Towards the Future Internet
G. Tselentis et al. (Eds.)
IOS Press, 2009

doi:10.3233/978-1-60750-007-0-123

Towards a Future Internet: Node Collaboration for Autonomic Communication

Tanja Zseby, Thomas Hirsch, Michael Kleis, and Radu Popescu-Zeletin

Fraunhofer FOKUS, Berlin, Germany
{tanja.zseby, thomas.hirsch, michael.kleis,
radu.popescu-zeletin}@fokus.fraunhofer.de

Keywords: Future Internet, Situation Awareness, Collaboration Strategies

Abstract. The Internet today is a complex agglomerate of protocols that inherits the grown legacies of decades of patchwork solutions. Network management costs explode. Security problems are more pressing than ever, as organized crime discovers its value. The application and user demands on the Internet are increasing with mobile technologies and media content on the rise, all the while the number of participating nodes is equally boosting. As a direct consequence the recently triggered research on concepts for the future Internet has to cope with a high complexity at network layer and significance in mission critical service infrastructures of society. As part of this effort, the research field of autonomic communication (AC) aims at network self-management and self-protection, following the autonomic computing paradigm invented by IBM. We argue that the collaboration of network nodes provides a valuable way to address the corresponding challenges. After an in-depth analysis of the problem space, we outline in this paper the advantages and challenges of collaboration strategies in deployment. We present the Node Collaboration System (NCS) developed at Fraunhofer FOKUS for the experimental investigation of collaboration strategies and show how the system can be used in a simple setting for network self-protection.

1 Introduction

When the Internet was designed, application requirements were low compared to today's standards. Mobility of network components was no issue and neighbor nodes were assumed trustworthy.

The world has changed. Nowadays, many communities and businesses rely on the Internet and demand mobility, quality of service, authorization, accounting and more to support application demands. Moreover, criminals control large parts of the Internet. A wide variety of attacks on network nodes, servers and end systems endanger the operation of components at their will and urgently call for secure solutions. Complexity and significance of critical networks let the costs for network administration explode.

Although the Internet Protocol (IP) is still the common denominator for communication in the Internet, we observe a growing patchwork of protocols deployed to serve

the needs of the increasing number of applications and different underlying communication technology. About 120 working groups within the Internet Engineering Task Force (IETF) standardize protocol after protocol to fulfill those demands. IP is still the dominant protocol but only on the networking layer for the data plane. Already on transport layer heterogeneity is growing. UDP and TCP used to be prevalent. But new protocols like the Stream Control Transmission Protocol (SCTP) and the Datagram Congestion Control Protocol (DCCP), that mix desired properties of both protocols, gain significance. Furthermore many adaptations to TCP have been proposed to address TCP problems in fixed networks and wireless environments.

On the control plane, complexity is even larger. A wide variety of control protocols to support IP (ICMP, ARP, DHCP, etc.), to provide routing (BGP, OSPF, ad hoc and multicast routing, etc.), QoS (RSVP, DiffServ) and security features (SSL, TLS, AAA) is required to operate today's Internet.

The new IP version IPv6 has been defined to cope with several problems of IPv4, most notably with the upcoming IP address shortage. However, due to the difficulties of migration and legacy support of IPv4, providers and users are switching but slowly to the new technology, and huge efforts are needed to organize co-existence of IPv4 and IPv6.

Future problems can be foreseen: Embedded devices in household and daily life applications become Internet aware. The representation of critical networks in telecommunication, health and government onto IP networks progresses quickly. Worldwide Internet connectivity is increasing and the considerations on green IT have imposed new requirements.

Future Internet initiatives address current problems and future demands of the worldwide network. Approaches span from evolutionary proposals, that target incremental changes to the existing Internet, to revolutionary ideas that plan to design a new Internet from scratch, a process dubbed clean slate design. In this paper we provide a short overview of currently proposed solutions for the future Internet. We argue that the immense administrative costs and the demands for security present the most challenging issues in future networks. We focus on the research field of autonomic communication, which provides a framework to realize self-management and self-protection of network components. Our contribution is the investigation of collaboration strategies to improve such techniques. We introduce and compare different collaboration strategies and show with an example how collaboration helps to realize self-protection.

