

## Research Article

# Application-Driven OAM Framework for Heterogeneous IoT Environments

**Janez Sterle, Urban Sedlar, Miha Rugelj, Andrej Kos, and Mojca Volk**

*Faculty of Electrical Engineering, University of Ljubljana, Tržaška Cesta 25, SI-1000 Ljubljana, Slovenia*

Correspondence should be addressed to Janez Sterle; [janez.sterle@fe.uni-lj.si](mailto:janez.sterle@fe.uni-lj.si)

Received 25 September 2015; Accepted 13 December 2015

Academic Editor: M. Anwar Hossain

Copyright © 2016 Janez Sterle et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

We present a novel approach for providing a comprehensive operational picture of heterogeneous networks by collecting system information from physical, data-link, network and application layers using extended methods and mechanisms for OAM, which take into account particularities of persistent access heterogeneity and IoT. A heterogeneous OAM (H-OAM) framework is proposed with a toolset for streamlined failure detection and isolation, and automated performance measurement and monitoring. The framework combines extended standardized OAM toolsets for physical and data-link layers with multiple well-defined and recognized IP network layer toolsets, which introduces possibilities for a tactical view of the monitored system and quick root cause analysis with unified interpretation and cross-correlation of horizontal and vertical levels. A practical deployment of an H-OAM system is presented and its use is demonstrated in a live mobile IoT testbed environment where performance is a function of a wide variety of physical layer parameters that need to be tuned and monitored by the operator. Results of two concrete usage scenarios performed in cooperation with two largest Slovenian mobile operators demonstrate how continuity check and connectivity verification, and performance diagnostics are conducted for Web-based IoT applications and network services of a live operational environment.

## 1. Introduction

The expansion of smart mobile terminals and tablet computers, relocation of the services into public and private clouds, the rise of the Internet of Things (IoT), and the increasing prevalence of machine-to-machine (M2M) communication are global evolutionary trends, which have introduced new usage and traffic patterns into mobile Internet systems. IoT and M2M paradigms in particular are bringing further dynamics into an already complex mobile domain, mainly by dramatically increasing the number of communication devices connected to the mobile systems. Also, IoT will integrate a myriad of traditionally separate solutions, significantly varying in their requirements. This includes home automation, entertainment, professional business solutions, and systems of societal importance, such as electronic toll collection, traffic control, and professional networks for critical communications. Finally, IoT will power the next

generation of critical infrastructures, which will lead to even greater increase in the heterogeneity of used communication technologies. Altogether, a new era of communication environments is on its rise, the principal characteristics of which are extreme heterogeneity on all levels of the system, including access network transparency, service quality and resilience requirements, and significantly increased requirements for transmission of large volumes of data.

This calls for further research in the direction of web-based surveillance and monitoring of IoT systems and the pertaining heterogeneous communication infrastructure, with advanced mechanisms and protocols for alerting and notification, and QoS/QoE monitoring and prediction.

*1.1. EPS as an Enabler for Heterogeneous IoT Environments.* One of the answers to the upcoming challenges associated with the rise of the IoT is evolved packet system (EPS), a powerful and scalable fourth-generation communication

platform [1]. The EPS introduces a technologically advanced mobile radio system called Long Term Evolution (LTE) and a new mobile core called Evolved Packet Core (EPC), which has replaced the existing GPRS/UMTS core network [1]. One of the important capabilities provided by the EPS is the integration of heterogeneous mobile, wireless, and fixed access domains, such as HSPA, LTE, WiFi, WiMAX, xDSL, FTTH, and DOCSIS, into a single communication platform. The prestandardization directions for the fifth generation of mobile systems (5G) take this capability even further and propose additional possibilities for expansion of the packet core in the direction of satellite access networks integration into a single packet core solution. From the services' and applications' point of view, the integrated mobile, wireless, satellite, and fixed systems will become a single unified communications platform, eliminating the need for network awareness state and logic at the application level.

With this, the EPS network itself will transparently integrate heterogeneous technologies into a single communication solution in a native manner [1] and perform management of network contexts such as user presence tracking [2], enforced security policy level, assessing the performance potential of the currently camped fixed, wireless, satellite, and mobile domains, and the preservation of the required Quality of Service (QoS) and Quality of Experience (QoE) requested by the services and applications. This will significantly reduce the complexity of the service and application development and in particular their use from the perspective of the end-users. Simultaneously, the EPS allows for separation of network functions from service and application logic and hence development of decoupled application ecosystems that can capitalise on the benefits of the EPS as an enabler for ubiquitous and transparent access. These two facts stand in favour of choosing the EPS platform for the forthcoming heterogeneous IoT (H-IoT) environments.

The architecture of the EPS system, which enables the integration of the heterogeneous access systems under a single network domain, defines the following fundamental network primitives [1]:

- (i) Seamless user authentication and authorization based on the EPS-AKA and EAP-AKA safety procedures.
- (ii) Terminal authorization enabled with support for International Mobile station Equipment Identity (IMEI) identifier.
- (iii) Security context (privacy and integrity) transfer between 3GPP and non-3GPP systems enforced with strong encryption algorithms, such as Advanced Encryption Standard (AES), enforcing an equivalent security level in all access domains.
- (iv) Mobility and seamless session preservation by means of advanced tunnelling techniques supported by the GTP and PMIPv6/GRE protocols.
- (v) Standardized functions for international and national user and service roaming.
- (vi) Mechanisms for static and dynamic enforcement of QoS.

