INTERNATIONAL JOURNAL OF NETWORK MANAGEMENT
Int. J. Network Mgmt 2017; **00**:1–22
Published online in Wiley InterScience (www.interscience.wiley.com). DOI: 10.1002/nem

Enabling autonomicity in wireless mesh networks with the ETSI AFI GANA reference model

Szymon Szott[1]*, Janusz Gozdecki[1], Katarzyna Kosek-Szott[1], Krzysztof Loziak[1], Marek Natkaniec[1], Michal Wagrowski[1], and Ranganai Chaparadza[2]

[1]*AGH University of Science and Technology, Poland*
[2]*IPv6 Forum*

SUMMARY

The distributed nature of wireless mesh networks (WMNs) allows them to benefit from multiple autonomic functionalities. However, the existing landscape of self-x solutions (e.g., self-configuration) is fragmented and the lack of a standardized framework through which interoperable autonomics can be developed has been hampering adoption and deployment of autonomics in real world service networks. There is a need for a standardized architectural framework that enables to comprehensively support and integrate interoperable components for autonomicity in WMNs. Such an architecture (autonomicity-enabled wireless mesh architecture) is currently being standardized by the working group called Evolution of Management towards Autonomic Future Internet (AFI) in the European Telecommunications Standards Institute (ETSI) within the Network Technologies (NTECH) Technical Committee. The proposed autonomic wireless mesh architecture is an instantiation of the AFI GANA (Generic Autonomic Network Architecture) Reference Model a standards based approach to autonomics. This paper complements and extends the early version of the architecture by further detailing the architectural principles and providing experimental and validation results. First, we provide a brief overview of the AFI GANA Reference Model and then show how each of its building blocks can be instantiated for WMNs. We evaluate the proposed architecture by implementing and testing the four basic self-x functionalities defined by the GANA model. The provided guidelines can now help researchers and engineers build autonomicity-enabled WMNs using a standardized framework that enables adoption and deployment of autonomics by industry, thereby enabling researchers and engineers to contribute to the further evolution of the standard in ETSI. Copyright © 2017 John Wiley & Sons, Ltd.

Received . . .

KEY WORDS: Standardized autonomicity-enabled wireless mesh network architecture; European Telecommunications Standards Institute (ETSI); self-organization; wireless mesh networks.

1. INTRODUCTION

Wireless mesh networks (WMNs) are known for their autonomic (i.e., self-managing) functionalities such as self-discovery and self-configuration. Furthermore, there exist a number of other mesh functionalities that offer the opportunity to introduce autonomicity such as neighborhood discovery, peer establishment, and channel management. For these reasons, WMNs are a great example to demonstrate not only the general advantages of autonomicity but also the benefits of a standardized autonomicity-enabled WMN reference architecture that is a result of instantiating a generic reference model for autonomic networking, cognitive networking and self-management

*Correspondence to: E-mail: szott@kt.agh.edu.pl

Contract/grant sponsor: Polish National Science Centre; contract/grant number: DEC-2011/01/D/ST7/05166

called the GANA (Generic Autonomic Network Architecture) model being standardized by the European Telecommunications Standards Institute (ETSI) in the "Evolution of Management towards Autonomic Future Internet" (AFI) working group [1, 2].

The AFI GANA Reference Model specifies the Functional Blocks (FBs) and the characteristic information that should be conveyed on the reference points among them for enabling autonomics in a network's data plane architecture and in its management and control architectures. It unifies the concepts of autonomic networking, cognitive networking, and self-management within a single holistic architectural reference model that is generic (as required of reference models) [1].

Research communities are now encouraged to adopt GANA as a standardized reference model and instantiate it in various reference architectures in their continuing research work in the field of autonomic networking, cognitive networking, and self-management [3]. The goal is to produce research results that can be used in accelerating the deployment of the autonomics technology while providing feedback to the responsible standardization groups. This is our motivation in this paper, in which we provide guidelines for the process of instantiating the AFI GANA Reference Model onto an IEEE 802.11-compliant wireless mesh network architecture[†]. Specifically, these guidelines are intended to:

- clarify and demonstrate the process of the instantiation of the AFI GANA Reference Model onto a wireless mesh architecture in order to create an *autonomic wireless mesh architecture* with the necessary GANA building blocks that enable developers to implement autonomics and self-x functionalities,
- present this new architecture to the mesh networking community in order to help designers to adequately place the control-loops and cognition as well as understand the notion of nesting and hierarchy of control-loops, by using the depicted place-holders for control-loops in the autonomicity-enabled WMN,
- encourage the mesh networking community to contribute to further describing the characteristics of the instantiated model (by using knowledge from other architectural frameworks and research projects) as well as to map their own work onto the autonomic wireless mesh architecture (with instantiated GANA functional blocks for autonomics) in order to elaborate on characteristics, data models, and other details that are implementation-oriented. This also enables them to respond to the call for PoCs (Proof-of-Concepts) on autonomics open in ETSI[‡].

The rest of the paper is structured as follows. In Section 2 we explain how GANA is related to other standardization efforts. In Section 3 we provide background knowledge on WMNs and show areas where autonomicity has currently been applied. Additionally, we show how our contribution fits into the state of the art. The GANA-oriented autonomic wireless mesh architecture is presented in Section 4. Therein, we first provide a brief overview of the AFI GANA Reference Model and then show how each of its building blocks can be instantiated for WMNs. We evaluate the architecture by demonstrating several self-x functionalities implemented using the instantiated GANA architecture (Section 5) – thereby complementing the aspects covered in [4]. Finally, in Section 6 we conclude the paper and outline future work. The nomenclature specific to this paper is given in Table I.

2. AUTONOMICITY-RELATED STANDARDIZATION EFFORTS

Even though the research community has been producing results in the area of autonomic networking, autonomic computing, and self-management, the development of standards had not yet been started until the recent efforts by ETSI within the AFI working group [1, 5] of ETSI's Network Technology (NTECH) Technical Committee. Various approaches to the area of autonomic

[†] Despite the focus on IEEE 802.11 networks, the presented ideas are potentially applicable to other mesh network types
[‡] http://ntechwiki.etsi.org

Table I. Nomenclature

DE	Decision-making-Element
DP&F	Data Plane and Forwarding
GANA	Generic Autonomic Network Architecture
GCP	Generalized Control Plane
KP	Knowledge Plane
MAN	Mesh Access Node
MBTS	Model-Based-Translation Service
ME	Managed Entity
MGW	Mesh Gateway
MRN	Mesh Relay Node
ONIX	Overlay Network for Information eXchange
Rfp	Reference point
RM_DE	Routing Management DE
RS_DE	Resilience and Survivability DE
WMN	Wireless mesh network

networking and management as described in [1] are generally characterized by the following limitations:

- Some approaches focus on attempts to introduce autonomics and self-management in existing network architectures in a way that is constrained by those architectures' inherent limitations and architectural principles, without a separation of generic architectural principles from implementation strategies and methods. Yet throughout the history of telecommunications, the OSI Reference Model has served the purpose of a generic model for the domain of networking in general, i.e., a reference model (in the true sense of a reference model by virtue of being a generic framework) that can be instantiated in various types of implementation-oriented technology specific reference architectures such as the PSTN, GSM, and UMTS architectures. For the domain of autonomic networking, cognitive networking and self-management a standardized generic reference model is now required. Such a generic model can then be instantiated onto any implementation-oriented reference network architecture, such as the 3GPP Evolved Packet Core (EPC) network architecture and the Broadband Forum's (BBF's) TR101 reference architecture, to create an autonomics-enabled reference architecture.
- Other approaches attempted to introduce autonomics in limited scopes either within the management plane, within individual network elements or even within individual networking protocols or applications, without being guided by a holistic generic architectural framework that should define the various abstraction levels at which autonomics and self-management capabilities can be designed from within a network element up to the management plane (with interworking between the abstraction levels). An attempt to create an evolvable holistic framework as a required generic architectural reference model was initiated by the European Commission-funded FP7 EFIPSANS project [6] that worked on introducing and validating the concept of a Generic Autonomic Networking Architecture (GANA), which was then evolved and extended in standardization efforts in ETSI.

Therefore, what is now proving to be helpful for the global community on autonomic network management and control of networks and services is the establishment of a standardized architectural reference model for autonomic networking, cognitive networking, and self-management, due to the fact that these concepts are closely related and must be unified within a single framework (expected to be generic and holistic). Such a model can then be applied in implementing interoperable systems that exhibit autonomic, cognitive, and self-management properties in their own capacity and collaboratively as networked systems. In [1, 5], the model in [6] was adopted and evolved by the ETSI AFI standardization group to create the AFI GANA Reference Model for Autonomic Networking, Cognitive Networking and Self-Management.

DOI: 10.1002/nem

The AFI GANA Reference Model unifies the various viable approaches developed by the research community through a more holistic architectural reference model that is generic enough to be applied to any particular implementation-oriented reference architecture in which autonomics, cognition, and self-management need to be introduced, e.g., in 3GPP, NGN, BBF, or wireless mesh architectures. The ETSI NTECH AFI Group fused a number of leading autonomics efforts/models, including FOCALE, IBM-MAPE, the 4D architecture, the Knowledge Plane for the Internet and other models, and developed GANA as a Unified Reference Model for Autonomic Networking, Cognitive Networking and Self-Management [1, 2]. The ETSI NTECH AFI WG is now producing a number of instantiation cases of the GANA onto various reference architectures towards industrial implementation of interoperable autonomics. For example, ETSI has published (in October 2016) the ETSI TR 103 404 on GANA instantiation onto the 3GPP Backhaul and Core architectures for enabling autonomics and self-management in such networks [7], while a separate effort for instantiating GANA onto the BBF architecture is under development [8].