2 Future Internet Trends

Future Internet research is supported by several programs in Europe, US and Asia. In the US research on future Internet and the provisioning of facilities for large scale experiments is funded by the Global Environment for Network Innovations (GENI) and the Future Internet Design (FIND) program.

The European Union also funds several projects on future Internet research and has recently started projects for the establishment of federated testdbeds to support experimental research, such as Onelab [1] and PanLab [2]. Several governments support such activities with national funding. In Japan and Korea similar activities can be ob-

served (e.g., AKARI in Japan [3], Future Internet Forum in Korea [4]). The common differentiation between revolutionary and evolutionary paradigms is followed in these programs.

Inspired by IBMs autonomic computing paradigm [5] Fraunhofer FOKUS started in March 2004 an initiative to establish a new research field called autonomic communication as basis for enabling self-properties like self-management and self-protection in future communication networks [6]. Under the lead of Fraunhofer FOKUS a consortium of partners from industry and academia founded the Autonomic Communication Forum (ACF). Now the ACF has become a standardization body that standardizes the theoretic foundations of autonomic communication [7].

In 2005 the EU started a research program on Situated and Autonomic Communication (SAC) to bring forward research in the area. In 2006 four integrated projects started under this program. Although the goals were quite ambiguous and aimed at organizing communication networks with absolutely new paradigms, today results of these projects have not only materialized in sophisticated concepts in paperwork but also in running code. In July 2008 the first public release of the Autonomic Networking Architecture core (ANAcore) has been released. The ANAcore substitutes the traditional fixed protocol stack with flexible functional blocks that are concatenated by the network on demand to serve various application needs in a highly heterogeneous underlying network. The concept used in the ANAcore is called ***functional composition.***

An approach to share resources in the future Internet between applications and user groups with different requirements is the concept of ***network virtualization***. Virtualization concepts are already used in operating systems to share resources among different tasks. Network virtualization can be seen as a radical advancement of the concept of overlay networks. Overlay networks nowadays already allow to build application- or community-specific structures on top of the current Internet. Virtualization tries to bring this idea further down into the network and generate separated networks by assigning network resources in routers and lines to slices for applications or user groups. With this each of the separate networks can serve the specific needs of the application or community. Virtualization was also proposed as solution to share resources for large scale experiments in distributed testbeds. GENI is following this approach for experimental research. The main challenge for virtualization is the management and conflict-free assignment of resources to different groups. Both, functional composition and virtualization require decision-making based on application demands and current network situation. For this we see Situation Awareness and collaboration strategies as essential building blocks. Other approaches have been motivated by the inherent problem of addressing in the current Internet. Currently IP addresses are assigned to hosts. They serve as identifer and locator at the same time. This leads to problems especially in mobile environments and with multi-homing. The Host Identity Protocol (HIP) and the Locator Identifier Split Protocol (LISP) are evolutionary approaches to split locator and identifier. More radical approaches propose to go towards a ***Network of Information***. It is based on the idea that the main interest of users is to get access to information in the Internet. Therefore the proposal is to address information and services instead of hosts. Basic concepts for addressing information are already known for file sharing and content-delivery networks.

In the following, we focus on decision-cycles within the network required to achieve self-management and self-protection. We describe how to achieve Situation Awareness and use collaboration strategies to provide the mentioned self-properties. Where other future Internet approaches require decision-making, we show how concepts from Autonomic Communication may be adopted for the network protection and management of resources in such environments.