However, despite the well-defined network primitives and broad support for state-of-the-art networking features, there are still two main challenges that need to be addressed in the EPS system to be able to support advanced heterogeneous IoT scenarios, as follows.

Firstly, the current EPS system only supports user camping in one access domain at a time. The concept of user and network mobility, which would enable simultaneous connectivity on multiple access networks, is not foreseen in the current standard [1]. To support multihoming connectivity, it is necessary to expand the control and data plane of the current EPS system with the logic of the dual stack mobile IPv6 protocol (DS-MIPv6) [3] for user multihoming and network mobility protocol functions (NEMO) with multiple care-of-addresses support [4] for network multihoming. Such capabilities are required for demanding communication environments with high availability and redundancy constraints, such as IoT-enabled heterogeneous systems for critical communications.

Secondly, another challenge is that EPS standards [1] do not provide methods and mechanisms for collecting current system state and available capacities of network resources (hereafter "network context") provided by the heterogeneous access networks of the non-3GPP family. This includes wireless, fixed, and satellite access networks. This might lead to situations where fall-back scenarios where user switches from the 3GPP access networks (e.g., LTE) to non-3GPP ones will result in loss of control over QoS and QoE. This is not in line with the prevailing trend of launching and providing a secure and quality-aware IoT service. Also, as the amount of IoT service provisioning over various existing access networks grows, this will lead to increased occurrence of fall-back scenarios, in particular between LTE and WiFi, which will further intensify the problem of QoS control and assurance.

For such advanced heterogeneous IoT environments, an appropriate policing and OAM framework is needed, which would allow collecting the network state of utilised access technologies, as well as mapping of service requirements (service context) to the network contexts.

## 2. Background

Review of the scientific and technical literature dictates a design of a new model for management, administration, and maintenance of such heterogeneous IoT-enabled environments. The *operations, administration, and management* (OAM) in packet-based networks represents a generic technological framework that covers an area of awareness of the state of network resources, available capacity of individual network segments, connectivity verification, fault detection, and network management [5]. It is based on collecting information on the state of resources of different network domains and represents the enabler for the dynamic control of network resources through standard mechanisms defined for Next-Generation Network Architecture [6], 3GPP [7], and IETF [7].

Despite the importance of OAM mechanisms and methods for the functioning of modern communications solutions, there is no single view on the concept of OAM. On the standardization level, there is no unified understanding of required features and mechanisms that must be supported [5]. Following a review of related work in the field of standardization, specifications, and recommendations of the International Telecommunication Union (ITU-T) [8], Internet Engineering Task Force (IETF) [9, 10], Metro Ethernet Forum (MEF) [11], Institute of Electrical and Electronics Engineers (IEEE) [12], and other scientific sources [7, 13], it can be concluded that no such framework exists that would define the concept of OAM in the transport and application layers of a TCP/IP protocol stack. The existing methods and concepts are limited to physical, data-link, and network layers. They are domain specific and are limited to a particular protocol (i.e., GTP, IPv4, and IPv6) or a family of technologies (i.e., Ethernet OAM, MPLS OAM).

We therefore conclude that a design of a new model for OAM in IoT environment is needed, which will provide a unified interpretation of horizontal (end-to-end) and vertical (stack) levels in a single OAM framework, and will allow for application-driven and centralized control of resources in convergent communication environments based on collection and coordinated interpretation of physical, data-link, network, and application contexts.

In this paper, we present a novel approach for providing a comprehensive operational picture of a heterogeneous system by collecting system information from physical, data-link, network, and application layers using extended OAM methods and mechanisms, which take into account particularities of persistent access heterogeneity and IoT.

The remainder of this paper is organized as follows. Section 3 proposes a heterogeneous OAM framework and Section 4 presents a practical design and implementation of such a system. Its use is demonstrated in a live mobile IoT testbed environment with heterogeneous access options in Section 5, followed by concluding remarks and future challenges in Section 6.

### 3. Application-Driven OAM Framework

The proposed solution is an H-OAM framework, which targets an application-driven OAM toolset for heterogeneous environments, supporting the following mechanisms and functions for the IoT environments [5]:

- (i) Streamlined failure detection and isolation.
- (ii) Automated performance measurement and monitoring.

The proposed framework is designed based on extending the IETF, MEF, and ITU-T OAM toolsets, which define OAM solutions for the physical and data-link layers (e.g., MPLS, MPLS-TP, Pseudowire, Ethernet, Metro Ethernet, LTE, and WCDMA OAM), as well as multiple well-defined and recognized IP network layer toolsets (Ping, Traceroute, OWAMP, TWAMP, and TRILL OAM).

As described in [5], we follow a multilayer OAM design approach where each layer has its own OAM protocol for

collecting failure, isolation, and performance monitoring parameters. In the figure (Figure 1(a)), we propose a generic protocol stack environment for the operation of the H-OAM system, where IoT devices are connected over the connecting physical access layer to the EPC core (in the figure represented as GTP protocol layer). Physical access layer and EPC core layer are forming the foundation for the EPS bearer, which is providing virtual connection between IoT devices and the IoT services subsystem supported by the IP transport layer infrastructure.