GANA distinguishes itself from other proposed autonomic and self-management architectural frameworks [9] in two ways. First, it represents a comprehensive approach which is not focused on one particular network type or a single self-x functionality (self-configuration, self-healing, etc.). One of the goals of the AFI group is instantiating the GANA reference model onto existing reference architectures for both wired and wireless network environments. Second, it is currently being developed as part of ETSI standards. Therefore, it has the potential to be implemented and deployed by the industry at large. To summarize, GANA represents a broad vision (all network types and self-x functionalities) which is supported through ETSI standardization.

It is also important to note that GANA as reference model for the AMC (Autonomic Management and Control of Networks and Services) paradigm, is now being integrated with reference models for the other emerging complementary networking paradigms of NFV (Network Functions Virtualization) [10], SDN (Software-Defined Networking) [11], E2E Orchestration of resources and services, and Big-Data Analytics for AMC. A recently launched industry initiative is addressing this topic and producing a unifying architecture in which these emerging networking paradigms are integrated [12]. More details on this topic, including how the Hybrid SON (Self-Organizing Networks) model being deployed today is actually compliant with the GANA model, are available in [2].

3. AUTONOMICITY IN WIRELESS MESH NETWORKS

Wireless mesh networks can be applied in many use cases. In this paper we focus on a scenario in which the wireless mesh network is treated as an access network with a single operator. The operator offers a relaying service for other operators or regular Internet access to end users. In such a scenario, a typical WMN topology is depicted in Figure 1. It consists of interconnected generic mesh nodes which may be of the following types:

- Mesh Gateway (MGW) — interconnects the mesh and the core networks using either wireless or wired links,
- Mesh Access Node (MAN) — offers network access to end users, typically equipped with at least two wireless interfaces: one for providing network access and the other for connecting to the mesh network,
- Mesh Relay Node (MRN) — interconnects MANs with MGWs and relays user traffic.

The key characteristics of WMNs distinguish them from IEEE 802.11 ad-hoc and infrastructure networks. The most fundamental differences are as follows:

- mesh nodes are stationary, so routing protocols do not need to take into account mobility aspects,
- mesh nodes have a regular power-supply, so power-saving issues (e.g., forced rerouting in case of low energy levels) are not applicable,
- all traffic at MRNs is transit, relayed between the access nodes and the gateways,

DOI: 10.1002/nem

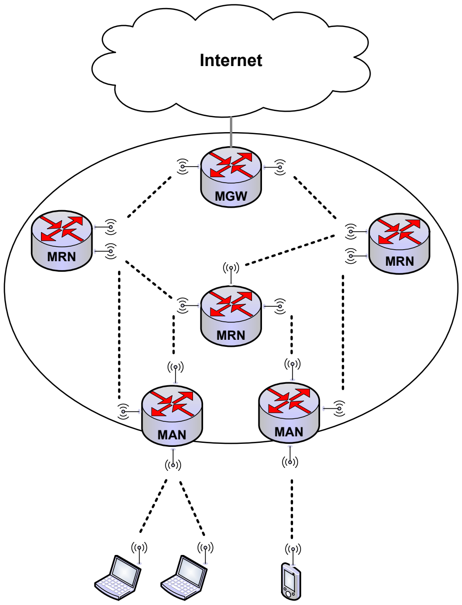


Figure 1. A typical wireless mesh network deployment: a single-operator access network [3]

- the set of links between mesh nodes is fixed.

These differences lead to the conclusion that a simple adaptation and direct implementation of well-known solutions (e.g., routing protocols from mobile ad-hoc networks) may result in suboptimal network operation. Therefore, multiple mesh-specific solutions (protocols, services, mechanisms) have been developed.

The goal of these solutions is to ensure the commercial success of wireless mesh network deployments, which relies on achieving the following objectives [13]:

1) smooth initial mesh network deployment and auto-configuration of nodes joining the mesh network without disturbing its correct operation,

2) connectivity with an adequate level of quality of service (especially for multimedia traffic),

3) dynamic node reconfiguration (e.g., coding scheme adjustments) in case of degradation of radio conditions which affect a selected part of the mesh network topology,

4) dynamic reconfiguration of the whole mesh network topology if link or flow optimization is required due to serious network failure (e.g., an MGW suddenly fails).

From this perspective it is clear that autonomic and self-management principles are essential within the mesh protocol stack.

This inherent need for autonomicity in WMNs has been noticed by researchers and engineers. The state of the art is abundant with examples of applying self-x functionalities to WMNs. Table II contains a brief overview of mesh functionalities that can be augmented with self-x behavior. Among the key enablers of autonomic behavior is continuous monitoring (Section 5.1). It allows for the efficient realization of different mesh-specific functionalities including initial node configuration, intrusion detection as well as channel, topology, and fault management.

Despite research performed in the respective areas (Table II), there remains the problem of the fragmentation of the proposed solutions. Much effort has been put into solving singular problems but now is the time to analyze how to achieve convergence among these efforts. This can be achieved through the autonomic wireless mesh architecture proposed in the following section (i.e., an architecture that takes into account the need to interwork various abstraction levels for autonomics defined by the AFI GANA model).

DOI: 10.1002/nem

Table II. Mesh functionalities that can be augmented with self-x behavior

Self-x behavior	Brief definition	Mesh specific functionality
Self-optimization	Improving performance and efficiency by tuning resources and balancing workloads	Radio technology selection, channel management [14, 15, 16, 17], congestion control [18], routing [19, 20, 21] and flow capacity optimization [22]
Self-configuration	Adding and accommodating new functional components	Topology management (performing network reconfiguration and incorporating new nodes into the existing structure) [23, 24, 25, 26]
Self-healing	Processing, discovering, diagnosing, and acting to prevent disruptions	Fault management (e.g., caused by unstable radio links) [27]
Self-protection	Anticipating, detecting, identifying, and protecting against threats	Intrusion detection [28, 29], detecting [30, 31, 32], reacting to [33, 34, 35, 36] and disincentivizing attacks [37]
Self-awareness	Conclusions derived by the system on being in a particular operational state	Continuous passive or active monitoring of the mesh network [38, 39, 40, 41, 42], interpretation and assessment of the results
Self-organization	Methods of collaboration between self-x functionalities in the context of global management objectives (policies)	Configuration of a new node (self-configuration) taking into account the optimization objectives (self-optimization) and the current state of nodes in the neighborhood (self-awareness, self-protection)

4. AUTONOMIC WIRELESS MESH ARCHITECTURE

In this section we first briefly describe the AFI GANA Reference Model and then show how its building blocks can be instantiated onto a wireless mesh architecture.

4.1. AFI GANA Reference Model

The AFI GANA Reference Model [1] is a unified model for autonomic networking, cognition, and self-management. It defines generic Functional Blocks (FBs), Reference Points (Rfps) between the FBs, and the characteristic information exchanged over the Rfps. These building blocks are specific to enabling autonomics in a target architecture. Therefore, the reference model can be instantiated onto an implementation-oriented reference architecture such as the wireless mesh architecture. The building blocks are generic enough to also be applied in designing future network architectures that must exhibit self-management capabilities from the outset.

The key aspects of the AFI GANA Reference Model can be found in Figure 2, which is an exemplary instantiation of autonomic routing. In general, self-manageability in GANA is achieved through instrumenting the network elements (the routers in this case) with autonomic **Decision-making-Elements** (DEs) that collaboratively work together. The Reference Model defines a hierarchy of DEs, i.e., four basic levels of self-management: the Protocol, Function, Node, and Network Levels. A complete list of DEs is presented in Figure 3. Each DE manages one or more lower-level DEs through a control loop. The lowest-level DEs are therefore considered the Managed Entities (MEs). Over the control loop, the DE sends commands, objectives, and policies to an ME and receives feedback in the form of monitoring information (e.g., the state of the ME) or other

DOI: 10.1002/nem

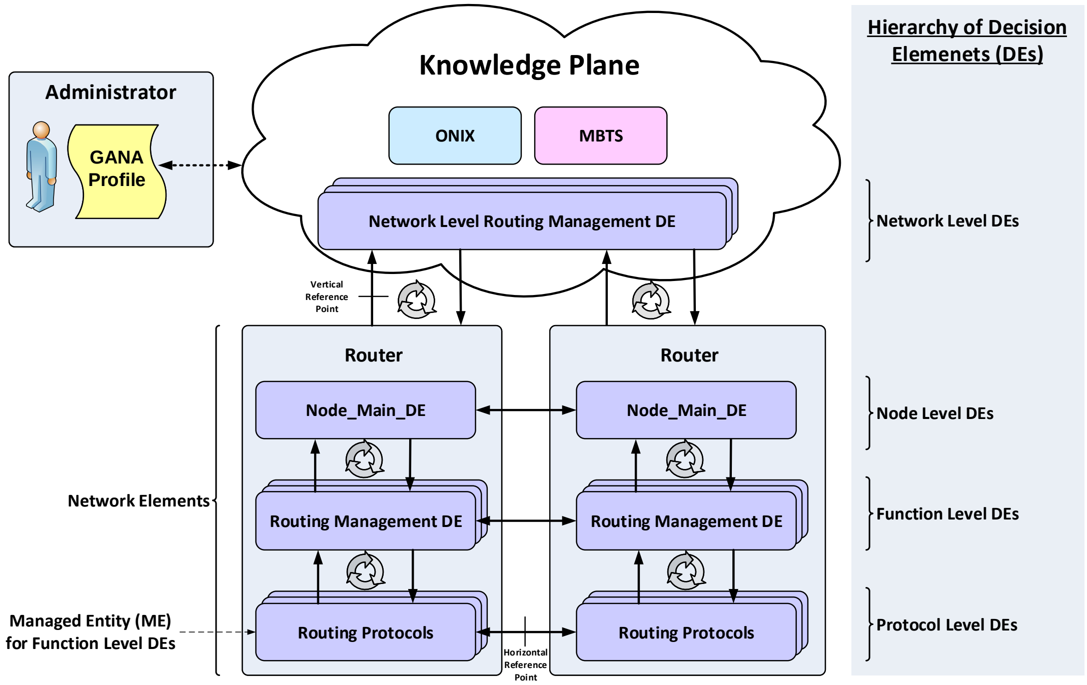


Figure 2. Global view of the GANA Reference Model as instantiated within a router [1]

type of knowledge. Each DE realizes specific control-loops and, therefore, represents an autonomic function. From an implementation perspective, the DE is the place-holder for implementing the control loops (i.e., algorithms) designed by researchers and engineers.