3 Situation Awareness

In this paper we use Situation Awareness to denote the process of perception of relevant conditions and events. Self- and context awareness are the perception of conditions within and surrounding the actor. In communication networks, Situation Awareness is a pre-requisite to make sound decisions; thus to establish autonomic communication principles. The situational view is the summary of all perceptible conditions and events. Situation Awareness is established on the one hand by observing and analyzing network node behavior and information flows in the direct neighborhood of an entity. On the other hand, collaboration is necessary to provide information on remote events. The situational view provides the basis to decide, based on the current state of the network. If perfect Situation Awareness is achieved, i.e. all important factors for the decision are known and processed with respect to the decision-makers goal, the decision is evident (see Fig. 1). Nevertheless, this ideal case is usually not achievable due to missing information, resource or time constraints. Usually it is necessary to make decisions without perfect Situation Awareness, i.e. with some degree of uncertainty about the situation, in order to invoke actions in time. Situation Awareness can be subdivided into three levels:

- ***Perception***: Build the situational view by collecting relevant information.
- ***Inference***: Understand the interplay of conditions, as well as other actors patterns and plans.
- ***Prediction***: Predict future events and actions.

Fig. 1. Context processing [29]

Implementing Situation Awareness is not a simple task. Network events are extremely dynamic and difficult to be perceived, interfered or predicted. Hence the view of the situation needs to be constantly updated. The utopistic ideal would be to gain a complete picture of the network, and be able to process it; Observe every packet, at every network node, and fully analyze it. Then we could perfectly direct the traffic to avoid congestion and detect even sophisticated application-level attacks. However, since this utopia requires at the very minimum equal processing powers as the rest of the network, we simply cannot measure everything everywhere.

We have to deal with resource limitations. Processing power, storage, transmission capacity and speed are limited. More dramatically, as network supervision is only a support function for network operation, they should not influence network performance at all. Their costs should not exceed costs for network operation itself. Moreover, the overwhelming amount of result data we could retrieve with specialized measurement hardware has to be processed. Resource limitations are grave in terms of transmission and processing power. They are even worse in wireless networks of small embedded devices and low bandwidth. We postulate the following requirements that a system should fulfill in order to establish Situation Awareness:

Cope with resource constraints The amount of data traffic carried by the Internet each day has increased dramatically over the last decades. A deceleration of this trend is not in sight. Technologies that allow higher data rates increase not just the amount of data that can be measured but also the quantity of measurement results needing to be processed, stored or transferred per time unit. Approaches to cope with resource constraints are the usage of dedicated hardware (e.g. [8], [9]), the improvement of algorithms for packet processing (e.g., [10], [11]) or the use of data selection techniques ([12], [13]).

Change viewpoints The ability to change viewpoints is extremely valuable for establishing Situation Awareness. In order to generate a good picture of the current situation, it is useful to have the option of zooming in or out. The capability to re-configure network observation tasks provides the basis for ***adaptive measurement*** techniques and is a pre-requisite for resource and accuracy control. Adaptive measurements can be used to tune towards events of interest by changing observation points, classification rules, or aggregation and selection techniques on demand (e.g., [14], [15]).

Respect privacy concerns The need to respect privacy concerns is often in contradiction with the desire to get as much information as possible. Privacy concerns need to be respected but they do constrain data collection and information sharing. Fraunhofer FOKUS investigates in privacy-aware monitoring methods in the EU project PRISM [16].

Cooperate to share information Sharing information is the prerequisite for learning from others. If one node observes strange or suspicious behavior it is useful to see whether other nodes have observed similar phenomena. If a node is infected by a virus or a worm that spreads within a network, it is worthwhile checking whether neighbor nodes or neighbor networks have experienced similar events in the past. If this is the case, information from neighbors can help to analyze the event, select appropriate countermeasures or nip it in the bud.

As a consequence of above considerations and described challenges we consider collaboration as one of the key enablers for Situation Awareness. Because of this fact we will describe different collaboration strategies in section 4. Since information sharing already is a form of collaboration we further elaborate on this in section 4.1. Fraunhofer FOKUS investigates methods for an efficient and flexible establishment of Situation Awareness in the EU project 4WARD [17].