To achieve an end-to-end OAM concept, we propose using native protocols (e.g., TCP, HTTP, and DNS) and applications (e.g., *wget* [14] and DNS *dig* utilities [15]) as an enabler of the application OAM toolset in the IP, TCP/UDP, and application layers. Generation of diagnostic traffic with native applications and protocols is used to enforce fate-sharing between OAM traffic that monitors the data plane and the data plane traffic it monitors [5]; therefore, there is a high probability that diagnostic OAM traffic will follow the same network path and cross the same passive and active system elements as native application flows. Also, the mechanisms of the continuity check and connectivity verification messages are enforced by sending native protocol messages of the monitored applications (e.g., HTTP *get* request and response) and collecting application status messages (e.g., HTTP status codes) for fault detection and isolation [5].

Another important aspect that goes in favour of using native protocols and applications, as opposed to developing dedicated ones, is the availability of OAM peer nodes that are used during continuity check and connectivity verification process. With the use of standardized application frameworks (e.g., *wget* or full-blown web browser frameworks such as *PhantomJS*), every publicly available web server can be used as fault detection and performance measurement peer in the OAM process. This extends the reach of the H-OAM system diagnostics across the entire Internet domain.

An example report with visualization of the H-OAM diagnostic cycle for a complex multilayer IoT system based on LTE access network, consisting of the LTE Phy and data-link layers, is depicted in the figure (Figure 1(b)). It follows the layered presentation approach, with performance indicators of the LTE physical layer OAM parameters (e.g., RSRP, RSRQ, RSSI, SINR, and Tx Power) at the bottom, followed by the status parameters collected from RRC/PDCP data-link layer (e.g., camped ECI, band and bandwidth, operator identifier, and EMM states), IP layer (e.g., PING RTT and speed), and TCP/UDP layers (e.g., TCP connection time), and status of the application protocol sessions and application Key Performance Indicator (KPI) values on the top (e.g., DNS response time, HTTP status code, URL redirects, application response time, and MOS).

In contrast to existing approaches, such as [13, 16], which use only horizontal end-to-end interpretation of the monitored environment, such layered presentation enables the tactical view of the monitored system and quick root-cause analysis with unified interpretation and cross-correlation of horizontal (end-to-end) and vertical (stack layers) levels of the H-IoT communication solution.

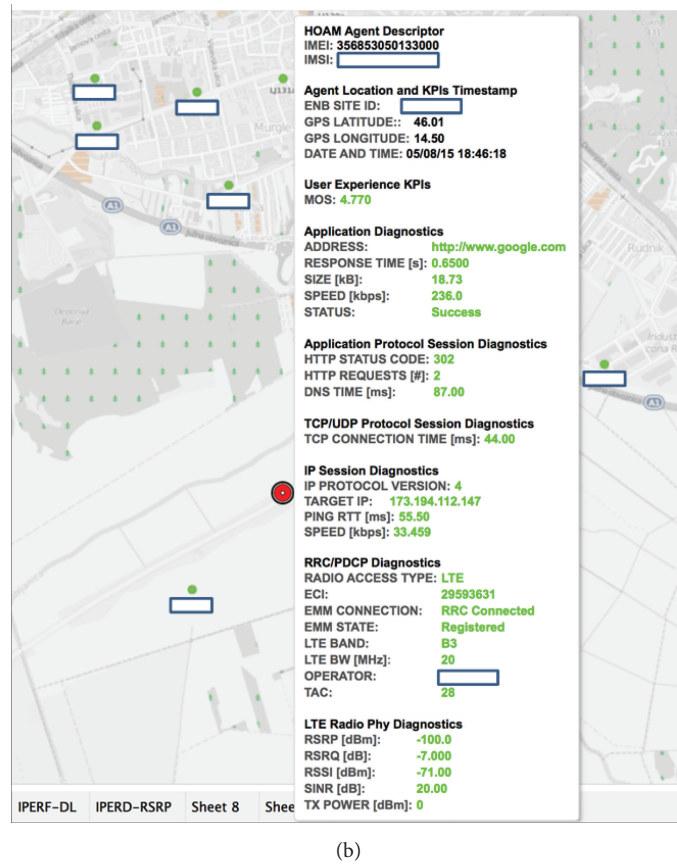
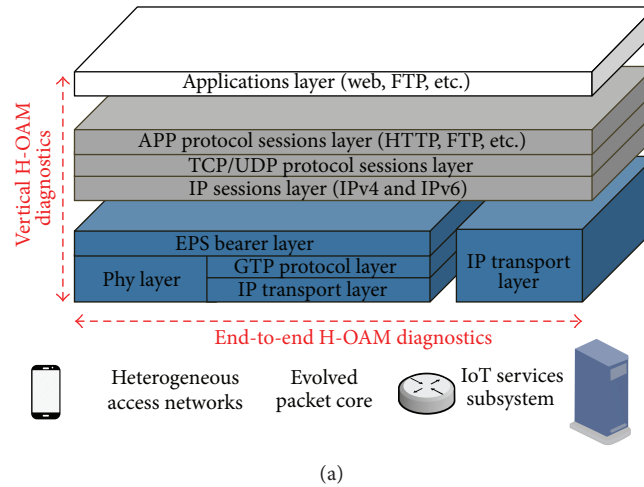


FIGURE 1: (a) Generic protocol stack for collecting OAM diagnostics in heterogeneous IoT environments. (b) Sample report for the H-OAM diagnostics.

