectures.

The remainder of this paper is structured as follows: Section II introduces MLR and further in section II-A provides a clear description of the MLR concepts and principles. Section III is dedicated at illustrating an exemplar application of MLR on a cloud management-based scenario. Finally, section IV summarises and concludes this paper.

[1] http://www.electronicsnews.com.au/news/japan-s-2011-earthquake-and-tsunami-communications, March 2011

TABLE I: Multi-level Resilience Concepts

	Covered Strategy Constituents	Enablers
Structural MLR (SMLR)	Defend, Diagnose, Refine	Replication, Diversity, Translucency
Analytical MLR (AMLR)	Detect, Diagnose, Refine	Context-awareness, Translucency
Functional MLR (FMLR)	Defend, Remediate	Translucency, Cross-layer interaction

II. Multi-Level Resilience (MLR)

Resilience as defined in [6] is the ability of a network (or system) to maintain "an acceptable level of service even in the presence of challenges". Such challenges can be of structural and operational nature. In general four challenge categories are being distinguished, i.e. *malicious activities*, *operational overload*, *mis-configurations*, and *equipment failure*. Initially the focus of this definition has been within the networking domain but it has been shown that it is also applicable in the systems space (e.g. clouds and data centres [8] [9]).

Early work on multi-level resilience [6] looked into the how to provide resilience between different protocol layers of system levels in the context of an overall resilience framework. In keeping with the traditional layered communication view resilience is a service property provided by a layer below to the one above. This also applies to different communication planes such as the data, control and management plan, as well as the network engineering level [12]. Cross-layer principles can then be applied to the protocol level where a protocol configuration at a specific layer depends on the resilience provided below this layer. However, additional information provided across the layers about the overall system state should aid a more adapted decision making across the layers. The concept of translucency allows the interaction between the layers and plans in order to optimise resilience across multiple levels.

Alongside multi-level resilience context awareness enables the system to detect and attribute a challenge correctly within a given environment. In doing so the resource trade-offs (i.e. where and what kind of resilience mechanisms can be deployed most efficiently) also have to be considered.

A. MLR Concepts & Taxonomy

In order to address multi-level resilience (MLR) more comprehensively we propose a taxonomy that structures the problem and solution space. In general there are two MLR aspects, i.e. *Structural Multi-Level Resilience* (SMLR) as mainly expressed through frameworks and architectural models and the assessment of the resilience level they offer (e.g. [12]), and *Operational Multi-Level Resilience* (OMLR), i.e. providing coordinated resilience mechanism across system layers and even system boundaries. Within both the analysis of resilience properties plays an important role. However, whereas for SMLR an infrastructure is analysed regarding its ability to withstand challenges and maintain normal operations, OMLR provides an (online) analysis of operational resilience parameters in order to discover anomalies and implements remediation actions.

At a structural level resilience is achieved through means such as *replication* and *diversity*, which can be implemented in a complementary manner at different system levels. This strategy allows a network or system in the event of failures to utilise alternative resources in order to maintain the service. At the operational level resilience is achieved through active detection, and remediation. This happens at different points within the systems infrastructure (ideally in a coordinated manner). In order to capture this in a systematic manner we propose three multi-level resilience concepts that are able to structure and subsume these aspects. *Structural Multi-Level Resilience* (SMLR) deals the analysis and provision of resilience at an infrastructure level across a number of infrastructure components. At the operational level there is *Analytical Multi-Level Resilience* (AMLR) and *Functional Multi-Level Resilience* (FMLR). Through AMLR the system state is assessed considering the different active elements of a connected system or infrastructure. FMLR refers to coordinated protective action across an infrastructure in form of detection, remediation and recovery. AMLR realises the multi-level principles of context awareness and translucency, whereas FMLR is mainly based on cross-layer interaction as part of the network and system management infrastructure. This is provided through components that observe the system state, detect anomalous behaviour and activities and take active actions against them. Table I summarises the different MLR concepts.