The lowest level DEs are at the **Protocol Level**. They represent protocols, services, and other fundamental mechanisms, possibly already implemented in today's networks. The DEs at this level are not fixed and can incorporate both existing protocols (such as OSPF – the Open Shortest Path First routing protocol) that intrinsically exhibit control-loops as well as newly designed ones. A Protocol Level DE is a decision-logic associated with a control-loop embedded inside a given protocol (if such an "autonomic protocol" has been designed already, as of today, or is desirable[§]). These DEs (seen simply as protocols) as well as all other individual protocols are managed by **Function Level** DEs such as Routing Management, Monitoring, and QoS Management. These Function Level DEs abstract specific functional aspects of the lowest level MEs (protocols, stacks, mechanisms, applications): the Routing Management DE abstracts routing protocols and mechanisms, the Monitoring DE abstracts monitoring protocols and mechanisms, etc. Currently there are seven Function Level DEs defined in the Reference Model (Figure 3). Each of them is present in every Network Element, depending on whether the element supports the relevant types of MEs at the lower level, which the DE is responsible for managing autonomically. This means, for example, if a Network Element is not meant to support routing protocols, then a Routing Management DE at the Function Level is not instantiated. The orchestration of the Function Level DEs is performed by a **Node Level** DE (the Node Main DE). There is one Node Main DE in every Network Element. At the top of the DE hierarchy, the **Network Level** DEs address similar aspects to the Function Level DEs but with a wider scope. Therefore, there is a Network Level Routing Management DE, Network Level Monitoring DE, etc. The instantiation of these DEs onto the wireless mesh architecture is described in Section 4.2.

[§] OSPF can be considered an example of the instantiation of a Protocol Level DE (though such autonomic-like features in OSPF are not cognitive in their operation and by their design).

DOI: 10.1002/nem

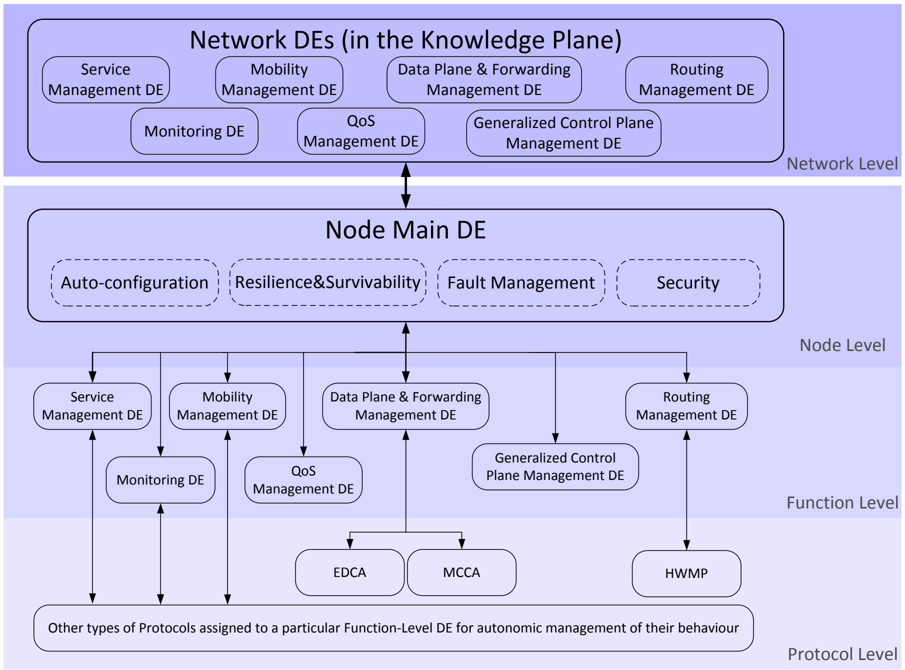


Figure 3. Block diagram of Decision Elements in an autonomic wireless mesh architecture [3]

The Network Level DEs constitute the main Functional Blocks of the **Knowledge Plane** (KP), a concept initially defined in [43] and characterized as an abstract entity which “gathers, aggregates and acts upon information about network behavior and operation” [44]. In the AFI GANA Reference Model, the KP also consists of ONIX (Overlay Network for Information eXchange) and MBTS (Model-Based-Translation Service). ONIX is a distributed scalable system of information servers that support publish-subscribe services for information discovery and exchange (to enable advanced auto-discovery), while MBTS forms an intermediation layer between the KP and the Network Elements for the purpose of translating information and commands from DEs and responses from the Network Elements. The instantiation of the KP onto the wireless mesh architecture is described in Section 4.4.

Finally, the network administrator can manage the operation of the whole network by submitting policies, network objectives and configuration data to the KP in a standardized format called the **GANA Profile** (Figure 2). This profile is composed of specific Node Profiles, which contain sub-profiles for the individual Function Level DEs to use in configuring their associated MEs. Node Profiles are then fetched by individual nodes from the ONIX (via a subscription process). Network Level DEs are involved in determining the Node Profile a node must receive based on the role it plays in the network, its point of attachment to the topology, and the capabilities of the node published into ONIX earlier.

In addition to defining the above-mentioned Functional Blocks, the AFI GANA Reference Model also specifies Reference Points: logical interfaces between Functional Blocks, over which characteristic information is exchanged. These can be either vertical (i.e., between DEs belonging to different levels) or horizontal (i.e., between DEs belonging to the same level). In the latter case, DEs form peering relationships used to exchange additional information. The instantiation of Rfps onto the wireless mesh architecture is described in Section 4.3.

According to the Reference Model, the three levels of hierarchical control loops (from the Function Level to the Network Level) that are realized by the corresponding DEs demonstrate how autonomics, cognition, and self-management can be gracefully introduced in today’s existing architectures. The Reference Model defines four basic levels of self-management, but the three levels indicated are the most important ones since it is better not to embed a control-loop into an

DOI: 10.1002/nem

individual protocol. This allows avoiding “protocol-intrinsic control-loops” which may complicate network manageability and create undesired emergent behavior in complex protocol interaction scenarios as known today (for more details on this subject, refer to [2]). As we go up the GANA DE hierarchy, more complex cognitive DE algorithms can be introduced as the scope of views operated upon by the DEs widens and the control-loops can be slower then the control-loops realized by lower-level DEs.

Having summarized the basic concepts of the AFI GANA Reference Model, we present its instantiation for WMNs in the following subsections.

4.2. Decision Elements

The complete set of Decision Elements (DEs) within the autonomic wireless mesh architecture is presented in Figure 3. The specific mesh functionalities of the most important DEs described below are presented in Table III.

There exists a strong relationship between the mesh node type (Section 3) and the supported Function Level DEs. Table IV presents a mapping between these DEs and the mesh node types. Certain Function Level DEs are critical for every mesh node type: Service Management, Monitoring, QoS Management, DP&F Management, and GCP Management. The Routing Management DE is crucial for the mesh core network which means that it should be instantiated in MGWs and MRNs. Alternatively, the Mobility Management DE, which deals with the handovers of user terminals, can be instantiated only by MANs.

For addressing the stability and coordination of DEs, the AFI GANA Reference Model includes techniques and architectural principles that ensure that control-loops can be designed in a way that guarantees non-coupling and non-conflicting behaviors of the DEs. Following these principles (in particular, the concept of DE ownership of an ME or its parameters), a DE-to-ME parameter mapping table is required for each instantiation of the reference model onto the target architecture. For all the MEs and parameters of the resources available at a node, this table must provide a one-to-one mapping of a particular configurable and controllable parameter of an ME to a single DE. Table V contains example mappings of Function Level DEs to parameters of three protocols defined by IEEE 802.11 for mesh networks: (a) Enhanced Distributed Channel Access (EDCA), (b) MCF (Mesh Coordination Function) Controlled Channel Access (MCCA), and (c) the Hybrid Wireless Mesh Protocol (HWMP).

4.3. Reference Points

The definition of Rfps within the reference model is general and abstract. Therefore, their instantiation for a target architecture (in this case: WMNs) must become precise as implementation-specific details are added. Among the Rfps defined in the AFI GANA Reference Model, in this paper we focus on intra-node and inter-node Rfps as the integration of mesh networks with management systems using the discussed reference model is left as future work.

The node-internal Rfp is a vertical interface, which implements **commands** and **views**. The commands are used to control the behavior of the MEs at the resources layer by the DE, the views are used to retrieve information from the ME. Such an interface is required to integrate an existing protocol or mechanism with the proposed architecture.

