Universidade Federal do Paraná

Departamento de Informática

Michele Nogueira Lima
Aldri Luiz dos Santos
Guy Pujolle

Biologically Inspired Architecture for Survivable Self-Organizing Wireless Networks

Relatório Técnico
RT-DINF 003/2010

Curitiba, PR
2010

Resumo

This work presents a survivable architecture for wireless self-organized networks inspired on the human body immune system. This architecture, called SAMNAR, focuses on providing network essential services, as link-layer connectivity, routing and end-to-end communication, even in the presence of attacks or intrusions. It employs a new approach for security management consisting in the coordinated use of preventive, reactive and tolerant defense lines in an adaptive way. The main goal lies in creating levels of obstacles for attacks and intrusions, and adapting them when necessary. SAMNAR comprises survival, communication and collect modules. Based on SAMNAR, we design a framework for security and performance management towards survivability in mesh networks. The framework owns different functional blocks, and for each one of them we highlight research directions in order to guide future works on our framework development.

1 Introduction

Self-organizing wireless networks, as ad hoc, mesh and sensor networks, request simultaneously high level of reliability, availability and security. These networks have increased the dependence of people on applications available on portable devices and supported by wireless communication. Mobile applications, such as those on commercial, financial and medical fields, mandate a predictable and acceptable network operation, guaranteeing data integrity, confidentiality and non-repudiation. Hence, self-organizing wireless networks must be *survivable* to attack and intrusion events. *Survivability* means the network capability of maintaining its essential services, as link-layer connectivity, routing and end-to-end communication, even under faults, attacks or intrusions [1].

Security is a challenge for self-organizing wireless networks. Several threats take advantage of protocol faults and vulnerabilities on operating systems of devices, as well as network characteristics. These networks are supported by shared wireless medium, highly dynamic network topology, multi-hop communication and low physical protection of portable devices [2]. These characteristics make self-organizing wireless networks prone to interferences, interruptions and misbehaviors, compromising easily network services.

Different security solutions have been proposed in the literature [2–4]. They apply preventive, reactive and tolerant security mechanisms. However, these mechanisms are not enough to put all attacks and intrusions off when applied separately. Preventive solutions attempt to thwart attacks by cryptography, authentication and access control mechanisms. They are vulnerable to malicious nodes that already participate in network operations. Reactive solutions, such as intrusion detection systems or reputations systems, seek to detect intrusions and react accordingly [5]. These solutions work efficiently only against well-known attacks or intrusions. Tolerant solutions focus on mitigating the impact of attacks using fault-tolerant techniques, typically redundancy and recovery mechanisms. However, these solutions remain still focused on one specific issue or particular layer of the protocol stack, being ineffective to ensure essential services.

In this article we address the problem of providing survivability in self-organizing wireless networks. We present SAMNAR, a conceptual architecture to maintain the operation of essential network services on an acceptable level even in face of faults, attacks or intrusions. The SAMNAR architecture is inspired on the human body immune system and proposes a new approach to security management. SAMNAR employs preventive, reactive and tolerant defense lines and manages them in a cooperative and adaptive way. SAMNAR also considers information from the environment and from

different layers of the protocol stack to take accurate decisions. We develop a security and performance framework based on the SAMNAR architecture. Next, we present research directions and open issues that can be considered on future works.

2 Survivable Architectures

In these last few years, research interests in survivability have increased. Initially addressed by military area, the first survivability architectures have been proposed in order to improve both security and dependability of information systems, distributed services and storage systems in the Internet domain [6–8]. Although the importance of all architectures in the survivability development, we emphasize Willow [8], SITAR [7] and SABER [6] architectures due to their completeness in terms of survivability properties.

The Willow architecture [8] is designed to enhance the survivability of critical information systems. This architecture proposes the merging of different mechanisms aiming to avoid, eliminate and tolerate faults. All of these mechanisms are based on a reconfiguration approach in which nodes of the network can together monitor and respond to faults. Each node and network operations are monitored continuously. However, the analysis of their operation is performed by central nodes, called servers, restricting the efficiency of the architecture.

SITAR [7] is a survivable architecture for distributed services whose goal is to provide the minimal level of services despite the presence of attacks. This architecture comprises different components such as proxy servers, monitors, audit control module and adaptive regeneration module. These components are transparent for the clients and servers of the service and each component has a backup in order to guarantee its operation. The architecture controls all requests and responses, and can be centralized or partially distributed.

The SABER architecture [6] integrates also different mechanisms to improve the survivability of Internet services. SABER proposes a multi-layer approach in order to block, evade and react to a variety of attacks in an automated and coordinated fashion. The SABER architecture is composed of a Denial of Service (DoS) resistant module, an Intrusion Detection System (IDS), a migration process and an automated soft-patching system. All of these components are controlled by an infrastructure of coordination. This infrastructure provides the communication and correlation among the components in a decentralized fashion.