#### 4. Design and Implementation of the Heterogeneous OAM Solution

A practical H-OAM solution was designed and implemented based on the proposed framework. The central part of the implemented framework is a system of centrally managed but autonomously operated H-OAM probes as depicted in the figure (Figure 2). The probes run purposely build software agents that are controlled from the cloud-based

management system. The agents can be configured to perform a variety of physical, network, and application-level diagnostic tests and were designed to remain autonomous if the connectivity is broken; this feature allows the agents to collect comprehensive physical, network, and application-level relevant data and submit it to the central storage when the connectivity is restored. Agents push their results (tickets) to a central H-OAM system in two ways: basic KPIs used for the connectivity check are sent to the real-time monitoring



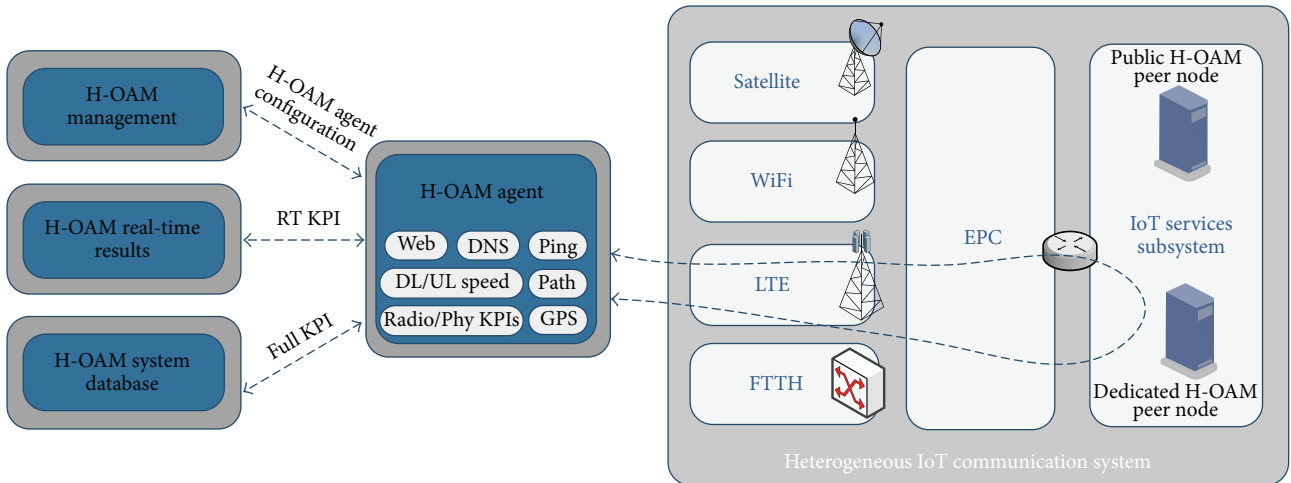


FIGURE 2: H-OAM system design.

server as they are measured, while the detailed measured and collected data are uploaded and inserted into the database after the entire diagnostic cycle is completed.

Thus, the proposed H-OAM system is by design optimized for the proactive operation mode [5]. This means that the H-OAM tests are performed on a continual basis, and keep-alive messages for continuity check and connectivity verification, as well as performance measurements, are conducted periodically, and faults or performance degradations in connectivity are detected when a certain number of expected protocol messages are not received, or when the performance KPIs are under the defined minimum threshold [5].

The presented H-OAM probes were implemented on x86 hardware running Linux OS and Python agent software that orchestrates the tests. We supported a diverse OAM toolset for network and application diagnostics, as well as for performance measurements, with some examples listed below:

- (i) Ping and Traceroute utilities for IP session connectivity check and path discovery.
- (ii) FTP, HTTP, and Iperf-based engines for diagnostics and performance measurement of mobile, wireless, and fixed access and core networks.
- (iii) wget utility [14], PhantomJS framework, and BrowserMob proxy [17] for web-based service and application diagnostics.
- (iv) DNS dig utility for DNS service diagnostics [15].

In addition, custom software logic was developed for extending the IP network and application layer indicators with physical layer indicators. For selected 2G, 3G, and 4G mobile radio modems, we developed dedicated software modules capable of capturing radio parameters and system information state. The developed OAM software module for LTE radio, for example, is capable of collecting various physical radio parameters, such as RSRP, RSRQ, RSSI, and Tx Power, as well as basic system information, such as mobile operator

identifier, cell identifier, band, channel bandwidth, tracking area code, and radio states, which are propagated over the radio interface by the mobile network system messages (MIB and SIB). These are vital indicators that define both the state and the performance characteristics of the LTE network.

Finally, a purposely built data driven analytics system was implemented for fault detection and performance monitoring in real time [18]. The dashboard console of the H-OAM module displaying active H-OAM agents with status updates, collected KPIs, and agent-generated tickets on geographical maps is presented in the figure (Figure 3).

Based on the above presented measured KPIs and collected status information on physical, data-link, network, and application layers, all fundamental tasks expected from the OAM diagnostics [5] in IoT environment can be achieved. We have demonstrated this with the following:

- (i) Continuity check of the network path, transport protocol services (e.g., TCP), and web-based applications.
- (ii) Connectivity verification based on emulation of the network and transport services and web-based applications.
- (iii) Performance measurement and monitoring of network/transport paths and applications.

Real-time KPI analytics, as well as detailed offline postprocessing and data analysis, can provide deep and multilayer insight into the health and capabilities of the monitored H-IoT system. The proposed setup supports multiple operational use cases, such as continuous service monitoring, monitoring performance and SLA of the system, predicting application performance under realistic load conditions, live network and application troubleshooting, and root-cause analysis, as well as testing, modelling, and prediction of QoS and QoE. Some exemplary insights are presented in the following.