Consider a Monitoring DE in a WMN which manages monitoring protocols, services, and mechanisms. Exemplary commands it would send to its MEs include: activate, deactivate, re-start, set measurement parameters (parameter list to be monitored, algorithms to be used, etc.). Exemplary views it would receive from its MEs include: retrieved information about node neighborhood or estimated channel parameters, state changes in the ME, errors and failure indications. Such views from the MEs together with other inputs on other DE interfaces help DE developers develop the DE’s algorithm (for individual DEs) that reacts to such views in a closed-loop fashion.

An example of a vertical reference point between GANA nodes is the one between the Node Main DE and Network Level DEs. It has to implement interfaces between all DEs depicted in Figure 3 belonging to the Node and Network Levels. Besides exchanging information specific to these DEs, this interface has to implement the exchange of security-related messages (trust,

Table III. Specific mesh functionalities of important DEs

GANA Level	DE	Specific Mesh Functionality
Function	Monitoring	Manages, configures, and collects passive and active measurements on the wireless interface. Provides cross-layer measurements to support QoS, routing, forwarding, and mobility management functions. Shares the measurements or orders MEs to feed the measurements directly to the FBs that require them.
Function	DP&F Management	Manages medium access functions and node synchronization.
Function	GCP Management	Manages beaconing for synchronization purposes, performs power control to optimize energy consumption and interference levels as well as channel management for performance optimization.
Function	Routing Management	Manages routing protocol(s).
Node	Auto-configuration	Manages neighborhood discovery, peer establishment, addressing, channel management, topology management, fetching of Configuration Profiles and Policies specified by the Operator (by subscribing to ONIX to receive the Node Profile).
Network	Monitoring	Orchestrates and manages network-wide monitoring. Analyses long term data (e.g., link stability for correct routing decisions, proper channel management to avoid interference with other networks).
Network	DP&F Management	Realizes a slower control loop (than its function level counterpart), when wider global knowledge is required in addressing the problems affecting the forwarding behavior.
Network	GCP Management	Manages control plane protocols and mechanisms.
Network	Routing Management	Optimizes flow capacity, number of hops, link reliability, provides network-wide address planning, topology management (channel planning).

authentication, domain identification). This interface is also used for communication between Network and Function Level DEs via the Node Main DEs. For example, to obtain information about the link quality between two network interfaces by the Network Level QoS Management DE, a request from the Network Level QoS Management DE is sent to the Node Main DE and forwarded to the Monitoring DE.

DOI: 10.1002/nem

Table IV. A mapping between the mesh node types and the Function Level DEs

Mesh Gateway	Mesh Relay Node	Mesh Access Node
Service Management	Service Management	Service Management
Monitoring	Monitoring	Monitoring
QoS Management	QoS Management	Mobility Management
DP&F Management	DP&F Management	QoS Management
GCP Management	GCP Management	DP&F Management
Routing Management	Routing Management	GCP Management

Table V. Exemplary DE-to-ME parameter mapping

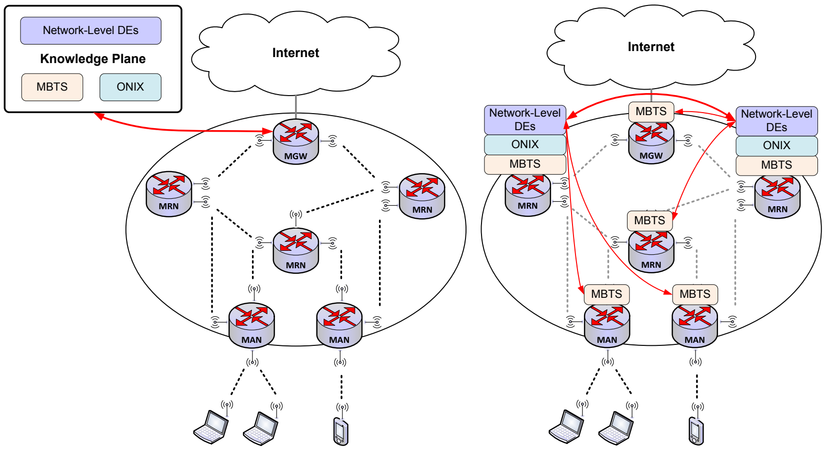
Parameter mapping	Function Level DE	ME (protocol)	Example (re)configurable ME parameter
Case 1 (preferred mapping): an ME is fully assigned to a single DE	DP&F Management DE	MCCA	Maximum fraction of time allowed for MCCA operation (Mesh Access Fraction)
	Routing Management DE	HWMP	Maximum number of retries for path request (PREQ) messages
Case 2: an ME partitioned such that varying parameter sets are assigned to different DEs	DP&F Management DE	EDCA	RTS/CTS threshold
	QoS Management DE	EDCA	Minimum contention window size for a given Access Category

To facilitate the exchange of information on the Rfps between independently developed DEs high layer protocols should be applied. This means that mainly XML-based protocols should be considered, but other solutions, such as IEEE 802.21 or SNMP may be applied as well. To additionally enhance compatibility between Node and Network Level DEs (which need to talk a language that is agnostic to the actual management protocol or vendor-specific technology used to convey management information on the Rfp) the MBTS service can be used as an interpreter and translator of exchanged messages that then takes into account technology and vendor-specific means to talk with underlying elements (nodes).

4.4. Knowledge Plane

The Knowledge Plane (KP) of the AFI GANA Reference Model is meant to be the next step in the evolution of traditional operations support systems (OSS) but can also be implemented to run as standalone entities that interwork with these systems [1]. Two paradigms can be applied when instantiating the KP onto a target architecture: centralized or distributed. For the single-operator network-access WMN scenario (Figure 1) we consider a centralized KP (Figure 4a). This centralized KP could be only logically, not physically, centralized, i.e., redundancy for resilience could be applied in the deployment of the KP. In the centralized paradigm, the KP is an independent functional block placed either in the MGW node or somewhere in the core network. In either case its location is disseminated to all mesh nodes during the auto-configuration phase.

The KP has a complete view of the whole WMN. Therefore, network operators, through direct control of the KP (including the submission of the GANA Profile, cf. Figure 2), can enforce their policies. However, if increased scalability is required then a distributed KP (Figure 4b) can be used. A comparison of the two paradigms is provided in Table VI.



(a) Centralized (b) Distributed

Figure 4. The Knowledge Plane in a mesh network [3]

Table VI. Comparison of centralized and distributed KPs

Feature	**Centralized KP**	**Distributed KP**
Scalability	Limited	Good
Information storage requirements	Low	High
Optimality	Good	Limited
Signaling overhead	Small	Large
Resilience to failures	Limited	Good
Computational capacity	Scalable	Limited
Self-configuration after network wide reboot	Simple	Complex
Self-configuration related to channel configuration	Efficient	Inefficient
Best application	Small, single-operator network	Large network

5. EXPERIMENTAL EVALUATION

In order to evaluate the usefulness of the GANA instantiation for a mesh network, described in the previous section, we implemented four self-x functionalities and performed several experiments in an autonomicity-enabled WMN. We first briefly discuss the implementation, the core of which are the monitoring functional blocks. We then proceed to describe the testbed and experiments performed. The goal of this evaluation is to highlight how designers of self-x functionalities can benefit from the presented GANA instantiation, which functional blocks require implementation, where the necessary control-loops must be placed, etc.

5.1. Implementation

In order to provide various mesh-specific functionalities, each wireless node performs continuous measurements and monitoring of several radio parameters. The monitoring of wireless mesh networks challenging due to the inherent uncertainties of the wireless medium, the impact of neighboring devices and their behavior, and finally the scarcity of bandwidth resources in an unlicensed wireless environment. Monitoring allows creating a topology of the mesh links, performing initial node configuration, and tracking changes in link parameters in order to re-configure the network in advance and according to its reliability. This is particularly true for long-term monitoring of a wide variety of radio-related parameters, which, along with additional measurements of higher layer metrics, provides an important feedback loop for all decisions taken in response to short-term radio behavior (e.g., link reconfiguration upon triggered alert). This can prevent traffic redirection through unstable links and their further reconfiguration. The granularity of the proposed measurements is fine because it considers per-frame analysis (i.e., in the time-scale of microseconds). Fast variations of radio channel characteristics require smoothing of the raw data measurements to avoid incorrect decisions based on temporary parameter values.

We have implemented the monitoring stack as two functional blocks residing in the GANA Protocol and Function Levels, respectively. The Monitoring ME, located within the kernel space of the operating system, is responsible for measurements and interface control. The Monitoring DE, located in the user space, is responsible for the aggregation and storage of the measured data. Together, the monitoring stack provides a passive monitoring service capable of measuring several parameters related to radio channel conditions, the capabilities of neighboring nodes, and the estimation of channel utilization. The Monitoring ME measures parameters at the PHY and MAC layers (with a granularity of microseconds) based on all received 802.11 radio frames. The interface's promiscuous operation mode is used to best observe the current radio channel status. Measurements are done in parallel to the regular operation of the wireless interface and can be taken for each wireless interface simultaneously. They are periodically reported to the Monitoring DE for analysis and storage. Overall, the monitoring service can be used to discover neighboring stations and calculate parameters for each of their interfaces: signal-to-noise ratio (SNR), frame and bit error rate (FER, BER), number of retransmissions, channel occupancy, frame size, etc.