4 Collaboration Strategies

Decision-making requires information on which the decision can be based. However, information in a distributed system cannot be gathered without consent. Hence, collaboration methods are required for information collection and decision-making.

Sharing resources is another benefit of collaboration. Finally, where information is provided by collaboration, privacy can be largely guaranteed by the information provider. We therefore argue that a participative information collection system is one way to handle the previously mentioned challenges.

But collaboration does not come for free. It requires a communication infrastructure, an incentive to cooperate, and means to trust the behavior of other nodes. A solution for collaboration for network protection should scale and is subject to timing requirements from the decision process. Further challenges include the processing of the information from multiple sources, resilience against involuntary inconsistencies and malicious communication, and reaching agreement and conclusive actions for joint decision making.

4.1 Collaboration for Information Sharing

The correlation of observations at multiple observation points in the network is essential to get a networkwide view and is further required to calculate network specific metrics as one-way delay or to gather information about internet routing. Existing tools face the challenges of clock synchronization, and the efficient correlation of packet events at different observation points (e.g.,[20], [21], [22]). A challenging combination of data selection techniques with multi-point measurements ensures that the same packet is selected at different points. Hash-based selection techniques are proposed in [21] and [13] that aim at an emulation of random sampling to apply statistical methods for accuracy assessment.

Several information sharing strategies help to improve a nodes Situation Awareness to support the decision process. In [23] a system is proposed where neighboring nodes may be searched for specific intrusion detection events. More general *Context information* helps to extend the network centric view. Such information covers data from different OSI Layers such as geo-location, user behavior or external events. Information from network services (e.g. DNS or AAA server) can further improve management and defense strategies [24]. For an example how to model context information we refer to [18].

To share information among network operators is a more difficult challenge. It can help to better identify bottlenecks to track the origin of a failure and to isolate the source

of the problem. It is extremely valuable for network protection since attack patterns can be learned from neighbors, and the path may be traced to the origin of the attack. But privacy and secrecy concerns make sharing of network data difficult. It can reveal information about network structure, users or vulnerabilities to competitors or potential attackers. Another collaboration is the delegation of analysis tasks that helps to make use of free resources, either centrally controlled or decentralized. Data analysis tasks may be shared between entities; strange and suspicious patterns can be forwarded to dedicated analysis components for further inspection. Commercial Intrusion Detection Systems, such as the Cisco Anomaly Detector, take a first step towards specialization of network components within a domain. In their system, anomalous traffic detected by the Anomaly Detector in the network is forwarded to a more specialized DDoS Mitigation component, the Cisco Guard [25]. Sharing information also requires standardized interfaces. In January 2008 the IETF standardized the IP Flow Information Export Protocol (IPFIX) [26] for exporting flow information from routers and network probes. This protocol can be also used for exporting packet information or derived data. In section 5.1 we will illustrate how we use this protocol for the FOKUS Node Collaboration System to share information with neighbor nodes.

5 Collaboration Principles for the Future Internet, a Case Study

This section presents prototypes of the awareness and collaboration approaches discussed in the previous sections. They serve as a research platform for the investigation of collaboration methods and constraints.

5.1 Node Collaboration System (NCS)

Fraunhofer FOKUS has developed a Node Collaboration System (NCS) for the investigation of collaboration strategies for self-management and self-protection. The establishment of Situation Awareness is supported by information sharing among nodes. The system for accessing arbitrary network context information is depicted in Fig. 2. Each node can serve as context provider and provides information to other nodes. Nodes cannot only offer information that they generated by local measurements but also information that they generated by processing of information from other sources. Information is modeled as abstract Context Data Objects. In order to make information accessible by other nodes, context providers register their available Context Data Objects with a directory.