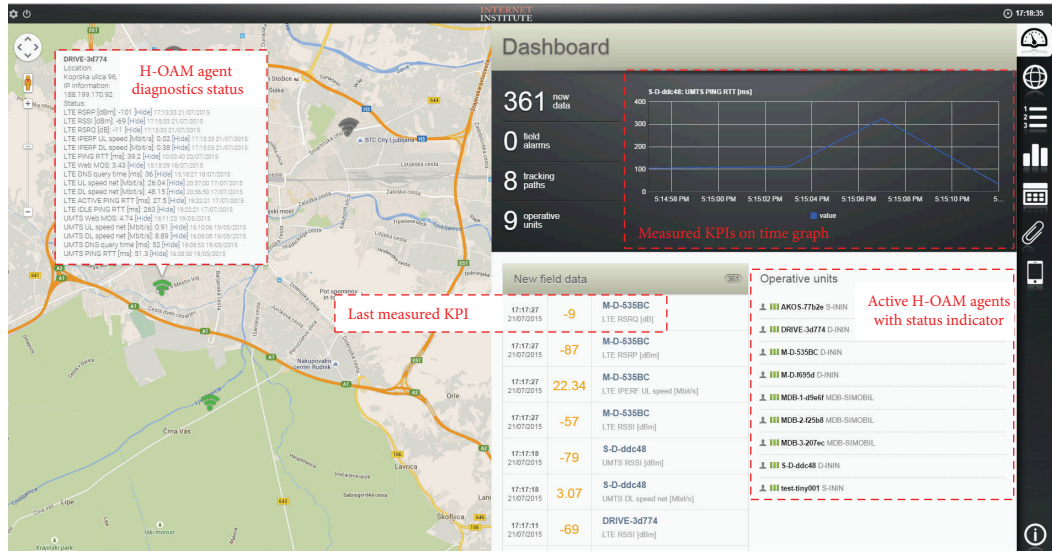


FIGURE 3: Real-time visualization and analytics of the H-OAM diagnostic KPIs.

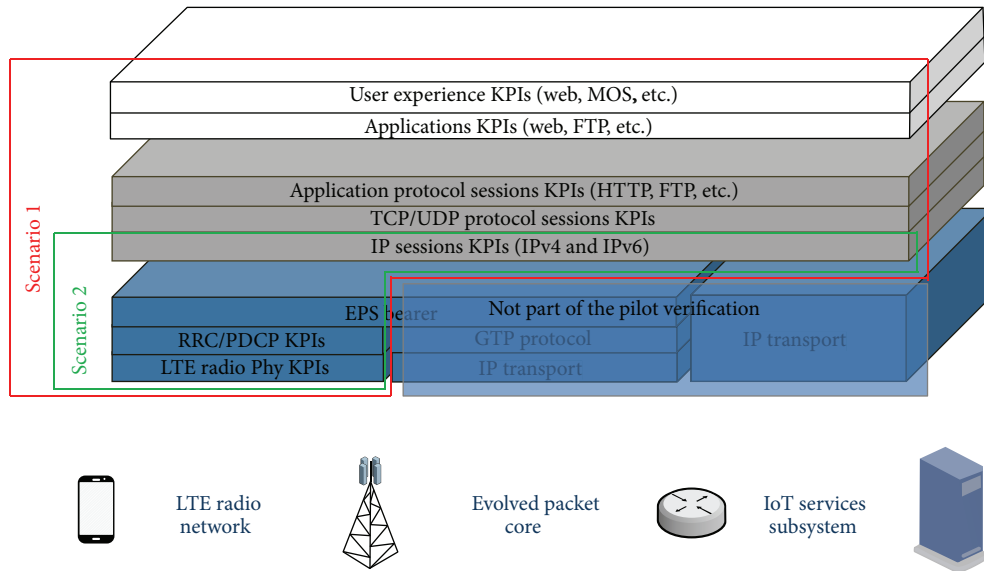


FIGURE 4: IoT system layers of the testbed environment monitored by the H-OAM agent.

## 5. System Testing and Operational Results

The presented H-OAM system was tested in the most challenging IoT setup, a live mobile network with heterogeneous access options where performance is a function of a wide variety of physical layer parameters that need to be tuned and monitored by the operator. H-OAM agents were used in two modes, as a stationary agent for a case where the system was primarily used for network and application continuity and connectivity verification and as a mobile agent for mobile system drive test verification and testing. The two largest mobile operators in Slovenia with national coverage were used as the enabling IoT testbed environment and the testing

was carried out in the period between May 1 and August 7, 2015. To verify the system operation, more than 10,000 unique diagnostic messages and performance measurements KPIs were taken with the H-OAM agent equipped with a Category 3 LTE modem.

The protocol stack of the pilot environment is shown in Figure 4. Due to the closed EPC core network deployment approach and operator's security policy issues, H-OAM diagnostic on the IP transport and GTP protocol layer was not possible and was not part of the pilot setup environment, even though the integration of the transport OAM mechanisms in the H-OAM solution would be possible.