5.2. *Testbed*

Building a test WMN required devices capable of supporting multiple wireless interfaces simultaneously. To avoid interference issues between the wireless interfaces of a single devices, [45], we decided to stack similar devices and have them act as a single multi-interface one. Cable-based connections and routing enabled physical emulation of a single node. We used two types of devices. The first one was based on a Mikrotik 435G router board equipped with a Mikrotik R52nM 801.11a/b/g/n wireless card and running the Mikrotik RouterOS operating system. The second was based on a Soekris Net5501 routerboard. Net5501 nodes were equipped with Mikrotik R52nM 801.11a/b/g/n or TL-WN662AG 802.11a/b/g wireless network cards. The Soekris Net5501 nodes were running Debian 6 with our GANA implementation. Initial tests showed that in terms of interference between interfaces our solution worked well.

Figure 5 presents the network topology deployed for our experiments. Four scenarios were considered (self-configuration, self-healing, self-optimization, and self-protection), each taking advantage of different parts of the network topology, as indicated in Figure 5. Stations were used as consoles for router configuration and in some cases they originated and terminated traffic. Traffic generation was done using `iperf` [46]. More details about the scenarios and test results are described in the following subsections.

5.3. *Experiments*

We conducted separate proof-of-concept experiments to demonstrate the four key autonomic principles:

- autonomic initial network bootstrap – an example of self-configuration,
- autonomic route reconfiguration – an example of self-optimization,
- autonomic response to link outage – an example of self-healing,
- autonomic response to selfish attack – an example of self-protection.

The goal of the examples is not to study the performance of the presented methods, but rather to show how certain management procedures can easily be automated using the described GANA architecture and lead to achieving a self-organizing WMN.

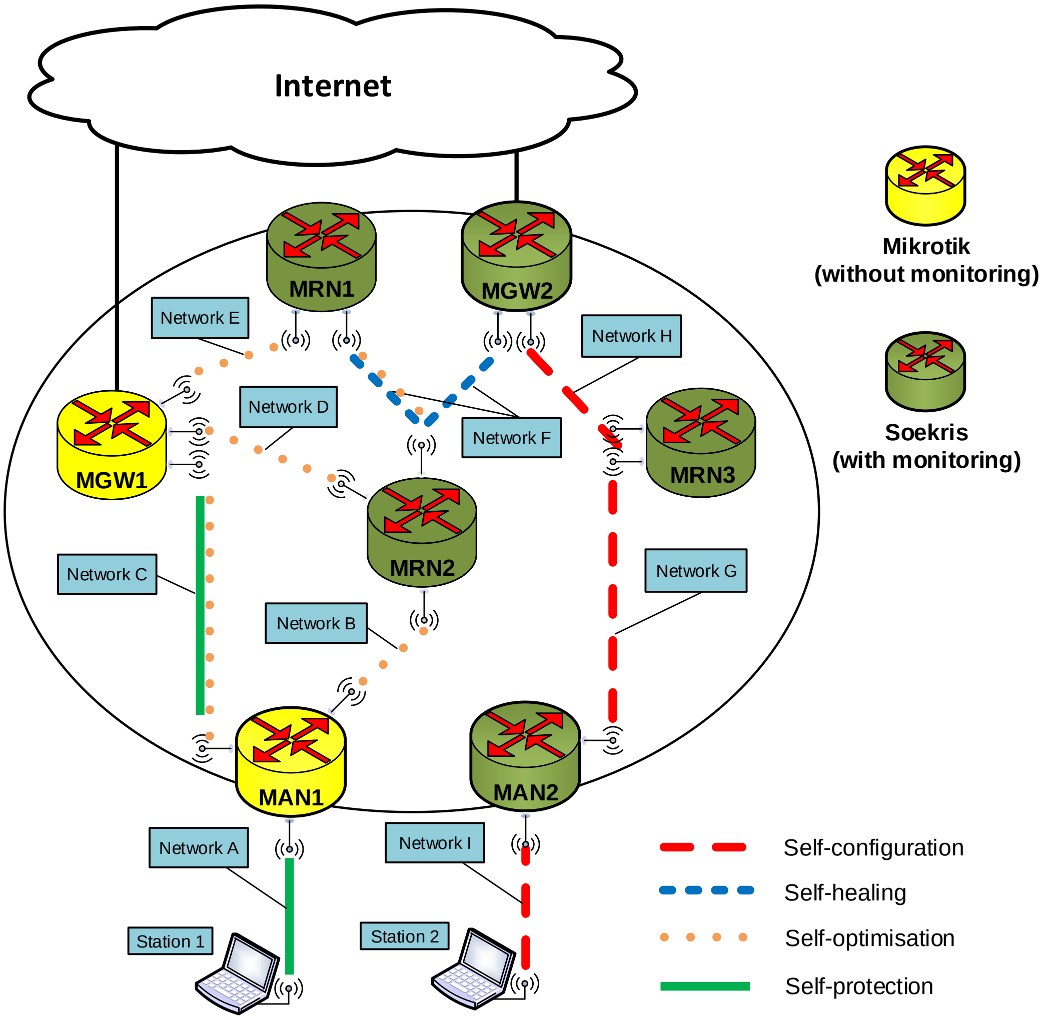


Figure 5. Network topology used during the experiments. Links which allowed studying the scenarios: self-configuration (red), self-healing (blue), self-optimization (orange), self-protection (green)

Table VII. GANA self-configuration elements involved in the network bootstrap example

GANA Level	GANA Element
Network	DP&F Management DE
Node	Auto-Configuration DE
Function	DP&F Management DE
Protocol	Interface ME

5.3.1. Self-configuration An important autonomic functionality for WMNs is network bootstrap, which provides the initial configuration of the MNs to relieve the network administrator from the cumbersome task of configuring each link. The administrator needs only submit a GANA Profile (Figure 2) containing the desired performance policy. This policy is translated by the Network Level DP&F Management DE into instructions (e.g., containing the addressing scheme) sent to each Node Level Auto-Configuration DE (Table VII). This functional block controls the Function Level DP&F Management DE responsible for the configuring of the network interfaces. The end result is a complete wireless network setup providing a connectivity service for other stations.

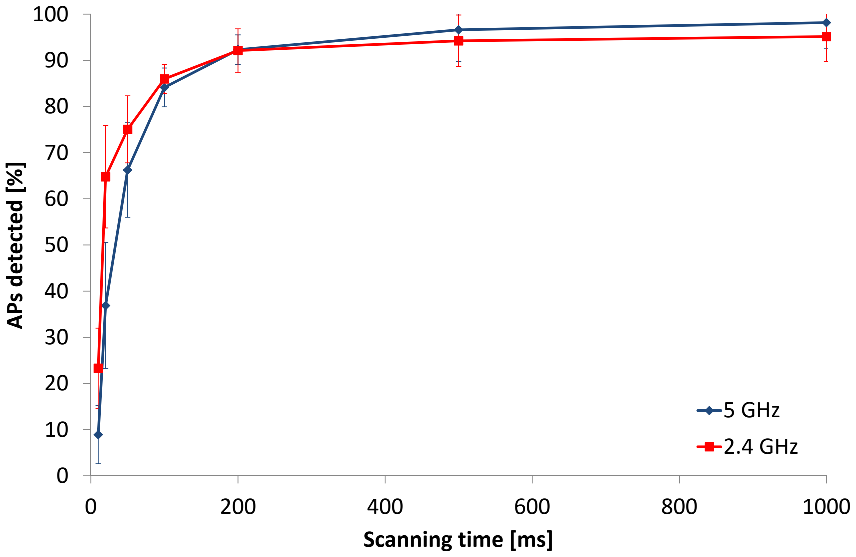


Figure 6. Percentage of all APs in the neighborhood being detected as a function of scanning time for the 2.4 GHz and 5 GHz bands

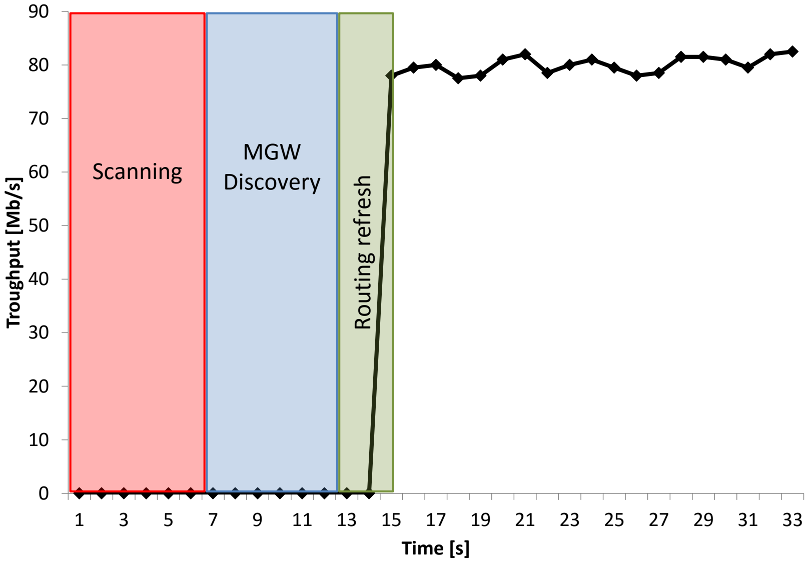


Figure 7. Throughput at MRN3 during the network bootstrap.