The context providers indicate the context they can provide and the means to access it (e.g. push or pull model, protocols supported by the context provider, etc.). The actual information remains with the context provider. The directory only contains references to its location using Unique Context Identifiers (UCIs). The UCI of a context data object can be seen as simple strings, which offers similar functionality as Unique Resource Identifiers (URIs) in HTTP protocol. It is also possible to register information that does not yet exist, but may be generated by the context provider, for example by invoking local measurements or processing information from other context providers.

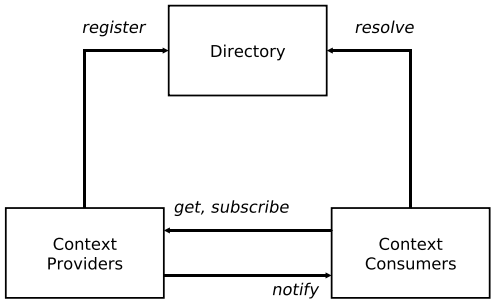

Fig. 2. Context management (picture taken from [28]) .

The decision-making process that needs to access information from other nodes acts as context consumer and can retrieve the context location and means to access the information with a request to the directory. Since the investigations on collaboration strategies for decision-making are our main focus and not the context distribution, we currently work with a centralized directory for simplicity. It is possible to later distribute the directory over multiple nodes using common name service algorithms.

We currently consider the following collaboration strategies for making joint decisions for network protection.

Election of a Leader In this approach the cooperative decision problem is on-demand reduced to a centralized case, but has the ability to flexibly assign who becomes this central node. For ad hoc networks the authors of [27] propose to combine clustering with a periodic leader re-election in each cluster. The actual monitoring is performed by the cluster members which propagate prefiltered monitoring results to the leader for analysis. If the cluster leader detects an intrusion it can coordinate the response.

Voting A less central approach are voting systems. For the case of sensor networks, [31] describes a voting system that can be realised without a priori knowledge about node behavior. Each sensor is able to observe its neighbors activities and defines majority sensor behavior as ”normal”, based on its local view. If one of its neighbors shows abnormal behavior, the observing sensor starts a voting process and presents evidence to its neigbors. Intruders are identified by a majority of responses.

Emergent Behavior The authors of [32] study an emergent behavior based collaborative information processing strategy to address the cooperative monitoring problem. Using a model of ants colonies, the actual monitoring results are translated into a pheromone concentration. Thus a path of intrusion in the sensor network can be identified by its pheromone concentration.

The means to transfer information from context provider to context consumer depend on the available transport methods at both entities. NCS provides a proprietary solution to provide efficient transport of context objects but also supports the transport of context objects by the IP flow information export protocol standard [26] if this is supported at the nodes. In this case the context provider acts as IPFIX exporter and the context con-

sumer as IPFIX collector. Integration with other commonly used protocols like SNMP is possible. Due to the flexibility of the IPFIX protocol it can be used without modifications. It is only necessary to add additional information elements for the required context objects.

Nodes can double as context consumer and provider. They may for instance take over pre-processing steps for a joint decision and report their local decision.

For the valuation of information a valuation library is provided. Valuation functions are running at each node that participates in the process. Valuation results are a specific form of local decisions and can be offered by a context provider as context objects. For the decision-making we are currently using policies expressed as list of rules. I next step we also consider to integrate DENng[19], which provides an information model enabling the design and the desired operation of an autonomic network and/or autonomic network elements. The model is positioned by the ACF and by the models chief architect, the ACF chair Prof. John Strassner as the major standardisation target of the ACF.

The collected valuations from other nodes can be weighted for instance based on by the capabilities, importance or history of the node (e.g. the ”opinion” of a AAA server may counts more than that of a new ad hoc node in the network). Then the decision-making process can use the valuations for instance in a voting process as shown below. It then generates a joint decision based on the local decisions of the majority. As shown above, other collaboration strategies are possible. The decision-making process then triggers the execution of the decision typically by invoking low level network functions (e.g. blocking or prioritization of traffic, re-routing, etc.).