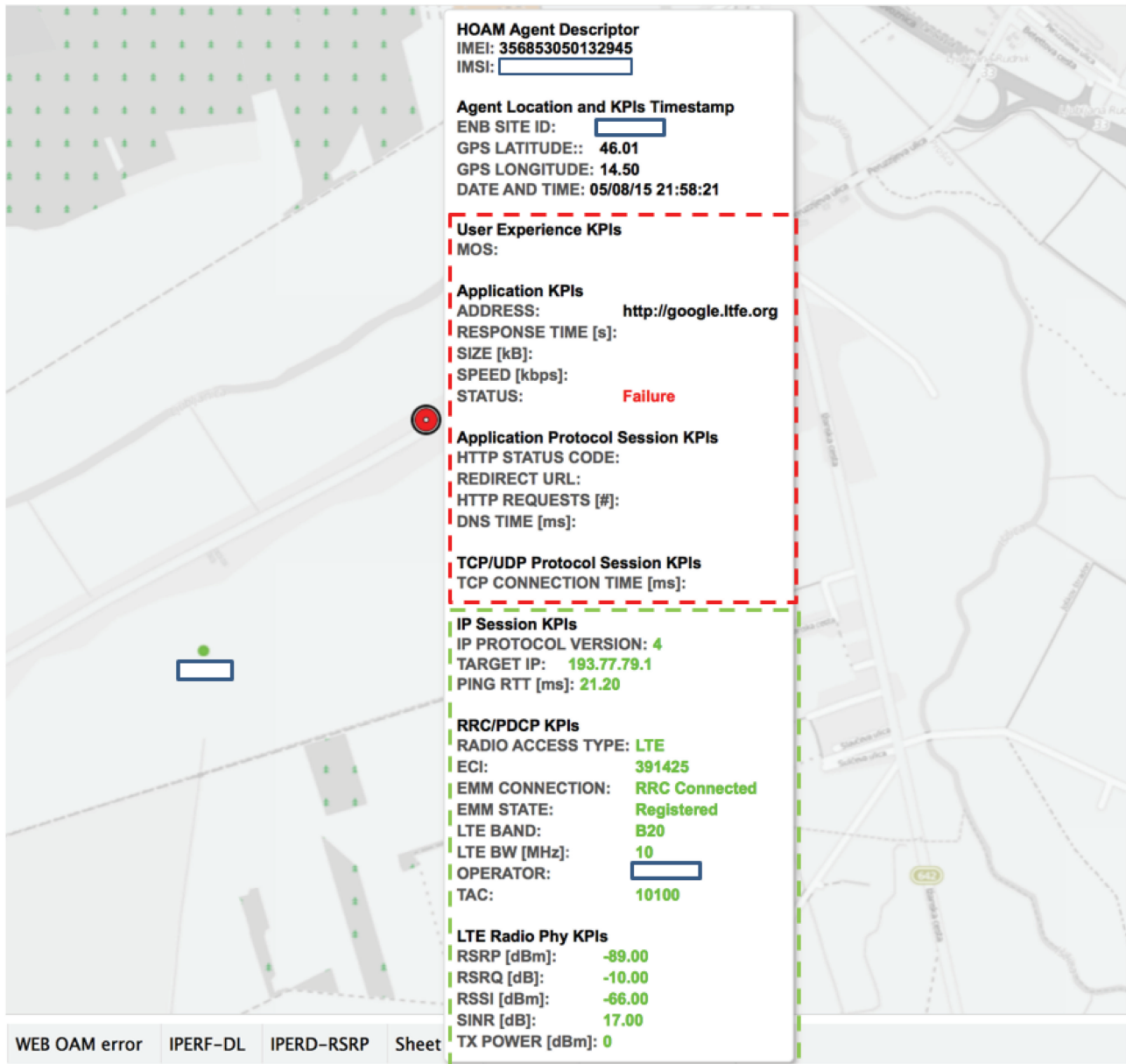


FIGURE 5: Root-cause analysis and fault localization based on the cross-layer KPI verification.

In the testbed deployment, two distinctive H-OAM use cases (Figure 4) were investigated and tested for web-based IoT applications and network services:

- (i) Continuity check and connectivity verification of the IoT applications.
- (ii) Performance diagnostics of network services.

**5.1. HTTP-Based IoT Application Monitoring.** In the first scenario, HTTP-based IoT applications were investigated for continuity check, connectivity verification, and performance diagnostics. The dashboard console was used to monitor the

collected KPIs in real time and to observe measurements in the agent tickets, as presented in the figure (Figure 3).

Complementary to that, we used advanced data postprocessing and analysis based on cross-layer KPI verification for fast problem detection and fault localization. Figure 5 shows a deployed H-OAM agent that is not able to connect to a web server service, which is indicated with the application KPI failure status. Although the connectivity from the H-OAM agent to the web server is available on the network layer (indicated by the EMM connection status and successful IP session ping response), the cause of the service fault is on the TCP level; the most probable reason for this is that the web server service is not running or is misconfigured or the TCP