To illustrate how this process is done, we performed an experiment in which MGW2 (Figure 5) scans through a predefined set of radio channels (in the 2.4 and 5 GHz bands) in order to find the least utilized channel with the smallest number of discovered stations: min{number of stations, utilization}. The experiment covered a setup where four channels were scanned in the 5 GHz band (153, 157, 161, 165) and three orthogonal channels in 2.4 GHz band (1, 6, 11). The scanning time per each channel was preconfigured to last one second, however, it can be decreased to a shorter period with similar efficiency according to operator needs. Our results show that the scanning time interval should be at least 200 ms (Figure 6). The bootstrap of MGW2 finishes with a configuration of the wireless interface to operate on the selected channel.

After successfully finishing the self-configuration procedure at MGW2, MRN3 scans through a predefined set of radio channels in order to discover the best neighbor acting as the gateway to the core network. The goal of the scanning procedure is to discover the best neighbor in terms of the strongest received MGW signal level and highest SNR. Experimental results for this sub-test cover the scenario of searching for the already configured MGW2. Figure 7 provides a trace of the backhaul throughput available at MNR3 with an indication of the procedures involved in network bootstrap[¶]. Channel scanning is followed by MGW discovery. Then, after a brief period for network layer convergence, data transmission can commence.

The self-configuration process finishes when all MANs and MRNs obtain connectivity to an MGW (either directly or through MRNs). Once this initial network configuration of all MNs is complete, it becomes the responsibility of the self-optimization process to ensure the network's proper online operation.

5.3.2. Self-optimization The varying link capacity, caused by radio and traffic conditions, provides a case for autonomic routing optimization in WMNs. In this scenario we consider communication between MAN1 and MGW1. The mesh backbone enables a direct connection between these two nodes as well as two indirect paths: either through MRN2 or through MRN2 and MRN1 (Figure 5). Of course, the direct path provides the smallest delay and consumes the least amount of energy, however, in case of its performance degradation there may be a reason to use alternatives. The operator can define also other performance indicators, which, appropriately weighted, may compose a complex objective function to support decisions regarding route selection. These indicators are periodically measured by Monitoring MEs managed by their respective Monitoring DEs at the Node and Network GANA levels. The measurement results are provided to the Routing Management DE, where appropriate algorithms process the data and reconfigure network elements (in this case, the Routing Protocol ME) appropriately (Table VIII). Thus, the network performance policy (as part of the GANA Profile) is implemented by the objective function including indicators from both Network- and Node-level Monitoring DEs.

To illustrate this issue, we implemented a scenario assuming the objective of throughput maximization. Since three paths are available between MAN1 and MGW1, during the test, the best links were consecutively degraded. First, the one-hop throughput became worse than the two-hop throughput, then the two-hop throughput decreased below the three-hop throughput. The presented scenario enables dynamic compensation of varying conditions in the radio environment caused by moving obstacles or interference. The route reconfiguration was introduced after a certain delay ΔT to protect the self-optimization mechanism against reaction to a temporary fluctuation and generation of unwanted signaling overhead traffic.

Figure 8 shows the throughput trace measured during the test and the switching points. Depending on the ΔT value we can observe in Figure 9 different mean throughput values as well as a gain obtained from applied self-optimization scheme for this example case. The gain was calculated as the relation of mean throughput values measured for the case with and without route reconfiguration.

This scenario partially represents also a case of the self-healing mechanism. When the link degradation is such that it indicates link failure, then the ability to reroute packets on-the-fly enables maintaining communication in the network. This becomes the trigger for the self-healing mechanisms to react.

5.3.3. Self-healing The quality of a radio link varies with time. Since the mesh backbone radio links are critical for the network operation, autonomic (self-healing) procedures are required to be triggered when the quality of a link degrades substantially. In GANA, link quality degradation is indicated by the Monitoring DE to the Node Level Fault Management DE, which initiates procedures controlled by the Network Level DP&F Management DE according to the administrator policies set in the GANA Profile. These procedures initiate the Function Level DP&F Management

[¶] The link in question used 802.11n with 2x2 MIMO and a 40 MHz channel which explains the higher throughput values in comparison to other results, where 802.11a was used.

DOI: 10.1002/nem

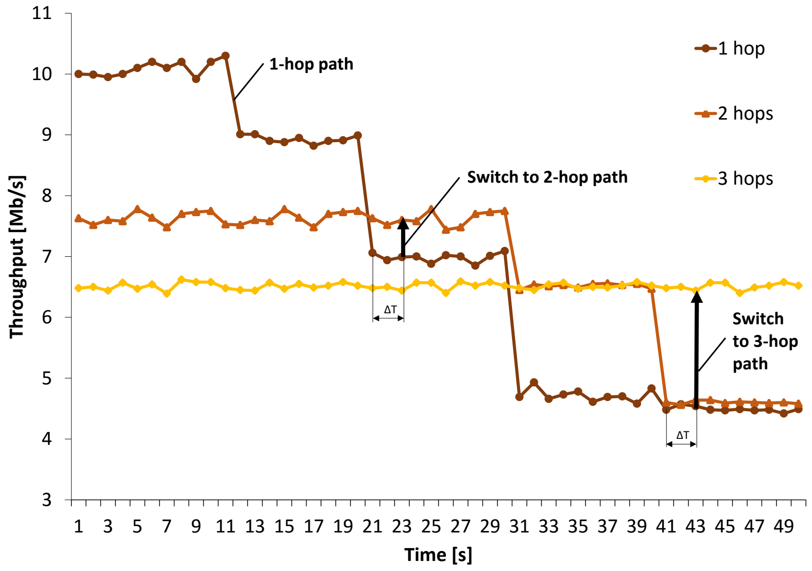


Figure 8. Throughput trace measured during the self-optimization experiment with points indicating route reconfiguration

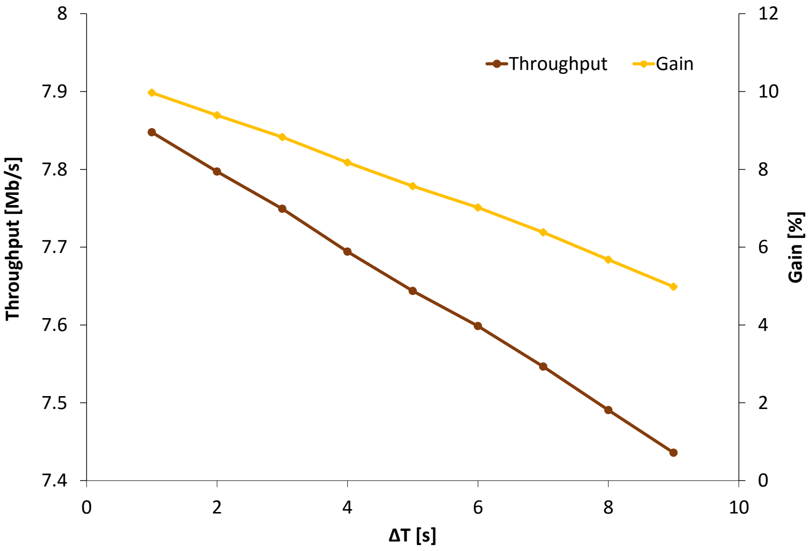


Figure 9. Mean throughput values achieved during the self-optimization experiment as well as the gain obtained from route reconfiguration as a function of ΔT

Table VIII. GANA self-optimization elements involved in the route reconfiguration example

GANA Level	GANA Element
Network	Routing Management DE
Node	Auto-configuration DE
Function	Routing Management DE
Protocol	Routing Protocol ME

Table IX. GANA self-healing elements involved in the link outage example

GANA Level	**GANA Element**
Network	DP&F Management DE
Node	Fault Management DE
Function	DP&F Management DE
Protocol	Interface ME

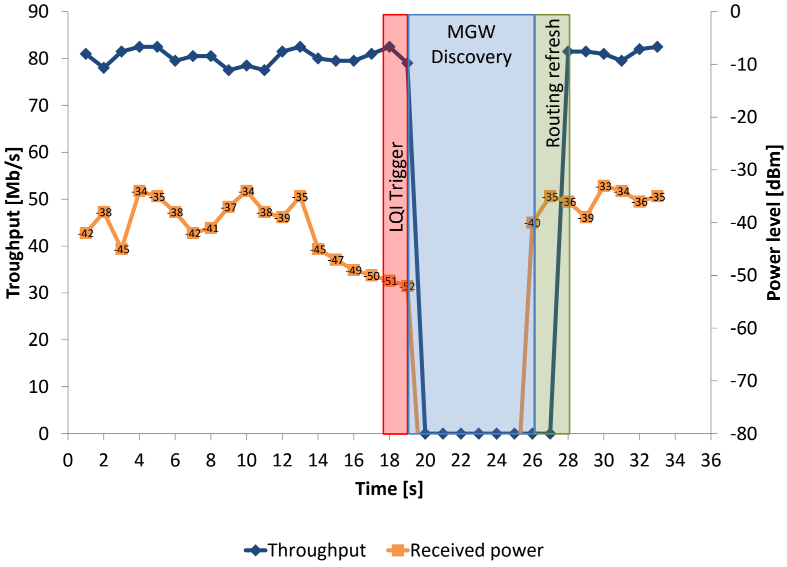


Figure 10. An example of self-healing: throughput and received power level at MRN during reconfiguration caused by link outage

DE (similarly to the self-configuration example), which results in a reconfiguration of the wireless interface (Table IX).

Link quality degradation can be triggered with the Link Quality Indicator (LQI) or the Link Failure (LF) alert [47]. The required reaction for these triggers leads to the selection of a new radio channel to operate on. The only difference is the trigger nature which initiates the procedure of the wireless interface channel reconfiguration. In case of LF the trigger is related to the link inactivity time, and generally should be predefined. It can be set to a predefined value (e.g., 5 seconds) after which the link is considered as failed and the process of neighbor discovery should be initiated once again, exactly in the way as it was described in the previous subsection related to self-configuration. The LQI considers a change of radio parameters, which can lead to poor link performance or even finally result with an LF.