We distinguish between two different multi-level resilience forms, i.e. *horizontal* and *vertical* MLR. Horizontal SMLR describes the structural analysis and coordinated deployment of protective system elements between different, independent (sub-)systems at the same level, e.g. an analysis of a communication network at sub-network level. Vertical SMLR involves a coordinated analysis and use of protective elements across the different levels of a system or infrastructure. An example would be the analysis of the computing infrastructure alongside the network infrastructure within a data centre, and the use of appropriate redundancy mechanisms. Horizontal AMLR refers to the coordination active detection at the same operational level, whereas horizontal FMLR would coordinate detection and remediation mechanisms across system components at one level. For instance, edge and core network management units can exchange information, anomaly detection results, and coordinate the remediation actions [13]. In this context the detection operates on homogeneous datasets (e.g. communication traces) and also the remediation actions are of the same kind (e.g. the selective dropping of packets belong to a DDoS attack at the different gateway routers). Within vertical AMLR information exchange and coordinated detection takes place across different system levels (e.g. malware detection at the hypervisor level of a VM based data centre and network interfaces of the VMs). Vertical FMLR coordinates remediation actions taking place at different levels of the infrastructure

TABLE II: Analytical vs. Functional MLR

	Horizontal	***Vertical***	***Multi-dimensional***
Analytical MLR	meta-data based analysis; dependency & cross-verification	joint feature analysis; anomaly detection in system context	meta-data based analysis; dependency & cross-verification; system & cross-domain context
Functional MLR	analysis based on homogeneous data; co-ordinate remediate across multiple systems of same level	analysis based on cross-system level data; system-level remediation, single context	analysis based on multi-source cross-system level data; cross-level remediation between multiple systems

(e.g. dropping packets that have been identified as malicious at the networking level and blocking system calls from malware related activities at the operating system level).

Essentially, horizontal forms of MLR operate on (sub-)systems of the same type, have a more homogeneous information and data basis, and remediation mechanisms are of similar kind (e.g. they are either network based or OS level remediation). In contrast, vertical MLR looks at infrastructure components with substantially different functionality and relies on the exchange and interpretation of information of different types (e.g. packet and flow based network data and system information such as CPU utilisation or number of processes). This is also true for the subsequent remediation action, which have to be tailored to a specific infrastructure component of a specific system level.

If horizontal and vertical aspects of MLR are considered together this is called *multi-dimensional* MLR. An example for this is the coordinated analysis and instantiation of protective mechanisms in distributed data centres where system and networking properties are jointly analysed and appropriate remediation actions are taken across the different infrastructure components. In parallel, SMLR is always offline and FMLR is by its nature an online operation, whereas AMLR can be both. But if it is carried out off-line it is for forensic purposes. Table II summarises the characteristics of both analytical and functional MLR.

III. MLR in Practice

Cloud resilience has gained some visibility recently [14], [15]. However, the main focus of these activities are at the virtual machine (VM) level and the detection and protection from misuse and threats towards hosted services. What has gained less attention so far are anomalies affecting the cloud management or how vulnerabilities at this level could be exploited. In the following use case we are looking specifically at cloud management-related anomalies and their effect as well as the feasibility of their detection while considering different information sources. Through this case study we demonstrate how some of the MLR concepts manifest themselves in such a concrete case.

A. Case Study: Cloud Management

A specific threat to cloud management is the exploitation of specific actions the Cloud Management System (CMS) takes in response to certain events. For instance, the CMS will try to load balance in case of growing demand. Thus, if a VM is resized it will eventually get migrated to another physical machine. Essentially, this feature can be exploited by an attacker who maliciously resizes the VM and triggers the CMS to migrate the VMs. Unavoidably, the latter action could potentially lead to a deterioration in the performance and availability of cloud resources.