5.2 D-CAF: collaboration for Self-protection

The theoretical aspects of collaboration described above are implemented in the FOKUS distributed context-aware firewall (D-CAF). It specifically makes use of the valuation library of the FOKUS Node Collaboration System. In the following we present a common Internet scenario and how it can be addressed by collaboration.

Protecting ones services and ones bandwidth against misuse is a difficult task. Today’s intrusion detection and prevention mechanisms are often insufficient, or restrictive for the legitimate users. This is due to two causes: First, it is virtually impossible to discern a malicious Denial of Service (DoS) attack from a sudden burst of legitimate users, a so-called flash crowd. Secondly, Intrusion Detection systems simply do not have the resources to analyze traffic with the same detail as the applications the traffic is addressed to. Thus, smart attacks may always slip past the defenses. To address these problems, we present D-CAF: a distributed context-aware firewall, which selectively limits the access to resources of the protected system by evaluating usage reports from protected services, and reacts accordingly.

The task of intrusion detection requires the analysis and classification of user behaviour on all protocol levels. Common state of the art Intrusion Detection Systems fail at this task, for the very same measurement challenges of complexity, amount of information, encryption and privacy. The alternative to monitoring the network therefore is, to profit from the collaboration of network services.

A web server is designed to parse HTTP data, to analyze user behaviour across network sites, and to detect positive and negative events, such as login attempts, system and database load, and processing of orders. It is therefore the right component to generate reports about user behaviour. In the D-CAF system, a lightweight library is available in several programming and web scripting languages. It allows to send a simple report of user identifier (IP address) and rating. It can be easily integrated in any existing application or website.

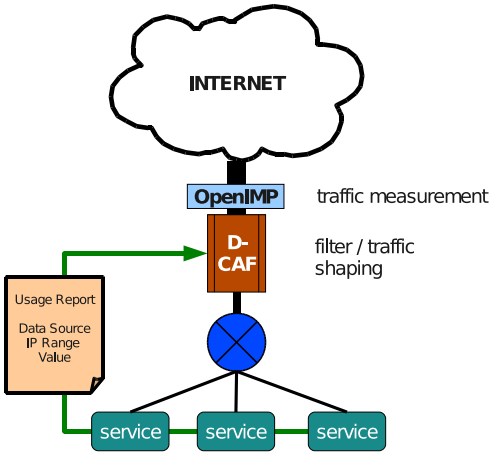

Fig. 3. D-CAF Information Flow.

In Fig. 3 we show the flow of information in the D-CAF firewall. The network is abstracted as such: A number of services is connected to the Internet via one link. On this link we place the FOKUS measurement platform OpenIMP [30] and the D-CAF system. The firewall receives information on the amount of observed traffic (total and per user) from the measurement system. In a first phase of normal operation, users connect from the Internet with our services as they normally would. This will generate positive and negative valuations of the users by the services, which we map to a numeric range of (-1;1). These ratings are transmitted to the D-CAF firewall.

During this phase, the information from all services is only collected, and weighted according to the importance and specialization of the services. The summary of ratings will provide the firewall with a differentiated valuation of all users which have used the services in the past. An example of such a summary is shown in Fig. 4. The chart displays the aggregated subjective value of each IP address for the services. Both single IP addresses or whole address ranges may be valued in the range (-1;1).

The next phase happens, when a DDoS attack is launched against one of the services protected by the firewall. This event is easily detectable by the surge of traffic reaching the service. We therefore define a simple traffic threshold which indicates whether the protected services is operating normally or whether it is about to be overloaded. The

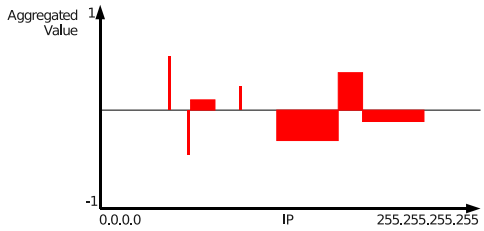

Fig. 4. D-CAF Usage Report.

firewall will take action, once the observed traffic reaches this threshold. If it is exceeded, it will begin to filter those users with the least favourable ranking. This filtering process continues until the remaining traffic is contained by the threshold. In Fig. 5, we exemplify the process: Given the previous ratings from Fig. 4 (bars) and the detected traffic per IP address(line), the algorithm can filter the worst rated IP addresses(blocks) and calculate an estimate of the traffic reduction thus attained.