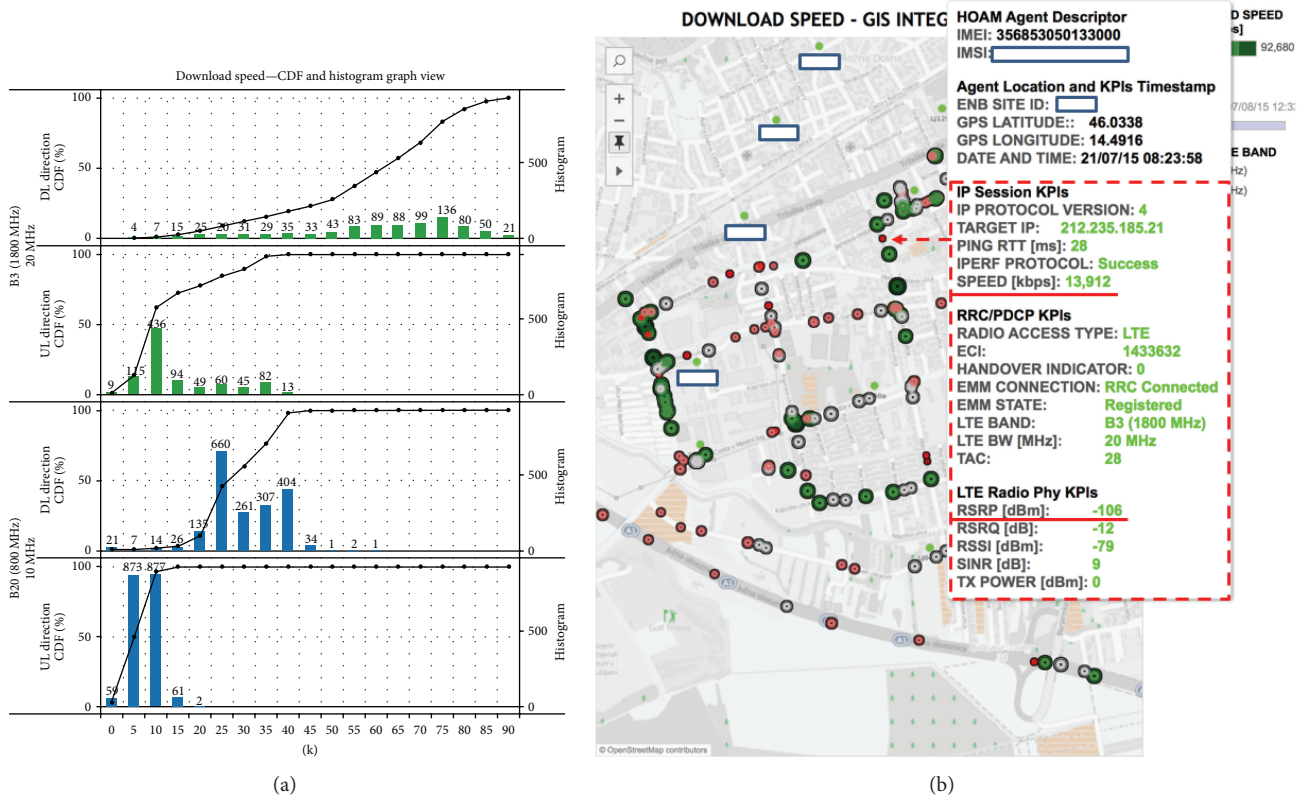


FIGURE 6: (a) CDF and histogram graph for download and upload speed. (b) Download speed map with diagnostic result for one measured ticket.

port is blocked by intermediate firewall, as can be inferred from the TCP connection timeout.

**5.2. Network Services Monitoring.** In the second scenario, network service between mobile H-OAM agents used in drive mode and a dedicated H-OAM termination point located in a data centre were investigated from the perspective of connectivity verification and performance diagnostics of the LTE mobile network. To achieve unbiased measurement results, dedicated Iperf server was deployed and extended with custom developed program logic that prevents test server overload. An area of the city of Ljubljana, Slovenia, was used as a pilot grid to perform mobile system drive test. In the figure (Figure 6(b)), download speed heat map of the measured grid is showing the areas with good bandwidth coverage indicated with scaled green dots and areas with poor bandwidth coverage indicated with scaled red dots. As can be observed from the collected diagnostic ticket in Figure 6(b), there are several reasons for varying performance of the LTE mobile interface. LTE mobile network has a complex radio access subsystem, where performance is a function of a variety of physical and data-link layer parameters that need to be tuned and monitored for optimal mobile system operation. Some of the causes of LTE connectivity performance degradation in mobile mode can be inferred from the H-OAM diagnostic measurements (Figure 6(b)):

- (i) Low mobile signal strength as a consequence of quickly changing radio propagation environment

(radio reflection from the moving vehicles and buildings), which impacts multiple radio parameters (e.g., RSRP, RSRQ, RSSI, and Tx Power).

- (ii) System frequency change (e.g., from 800 MHz to 1800 MHz) due to base station or cell change.
- (iii) Channel bandwidth change (from 20 MHz channel to 15 MHz, 10 MHz, or even less).
- (iv) High user saturation in the camped cell.

Graphs (CDF and histogram) in the figure (Figure 6(a)) show dependency of the achieved download (DL) and upload (UL) speeds of the LTE mobile interface as a function of channel bandwidth and used frequency band by the IoT device. With the channel bandwidth of 20 MHz, the achieved speed of the LTE radio interface goes up to 95 Mbps for download speed and up to 45 Mbps in the upload direction, while on the 10 MHz channel bandwidth, the upload and download speeds decrease drastically, in the download direction up to 60 Mbps and in the upload direction up to 25 Mbps.

## 6. Conclusion and Future Work

In this paper, we proposed an H-OAM framework that aims to unify diagnostics and performance measurements of heterogeneous networks. Due to the fact that heterogeneous connectivity has become the norm in IoT systems, such solution offers a wide range of applications in IoT and beyond,



including monitoring, tuning, analysing, and troubleshooting applications and network connectivity by inspecting data collected on multiple layers of the communication stack.