In the experiments carried out for this study we used a set-up with three physical machines of which two are running a range of cloud services (such as a mail server, Web Server, File Server, Haddop, etc.) whereas one is running the CMS (in our case OpenStack running on Ubuntu 12.04). During the test, two VMs are resizing, one carries out a legitimate resizing action (i.e. moving from 1vCPU, 2GB RAM, 40GB Disk, 386MB Swap to 2vCPU, 4GB RAM, 60GB Disk, 512MB Swap) whereas the other one maliciously resizes (i.e. going to 4vCPU, 10GB RAM, 120GB Disk, 1024MB Swap). Both actions take place at the same time (i.e. minutes 1 and 6). Our detection approach relies on the methodology illustrated in Fig 1. Our initial empirical observations allowed us to establish the relevant network and system features (note, the network feature are to the separate management network, not the general Cloud interconnection) as well as thresholds that allow to distinguish legitimate resizing from excessive (i.e. malicious) resizing activities. Subsequent to the initial data pre-processing performed over the measured raw features, we run the AD3 density detection algorithm in order to achieve real-time anomaly detection. The background (management) network traffic was generated through Web, FTP, Mail, and a Hadoop HDFS Job and system data were collected at both compute nodes (i.e. physical cloud service machines).

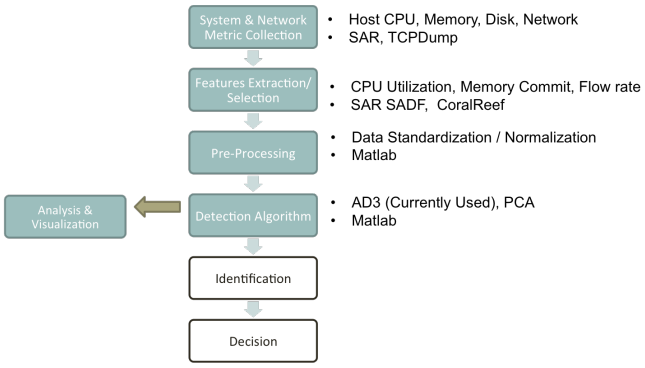

Fig. 1: Detection Methodology within a Cloud Management Scheme

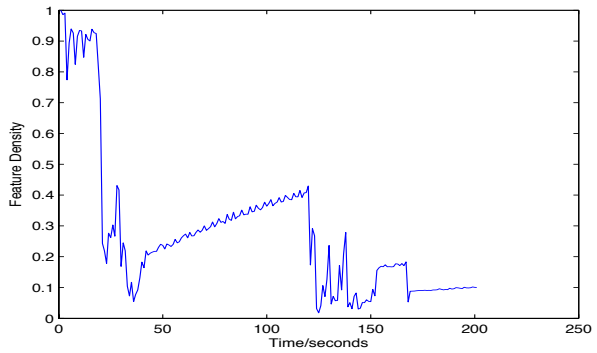

Fig. 2: Simultaneous malicious VM resizing on a physical host

B. Results in the Context of MLR

Figure 2 shows the results of the AD3 analysis. The features that have been identified as relevant for VM resizing anomalies are *MngtByteCount, MngtPktsCount*, *CPU and Memory Commit*. The identified features are on the one hand network level features and on the other hand system level features. According to the MLR taxonomy this is a case of vertical analytical multi-level resilience (vAMLR) where features from different system levels within the same system context are taken into account. As can be seen, in both cases where the resizing takes place there is a significant drop in the observed normalised data density that consequently indicates an anomaly. However, what the analysis does not allow to do is to identify the cause, i.e. the attribution of the anomaly and identification of the source is not possible. In order to attribute our anomalies we consider additional information sources. In our use case we have utilised the system log to identify the VM and processes that have carried out a resizing activity and subsequently to compare their actions with the original Service Level Agreement (SLA). In order to do so we looked at the OpenStack management logfile for specific time windows (i.e. the time around the anomalies were detected) and identified all re-sizing activities. The values for the memory, disk and number of CPU of the resizing attempt are used for further analysis. Since this is carried out at the level of the cloud management with a view of also managing the resilience the two detection actions together (i.e. the original AD3 analysis of system and network features and the syslog inspection) are and example of horizontal Functional Multi-Level Resilience (hFMLR). What would be the next step is the suspension of the offending VM in order to ensure that the operation of the cloud can be maintained.

IV. Conclusions & Future Work

Resilience is considered a core property of next generation networked systems. Despite the several efforts on developing resilience frameworks there has not been yet a generic, unified approach that is not tied to a particular networked application (e.g. utility networks, SmartGrid) and does not consider single-level homogeneous data for online or offline resilience mechanisms. This paper outlines the concepts and current activities undertaken in the scope of developing a unified *Multi-Level Resilience* (MLR) framework that aims to agglomerate several resilience properties and requirements. We have provide a taxonomy of MLR and present its basic principles. In addition the paper demonstrates the applicability of the concepts in the context of cloud management. In the near future we aim to use the framework in different application domains ranging from the SmartGrid up to Industrial Control Systems to prove its overall applicability.