In our considered case of link quality degradation (Network F in Figure 5), the MGW and MRNs should reconfigure their wireless interfaces in order to operate on a radio channel which offers better performance. Based on the scanning procedure results, the channel reconfiguration should be done so as to select one which is less occupied. Our experiment was based on the assumption that the target radio channel is already known and the whole process is limited just to convey a reconfiguration message from the MGW to the MRNs with the desired channel number, and acknowledge from both MRNs of channel reconfiguration. In the example presented in Figure 10, the measured overall time of channel reconfiguration between MGW and MRNs took about 10 seconds. The procedure was initiated when the received power level detected at the MRN side dropped below a preset threshold of -50 dBm of received power for a period of

DOI: 10.1002/nem

1 second. Afterwards, a new MGW discovery phase was required, followed by having the routing protocol establish new paths. The link was again operational after the completion of the self-healing procedure.

The described prediction process has been analyzed in [47]. Performed experiments showed that prediction requires raw data smoothing pre-phase which aims to reduce the fluctuations of the raw signal values and also helps to convert the time series data into a data set with fewer fluctuations. This also helps prevent unnecessary triggers, making the LQI more reliable.

Table X. GANA self-protection elements involved in the selfish attack example

GANA Level	GANA Element
Network	Security Management DE
Node	Security Management DE
Function	DP&F Management DE
Protocol	Traffic Control ME

5.3.4. Self-protection The goal of the self-protection functionality is to ensure that security policies set by the administrator are executed automatically. The GANA-enabled WMN needs to be able to detect and respond to any security threat. This requires the cooperation of the GANA elements listed in Table X.

An example of a security threat relevant to WMNs is that of selfish attacks. Selfish attacks are performed by insiders – stations that have already been authenticated and are a legitimate part of the network, with a goal of directly or indirectly increasing their quality of service (QoS) by abusing network mechanisms [48]. We anticipate these attacks to occur at the edge of the mesh network (Figure 5), where Station 1 accessing the WMN may be controlled by a selfish user. The WMN monitors station behavior and responds accordingly at MAN1, through which the station accesses the network. The operation of the particular GANA elements involved in the self-protection scenario is as follows. The Net-Level Security Management DE operates according to the security policy contained within the GANA Profile. This security policy is translated into instructions provided to the Node-Level Security Management DE operating at the MANs. Measurement metrics are inferred from these instructions and requested from the Monitoring DE. This function level DE performs statistical analysis on the data trace provided by the Monitoring DE and passes the results to the Node-Level Security Management DE. The node level DE decides if the security policy has been breached and what countermeasures to undertake. These countermeasures can then be executed, depending on their nature, e.g., by the Data Plane & Forwarding Management DE (as in the case of the traffic policing described below).

As an example of a selfish attack we consider a backoff attack. It belongs to the medium access parameter manipulation class of selfish attacks. In the case of the backoff attack, the selfish station deliberately changes the CWmin/max values. This attack increases a station's medium access probability and, hence, may increase its QoS. Such attacks have been well studied in the literature, although mostly for single-hop networks [48]. In mesh topologies, the impact of this attack is limited to the first hop (the selfish attacker being the sender with modified parameters). Nonetheless, Figure 11 shows that after enabling the attack at $t = 40$ s, the attacker's average throughput increases. As a reaction to this attack, we have configured MAN1 to apply a traffic shaping policy to stations violating the medium access rules. To visualize the effect of the traffic shaping policy, its enforcement was delayed until $t = 70$ s. Afterwards, the attacker's throughput dropped to below pre-attack levels. Obviously, the goal of this example is not to study the performance of the attack detection and reaction methods, but rather to show how security policy enforcement can be automated adopting the GANA architecture to achieve self-protecting WMNs.

DOI: 10.1002/nem

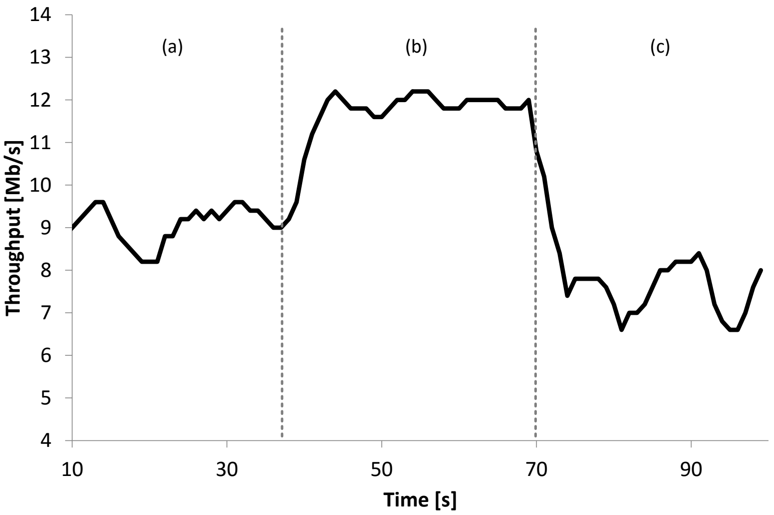


Figure 11. Station throughput change in the self-protection scenario: (a) during normal operation, (b) during the attack, (c) after the reaction policy (traffic shaping) is applied

6. SUMMARY AND FUTURE WORK

The need for applying autonomic networking principles to WMNs has been apparent from their inception. However, the lack of a unified approach has hindered the adoption of independently developed solutions. To solve this gap, the ETSI AFI group is working on an autonomic wireless mesh architecture, which is an instantiation of the AFI GANA Reference Model for WMNs. The objective of this reference model is to provide a well-structured standardization of the self-x, autonomic management, and cognitive networking concepts.

The guidelines presented in this paper show how to create an autonomic WMN with the instantiated GANA building blocks. In particular, we have presented mesh-specific DEs (the basic components and place-holders for control loops for any DE vendor/developer to innovate their own DE algorithms), the reference points between them (important for the cooperation of independently designed and implemented DEs), as well as the organization of the KP in a WMN. As a proof of concept we showed results of several experiments, in which example implementations of autonomic features for WMN were tested. Based on the considerations and experiments we can see the potential for the development and integration of self-x functionalities. We hope this architecture will improve interoperability by helping mesh network designers adequately place the required control-loops and understand their hierarchy. Furthermore, we encourage the mesh networking community (protocol designers, chipset manufacturers, equipment vendors) to contribute by mapping their own work to the presented architecture in order to elaborate on characteristics, data models, and other implementation-oriented details, so that the multitude of self-management efforts can be converged.

Within the ETSI NTECH AFI WG we are currently working on the precise definitions of the reference points as well as the integration of WMNs with existing management systems. Furthermore, we plan to demonstrate how the proposed architecture can be extended onto other radio technologies in order to provide full support for autonomicity in heterogeneous wireless mesh networks. The outcome of this work will be published as an ETSI Technical Specification and serve as a guideline for researchers and engineers implementing autonomicity in wireless mesh networks.

ACKNOWLEDGEMENT

This work was partially supported by the Polish National Science Centre (decision no. DEC-2011/01/D/ST7/05166).