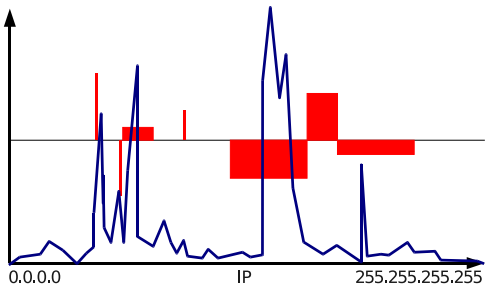

Fig. 5. Unfiltered traffic example.

The system thus reacts to attacks by prioritizing the users which have shown to behave correctly in the past - this would typically include paying customers and users with active accounts. Unknown users and systems which have disbehaved in the past are more prone to be filtered. Note that even though legal users may be filtered in the process, action is only taken when the system is overloaded. No action would imply the breakdown of the service for all users. After a pre-defined time the filter rules will be removed to be able to react to changing traffic patterns.

Finally, the firewall is distributed, as its very simple valuation semantics allow it to exchange information about the IP addresses with other similar firewalls. A complete snapshot of all the valuations in one firewall can be sent to other D-CAF instances in the same or remote networks. This is then again considered to be a subjective report from a specialized application.

6 Conclusion

We surveyed approaches to handle the challenges of the future Internet and point out the demand for self-management and self-protection. We show that current and expected future complexity of networking leads to loss of measurability, due to the amount of information, its distribution and its protection by the owners. This resulting challenge can best be handled by facilitating collaboration strategies in the complex network. Collaboration leads to sharing of resources, sharing of information, and owner consent on protected data sharing. We identify the challenges in collaboration and decision making in a widely distributed group, and presented several collaboration strategies for various requirements. We present our Node Collaboration System (NCS) designed to investigate collaboration strategies for self-management and self-protection and show in an example implementation how the system can be used to achieve network self-protection by node collaboration. As part of future work we will evaluate different collaboration strategies by utilizing the FOKUS Node Collaboration System. Based on the requirements of future network scenarios the best performing schemes will be used to develop a platform for Information Sharing and Decision Making which serves as an enabler for Situation Aware Networking.

References

1. EU Project OneLab. http://www.one-lab.org
2. A. Gavras and H. Bruggemann and D. Witaszek. Pan European Laboratory for next generation networks and services, March 2006 Testbeds and Research Infrastructures for the Development of Networks and Communities, 2006. TRIDENTCOM 2006.
3. http://akari-project.nict.go.jp/eng/conceptdesign.htm
4. http://fif.kr/
5. IBM. An architectural blueprint for autonomic computing. white paper, IBM, 2006.
6. http://www.autonomic-communication.org/projects/acca/index.html
7. http://www.autonomic-communication-forum.org/
8. C. Fraleigh, C. Diot, B. Lyles, S. Moon, P. Owezarski, D. Papagiannaki, and F. Tobagi. Design and deployment of a passive monitoring infrastructure. *Lecture Notes in Computer Science*, 2170:556+, 2001.
9. L. Deri. nprobe: an open source netflow probe for gigabit networks. In *In Proc. of Terena TNC2003*, 2003.
10. G. Iannaccone, C. Diot, I. Graham, and N. McKeown. Monitoring very high speed links. In *ACM Internet Measurement Workshop*, 2001.
11. A. Kumar, J. Xu, J. Wang, O. Spatscheck, and L. Li. Space-code bloom filter for efficient per-flow traffic measurement. In *Infocom*, 2004.
12. N. Duffield. Sampling for passive internet measurement: A review. In *Statistical Science*, Volume 19, pp. 472–498, 2004.
13. T. Zseby, M. Molina, N. Duffield, S. Niccolini, and F. Raspall. Sampling and Filtering Techniques for IP Packet Selection RFC 5475, February 2009.
14. B.-Y. Choi, J. Park, and Z.-L. Zhang. Adaptive Random Sampling for Load Change Detection. *SIGMETRICS Perform. Eval. Rev.*, 30(1): pp. 272–273, 2002.
15. C. Estan, K. Keys, D. Moore, and G. Varghese. Building a Better NetFlow. In *SIGCOMM*, 2004.
16. EU Project PRISM. http://www.fp7-prism.eu/