Acknowledgments

The authors would like to thank the UK EPSRC funded "Situation-Aware Information Infrastructure" (SAI^2) project, EP/L026015/1, that has kindly supported this work.

References

[1] A. Mauthe, P. Thomas: "Professional Content Management Systems - Handling Digital Media Assets", Wiley Broadcast Series, John Wiley & Sons Ltd., 2004

[2] S. Vaughan-Nichols: "Worst DDoS attack of all time hits French site", in ZDNet", http://www.zdnet.com/worst-ddos-attack-of-all-time-hits-french-site-7000026330/, February 2014

[3] P. Mah: "Internal misconfiguration may be cause of massive Internet outage in China", in FierceCIO, http://www.fiercecio.com/techwatch/story/internal-misconfiguration-may-be-cause-massive-internet-outage-china/2014-01-24, January 2014

[4] J. Wang, L. Rong, "Cascade-based attack vulnerability on the US power Grid", Elsevier Safety Science Journal, Vol. 47, No. 10, December 2009

[5] C. Doerr, J. M. Hernandez: "A Computational Approach to Multi-Level Analysis of Network Resilience", in Third International Conference on Dependability (DEPEND), 2010

[6] P. Smith, D. Hutchison, J. Sterbenz, M. Schoeller, A. Fesssi, M. Karaliopoulos, C. Lac, B. Plattner: "Network Resilience: A Systematic Approach", IEEE Communications Magazine, vol. 49, no. 7, July 2011

[7] PaCr2015) Pandit, A., Crittenden, J.C.: "Index of Network Resilience (INR) for Urban Water Systems" International Journal of Critical Infrastructure (In Press), 2015

[8] A. Marnerides, M. Watson, N. Shirazi, A. Mauthe, D. Hutchison, "Malware Analysis in Cloud Computing: Network and System Characteristics", in proceedings of IEEE GLOBECOM CCSNA workshop 2013, Atlanta, USA, Dec, 2013

[9] Marnerides, A., K., Spachos, P., Chatzimisios, P., Mauthe, A., "Malware Detection in the Cloud under Ensemble Empirical Mode Decomposition", in IEEE ICNC 2015, Anaheim, California, Feb, 2015

[10] A. K. Marnerides, A. Bhandari, H. Murthy and A. U. Mauthe, "A multi-level resilience framework for unified networked environments," 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), Ottawa, ON, 2015.

[11] PaCr2015) Pandit, A., Crittenden, J.C.: "Index of Network Resilience (INR) for Urban Water Systems" International Journal of Critical Infrastructure (In Press), 2015

[12] J. Sterbenz, D. Hutchison, E. Cetinkaya, A. Jabbar, J. Rohrer, M. Schoeller, P. Smith: "Redundancy, Diversity, and Connectivity to Achieve Multilevel Network Resilience, Survivability and Disruption Tolerance", Journal Telecommunications Systems, vol. 56, no. 1, May 2014

[13] A. Marnerides, C. James, A. Schaeffer-Filho, S. Sait, A. Mauthe, H. Murthy: "Multi-level network resilience: traffic analysis, anomaly detection and simulation", in ICTACT Journal on Communication Technology, Special Issue on Next Generation Wireless Networks and Applications. Vol. 2, No. 2, June 2011

[14] M. R. Watson, N. u. h. Shirazi, A. K. Marnerides, A. Mauthe and D. Hutchison, "Malware Detection in Cloud Computing Infrastructures," in IEEE Transactions on Dependable and Secure Computing, vol. 13, no. 2, pp. 192-205, March-April 1 2016.

[15] N. Shirazi, S. Simpson, S. Oechsner, A. Mauthe, D. Hutchison, "A framework for resilience management in the cloud", in e i Elektrotechnik und Informationstechnik, Vol. 132, No. 2, March 2015