We demonstrated the design and practical implementation of the framework and showed that it yields useful results when deployed in a real-life LTE network to perform continuous diagnostic tests. Our implementation collects KPIs on the physical LTE layer (RSRP, RSRQ, RSSI, and Tx Power, as well as basic mobile system information) and IP and TCP/UDP layers, as well as on the IoT application layer (focusing on DNS and HTTP protocols that are common in modern IoT applications). As demonstrated, either visualization and analysis of the diagnostic results can be done in real time for a limited set of KPIs or a deeper analysis can be performed in the postprocessing.

The proposed solution leverages the EPS architecture, which makes it especially suitable for HSPA and LTE networks; however, many challenges remain with networks that are not yet integrated into the EPS, such as satellite access and simultaneous multihoming capabilities. While some of these will be addressed in 5G systems, future work is needed in this area to address unmanaged connectivity technologies.

Additionally, many opportunities exist for optimization of the proposed system in terms of diagnostic procedures that are tailored to individual use cases. In this way, different cost metrics can be applied, such as minimizing the use of resources (the required amount of traffic, processing power, or energy efficiency [19]) when they are scarce or maximizing the speed of response to changing conditions. This will be another area of research addressed in future work.

## Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

## Acknowledgments

The research and development work was in part supported by the European Commission (CIP-ICT-PSP-2011-297239), the Slovenian Research Agency under Grant Agreements P2-0246, L2-4289, and L7-5459, and Internet Institute, Ltd.

## References

- [1] 3rd Generation Partnership Project, "Technical specification group services and system aspects; General Packet Radio Service (GPRS) enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access (release 10)," 3GPP TS 23.401, 2015.
- [2] L. Vidmar, M. Štular, A. Kos, and M. Pogačnik, "An automatic Wi-Fi-based approach for extraction of user places and their context," *International Journal of Distributed Sensor Networks*, vol. 2015, Article ID 154958, 15 pages, 2015.
- [3] K. H. Lee, H. K. Jung, H. W. Lee, S. K. Lee, and Y. H. Han, "A network-based IP mobility management scheme with IPv4/IPv6 dual stack support," in *Future Information Communication Technology and Applications*, vol. 235 of *Lecture Notes in Electrical Engineering*, pp. 199–208, Springer, 2013.
- [4] C. Park, J. Park, H. Wang, and H. Choo, "The fast handover scheme for mobile nodes in NEMO-enabled PMIPv6," in *Computational Science and Its Applications—ICCSA 2012: 12th International Conference, Salvador de Bahia, Brazil, June 18–21, 2012, Proceedings, Part III*, vol. 7335 of *Lecture Notes in Computer Science*, pp. 283–296, Springer, Berlin, Germany, 2012.
- [5] T. Mizrahi, N. Sprecher, E. Bellagamba, and Y. Weingarten, "An overview of operations, administration, and maintenance (OAM) tools," RFC 7276, IETF, 2014.
- [6] J. Song, M. Y. Chang, S. S. Lee, and J. Joung, "Overview of ITU-T NGN QoS control," *IEEE Communications Magazine*, vol. 45, no. 9, pp. 116–123, 2007.
- [7] I. Atanasov, E. Pencheva, and R. Dimova, "Toward open service access to policy and charging control in evolved packet system," *Telecommunication Systems*, vol. 59, no. 3, pp. 365–380, 2015.
- [8] International Telecommunication Union, "OAM functions and mechanisms for Ethernet based networks," ITU-T Recommendation Y.1731, 2008.
- [9] P. Saste and J. Martis, "Converged OAM," in *Proceedings of the 2nd International Conference on Computer and Communication Technologies*, vol. 381 of *Advances in Intelligent Systems and Computing*, pp. 437–444, Springer, 2015.
- [10] T. Nadeau, M. Morrow, G. Swallow, D. Allan, and S. Matsushima, "Operations and management (OAM) requirements for multi-protocol label switched (MPLS) networks," RFC 4377, IETF, 2006.
- [11] Metro Ethernet Forum, "Service OAM requirements & framework—phase 1," MEF Technical Specification MEF 17, 2007.
- [12] M. McFarland, S. Salam, and R. Checker, "Ethernet OAM: key enabler for carrier class metro ethernet services," *IEEE Communications Magazine*, vol. 43, no. 11, pp. 152–157, 2005.
- [13] B. Hedstrom, J. Schnitzer, and A. Sundelin, "An efficient mechanism for service OAM performance monitoring metric collection for MEF carrier ethernet," *IEEE Communications Magazine*, vol. 50, no. 9, pp. 81–87, 2012.
- [14] Gwget, July 2015, <https://projects.gnome.org/gwget/>.
- [15] July 2015, <http://www.isc.org/downloads/>.
- [16] R. Hofstede, I. Drago, G. C. M. Moura, and A. Pras, "Managing the dynamics of networks and services: carrier ethernet OAM: an overview and comparison to IP OAM," in *Proceedings of 5th International Conference on Autonomous Infrastructure, Management, and Security (AIMS '11)*, Nancy, France, June 13–17, 2011, vol. 6734 of *Lecture Notes in Computer Science*, pp. 112–123, Springer, 2011.
- [17] PhantomJS Project, July 2015, <http://phantomjs.org/>.
- [18] QMON project, July 2015, <http://www.qmon.eu>.
- [19] I. Humar, X. Ge, L. Xiang, M. Jo, M. Chen, and J. Zhang, "Rethinking energy efficiency models of cellular networks with embodied energy," *IEEE Network*, vol. 25, no. 2, pp. 40–49, 2011.