17. EU Project 4WARD. http://www.4ward-project.eu/
18. J. Strassner, S. Samudrala,G. Cox,Y. Liu,M. Jiang,J. Zhang,S. v. Meer,M. Foghlu, and W. Donnelly. The Design of a New Context-Aware Policy Model for Autonomic Networking. In *Proceedings of the 2008 international Conference on Autonomic Computing*, 2008.
19. J. Strassner. Introduction to DENng for PanLab II. ACF, 2008-2009, tutorial given 21.01.2009 in Fraunhofer FOKUS.
20. I. D. Graham, S. F. Donnelly, S. Martin, J. Martens, and J. G. Cleary. Nonintrusive and accurate measurement of unidirectional delay and delay variation on the internet. In *INET*, 1998.
21. N. G. Duffield and M. Grossglauser. Trajectory sampling for direct traffic observation. In *SIGCOMM*, pp. 271–282, 2000.
22. T. Zseby, S. Zander, and G. Carle. Evaluation of building blocks for passive one-way-delay measurements. In *Proceedings of Passive and Active Measurement Workshop (PAM 2001)*, April 2001.
23. T. Gamer, M. Scharf, M. Schöller. Collaborative Anomaly-based Attack Detection. Proceedings of 2nd International Workshop on Self-Organizing Systems (IWSOS 2007), p. 280-287, Springer, English Lake District, Sep 2007.
24. T. Zseby, E. Boschi, N. Brownlee, and B. Claise. IP Flow Information Export (IPFIX) Applicability. RFC 5472, Feb. 2009.
25. http://www.cisco.com/en/US/products/ps6235/
26. B. Claise. Specification of the IP Flow Information Export (IPFIX) Protocol for the Exchange of IP Traffic Flow Information. RFC 5101 (Proposed IETF Standard), Jan 2008, Internet Engineering Task Force, http://www.ietf.org/rfc/rfc5101.txt.
27. Yi An Huang and Wenke Lee. A cooperative intrusion detection system for ad hoc networks. In *SASN '03: Proceedings of the 1st ACM workshop on Security of ad hoc and sensor networks*, pages 135–147, New York, NY, USA, 2003. ACM.
28. D. Witaszek, and J. Tiemann. Context Dissemination System: Requirements, Architecture and Ability to Support Measurement Results. *Technical Report TR-2008-0130*, Fraunhofer FOKUS.
29. J. Tiemann, and D. Witaszek. Context Coordination and Dissemination System - Architecture and Basic Implementation. *Technical Report TR-2008-0303*, Fraunhofer FOKUS.
30. M. Lutz. http://www.ip-measurement.org/openimp/index.html
31. Fang Liu, Xiuzhen Cheng, and Dechang Chen. Insider attacker detection in wireless sensor networks. *INFOCOM 2007. 26th IEEE International Conference on Computer Communications. IEEE*, pages 1937–1945, 6-12 May 2007.
32. Soumya Banerjee, Crina Grosan, Ajith Abraham and P.K. Mahanti. Intrusion Detection on Sensor Networks Using Emotional Ants. IN *International Journal of Applied Science and Computations*, USA, Vol.12, No.3, pp.152-173, 2005.