REFERENCES

1. ETSI GS AFI 002: Generic Autonomic Network Architecture (An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management) April 2013. URL `http://www.etsi.org/deliver/etsi_gs/AFI/001_099/002/01.01.01_60/gs_afi002v010101p.pdf`.
2. ETSI White Paper No. 16: GANA Generic Autonomic Networking Architecture Reference Model for Autonomic Networking, Cognitive Networking and Self-Management of Networks and Services. (published in October 2016). URL `http://www.etsi.org/images/files/ETSIWhitePapers/etsi_wp16_gana_Ed1_20161011.pdf`.
3. Chaparadza R, Jokikyyny T, Ladid L, Ding J, Prakash A, Soulhi S. The diverse stakeholder roles to involve in standardization of emerging and future self-managing networks. *GLOBECOM Workshops*, 2011, doi:10.1109/GLOCOMW.2011.6162522.
4. Szott S, Wodczak M, Chaparadza R, Meriem TB, Tsagkaris K, Kousaridas A, Radier B, Mihailovic A, Natkaniec M, Loziak K, *et al.*. Standardization of an autonomicity-enabled mesh architecture framework, from ETSI-AFI group perspective (2 part paper). *Proc. of IEEE Globecom Workshops: International Workshop on Management of Emerging Networks and Services (MENS) Workshop*, 2012.
5. Wódczak M, Meriem TB, Chaparadza R, Quinn K, Lee B, Ciavaglia L, Tsagkaris K, Szott S, Zafeiropoulos A, Radier B, *et al.*. Standardising a Reference Model and Autonomic Network Architectures for the Self-managing Future Internet. *IEEE Network* 2011; **25**:50–56.
6. Simon C, Chaparadza R, Benko and P, Asztalos D, Kaldanis V. Enabling autonomicity in the future networks. *GLOBECOM Workshops (GC Wkshps), 2010 IEEE*, 2010, doi:10.1109/GLOCOMW.2010.5700398.
7. ETSI TR 103 404 on GANA instantiation onto the 3GPP Backhaul and Core (EPC) architectures for enabling autonomics and self-management in the 3GPP Backhaul and Core network. URL `http://www.etsi.org/deliver/etsi_tr/103400_103499/103404/01.01.01_60/tr_103404v010101p.pdf`.
8. ETSI Specialist Task Force STF 501 on Autonomic and Self-Managed Networks Phase 2 (BBF). URL `https://portal.etsi.org/stfs/ToR/ToR501v23_NTECH_AFI_Ph2_BBF.doc`.
9. Movahedi Z, Ayari M, Langar R, Pujolle G. A survey of autonomic network architectures and evaluation criteria. *Communications Surveys Tutorials, IEEE* 2012; **14**:464–490, doi:10.1109/SURV.2011.042711.00078.
10. Kosek-Szott K, Gozdecki J, Loziak K, Natkaniec M, Szott S, Wagrowski M. ViMeNO: A Virtual wireless mesh network architecture for operators. *Wireless Information Networks and Systems (WINSYS), 2013 International Conference on*, 2013.
11. Gallo P, Kosek-Szott K, Szott S, Tinnirello I. Sdn@home: A method for controlling future wireless home networks. *IEEE Communications Magazine* 2016; **54**(5):123–131, doi:10.1109/MCOM.2016.7470946.
12. Chaparadza R, Meriem TB, Lalande P. Industry Harmonization for Unified Standards on Autonomic Management & Control of Networks and Services, SDN, NFV, E2E Orchestration, and Software-oriented enablers for 5G. *Technical Report*, TMForum 2015. URL `http://projects.sigma-orionis.com/eciao/wp-content/uploads/2015/07/Report-on-Joint-SDOs-Industry-Harmonization-for-Unified-Standards-on-AMC_SDN_NFV_E2E-Orchestration_ver3.01.compressed.pdf`.
13. Aruba Networks. The next step in the evolution of wireless mesh networking. White Paper August 2010. Available: `http://www.arubanetworks.com/pdf/technology/whitepapers/wp_Evolution-Wireless-Mesh-Networking.pdf`.
14. Marina M, Das S, Subramanian A. A topology control approach for utilizing multiple channels in multi-radio wireless mesh networks. *Computer networks* 2010; **54**:241–256.
15. Skalli H, Ghosh S, Das S, Lenzini L, Conti M. Channel assignment strategies for multiradio wireless mesh networks: issues and solutions. *Communications Magazine, IEEE* 2007; **45**:86–95.
16. Ramachandran K, Belding E, Almeroth K, Buddhikot M. Interference-aware channel assignment in multi-radio wireless mesh networks. *Proc. of INFOCOM*, 2006.
17. Roy C, Dziong Z, Gregoire J. Fast multichannel switching for ieee 802.11s multiradio wireless mesh networks. *Prof. of GLOBECOM Workshops*, 2011, doi:10.1109/GLOCOMW.2011.6162458.
18. Zhang Y, Wang F, Li M. Research on Reliability Optimization Method for Mesh Network Communication Based on Node Congestion Degree. *Proc. of Computational Intelligence and Software Engineering (CiSE)*, 2010, doi:10.1109/CISE.2010.5676936.
19. Ancillotti E, Bruno R, Conti M. Load-balanced routing and gateway selection in wireless mesh networks: design, implementation and experimentation. *Proc. of WoWMoM*, 2010, doi:10.1109/WOWMOM.2010.5534991.
20. Kyasanur P, Vaidya N. Routing and interface assignment in multi-channel multi-interface wireless networks. *Proc. of WCNC*, 2005.
21. Paris S, Nita-Rotaru C, Martignon F, Capone A. EFW: A cross-layer metric for reliable routing in wireless mesh networks with selfish participants. *Proc. of INFOCOM*, 2011, doi:10.1109/INFCOM.2011.5935230.
22. Kim TS, Yang Y, Hou J, Krishnamurthy S. Joint resource allocation and admission control in wireless mesh networks. *Proc. of WiOPT 2009*, 2009, doi:10.1109/WIOPT.2009.5291636.
23. Li N, Hou J. Localized fault-tolerant topology control in wireless ad hoc networks. *Parallel and Distributed Systems, IEEE Transactions on* 2006; **17**:307–320.
24. Hamida E, Chelius G, Busson A, Fleury E. Neighbor discover y in multi-hop wireless networks: evaluation and dimensioning with interference considerations. *Discrete Mathematics and Theoretical Computer Science* 2008; **10**:87–14.
25. Abdelali D, Theoleyre F, Bachir A, Duda A. Neighbor discovery with activity monitoring in multichannel wireless mesh networks. *Proc. of WCNC*, 2010, doi:10.1109/WCNC.2010.5506146.
26. Egoh K, Rojas-Cessa R, Ansari N. Distributed diffusion-based mesh algorithm for distributed mesh construction in wireless ad hoc and sensor networks. *Proc. of ICC*, 2010, doi:10.1109/ICC.2010.5502670.

DOI: 10.1002/nem

27. Hakami S, Zaidi Z, Landfeldt B, Moors T. Detection and identification of anomalies in wireless mesh networks using principal component analysis (pca). *Proc. of I-SPAN*, 2008, doi:10.1109/I-SPAN.2008.14.
28. Hugelshofer F, Smith P, Hutchison D, Race NJ. OpenLIDS: a lightweight intrusion detection system for wireless mesh networks. *Proc. of MobiCom*, 2009, doi:10.1145/1614320.1614355.
29. Wang X, Wong J, Stanley F, Basu S. Cross-Layer Based Anomaly Detection in Wireless Mesh Networks. *Proc. of SAINT*, 2009, doi:10.1109/SAINT.2009.11.
30. Serrano P, Banchs A, Targon V, Kukielka J. Detecting selfish configurations in 802.11 WLANs. *Communications Letters, IEEE* 2010; **14**:142–144.
31. Raya M, Aad I, Hubaux JP, El Fawal A. DOMINO: Detecting MAC layer greedy behavior in IEEE 802.11 hotspots. *IEEE Transactions on Mobile Computing* 2006; **5**:1691–1705.
32. Szott S, Natkaniec M, Canonico R. Detecting backoff misbehaviour in IEEE 802.11 EDCA. *Wiley European Transactions on Telecommunications* 2011; **22**:31–34.
33. Cagalj M, Ganeriwal S, Aad I, Hubaux JP. On Selfish Behavior in CSMA/CA Networks. *Proc. of INFOCOM*, 2005.
34. Konorski J. A game-theoretic study of CSMA/CA under a backoff attack. *IEEE/ACM Transactions on Networking* 2006; **14**:1167–1178.
35. Szott S, Konorski J. A Game-Theoretic Approach to EDCA Remapping Attacks. *Proc. of International Conference on Wireless Communications, Networking and Mobile Computing (WiCom)*, 2012.
36. Szott S, Natkaniec M, Pach AR. Improving QoS and security in wireless ad hoc networks by mitigating the impact of selfish behaviors: a game-theoretic approach. *Security and Communication Networks* 2013; **6**(4):509–522, doi: 10.1002/sec.677.
37. Konorski J, Szott S. Discouraging traffic remapping attacks in local ad hoc networks. *Wireless Communications, IEEE Transactions on* 2014; **13**:3752–3767.
38. Naudts D, Bouckaert S, Bergs J, Schouttcet A, Blondia C, Moerman I, Demeester P. A Wireless Mesh Monitoring and Planning Tool for Emergency Services. *Proc. of E2EMON*, 2007, doi:10.1109/E2EMON.2007.375316.
39. Nanda S, Kotz D. Mesh-Mon: A multi-radio mesh monitoring and management system. *Computer Communications* 2008; **31**:1588–1601, doi:10.1016/j.comcom.2008.01.046.
40. Huang F, Yang Y, He L. A flow-based network monitoring framework for wireless mesh networks. *Wireless Communications, IEEE* 2007; **14**:48 –55, doi:10.1109/MWC.2007.4396942.
41. Zaidi ZR, Landfeldt B. Monitoring assisted robust routing in wireless mesh networks. *Proc. of Mobile Adhoc and Sensor Systems (MASS)*, 2007, doi:10.1109/MOBHOC.2007.4428724.
42. Kolar V, Razak S, Mahonen P, Abu-Ghazaleh N. Measurement and Analysis of Link Quality in Wireless Networks: An Application Perspective. *Proc. of INFOCOM*, 2010, doi:10.1109/INFCOMW.2010.5466673.
43. Clark DD, Partridge C, Ramming JC, Wroclawski JT. A knowledge plane for the internet. *Proc. of SIGCOMM*, 2003.
44. Quirolgico S, Mills K, Montgomery D. Deriving knowledge for the knowledge plane. *Technical Report*, National Institute of Standards and Technology Advanced Network Technologies Division Gaithersburg 2003.
45. Robitzsch S, Niephaus C, Fitzpatrick J, Kretschmer M. Measurements and evaluations for an ieee 802.11a based carrier-grade multi-radio wireless mesh network deployment. *Wireless and Mobile Communications, 2009. ICWMC '09. Fifth International Conference on*, 2009; 272–278, doi:10.1109/ICWMC.2009.52.
46. iperf – the network bandwidth measurement tool. URL `https://iperf.fr/`.
47. Chin E, Chieng D, Teh V, Natkaniec M, Loziak K, Gozdecki J. Wireless link prediction and triggering using modified Ornstein–Uhlenbeck jump diffusion process. *Wireless Networks* 2014; **20**:379–396, doi:10.1007/s11276-013-0610-0. URL `http://dx.doi.org/10.1007/s11276-013-0610-0`.
48. Szott S. Selfish insider attacks in IEEE 802.11s wireless mesh networks. *Communications Magazine, IEEE* 2014; **52**:227–233.