Albeit various survivable architectures exist, few of them were developed for self-organizing wireless networks. Aura and Maki [9], for example, pro-

posed a distributed architecture towards a survivable access control in ad hoc networks. The survivability is achieved creating secure groups of nodes, managing their membership and proving group membership. Operations of security are based on public key certificates, being all the architecture based on cryptography. Groups are formed to grant access rights to nodes. Then, the survivability of this scheme is reached by the existence of multiple groups and by their independence. If a group does not exist anymore, another group can execute access control operations. Despite authors claim to propose an architecture, the solution is a specific survivable scheme for access control, not presenting a set of rules, concepts or models. Moreover, we identified that only resistance and recovery survivability properties are reached by this scheme.

A survivable architecture for wireless sensor networks (WSNs) was proposed by Tipper *et. al* [10]. The architecture aims to provide critical services in spite of physical and network based security attacks, accidents or failures. However, the architecture is limited to identify a set of requirements related to security and survivability, such as energy efficiency, reliability, availability, integrity, confidentiality, and authentication.

3 Bio-inspired Principles

The immune system provides defenses for human body to overcome all types of microorganisms. Human body environment is composed of millions of tiny attackers (bacteria, toxins, pathogens, viruses) and the human body is constantly under the attack of these tiny organisms. The immune system comprises special cells, proteins, tissues and organs, aiming to defend human body against these microorganisms through a series of steps called the immune response.

The immune system presents three types of immunity as natural, active and passive. The natural immunity includes external barriers of the body, such as the skin and mucous membranes, working as the first line of defense. Usually, the skin **prevents** invasion by microorganisms unless it is damaged, for example, by an injury, insect bite, or burn.

Mucous membranes, such as the linings of the mouth and nose, are coated with secretions that overcome microorganisms. The mucous membranes of the eyes produce tears, which contain an enzyme that tackles bacteria and helps to protect the eyes from infection. The airways filter out particles presented in the air and breathed in. The walls of the passages in the nose and airways are coated with mucus. Microorganisms in the air become stuck to the mucus, which is coughed up or blown out of the nose. Mucus removal

is aided by the coordinated beating of tiny hairlike projections (cilia) that line the airways. The cilia sweep the mucus up the airways, away from the lungs. The digestive tract has a series of effective barriers, including stomach acid, pancreatic enzymes, bile, and intestinal secretions. The contractions of the intestine (peristalsis) and the normal shedding of cells lining the intestine help to **remove** harmful microorganisms.

If the first defense is broken, the body **reacts** with the active immunity represented particularly by white blood cells, or leukocytes. Two types of leukocytes exist, phagocytes and lymphocytes. Together, they **seek out** and **destroy** the microorganisms and substances that cause diseases. Phagocytes are cells that chew up invading organisms whereas lymphocytes allow the body to **remember**, **recognize** and **adapt** to previous invaders and help the body destroy them.

Passive immunity is in general provided by another source and it lasts for a short time until the body can make stronger their own defenses. This immunity provide **tolerance** for the body against microorganisms. For example, antibodies in a mother's breast milk provide an infant with temporary immunity to diseases that the mother has been exposed to. This can help to protect the infant against infection during the early years of childhood.

These defenses work cooperatively to maintain the human body alive. The immune system controls and manages the three defense lines stimulating each one when necessary. This perfect combination among defenses keeps our body protected against all threats, guaranteeing the individual survivability. An example is observed when a person dies, and then its immune system stops. Quickly, the body is attacked and damaged by microorganisms resulting in its deterioration.

4 Correlating Bio-inspired Principles and The Proposed Approach

Inspired by the immune system of the human body, we argue that network survivability can be reached by the cooperative and adaptive use of preventive, reactive and tolerant defense lines. Fig. 1 illustrates our survivable approach. It consists of different levels of obstacles, that must work together in an adaptive way, against attack and intrusion events.

The first obstacle is generated by preventive security mechanisms aiming to avoid any type of attack. Examples of these mechanisms are firewalls and cryptography. They block certain attacks, but naturally will be incapable of preventing others due to their limitations. Cryptography and firewall,

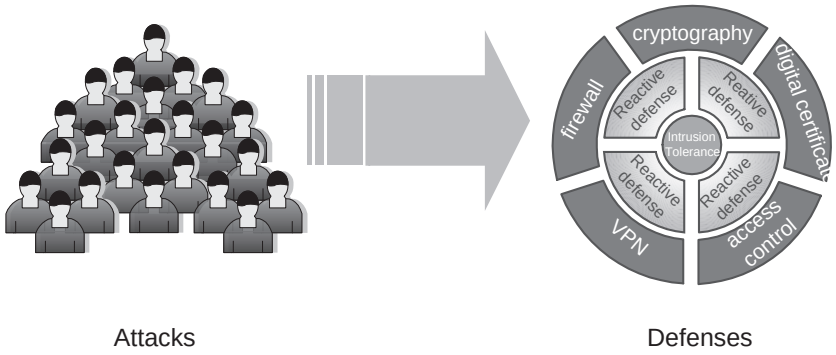

Figura 1: All defenses working together

for example, are vulnerable to attacks produced by nodes already legally participating in the network.

For some attacks succeeding to intrude into a node or network, reactive defenses will try to detect and react against them. Mechanisms such as intrusion detection systems or reputation systems intend to evaluate the behavior of nodes in the network. However, reactive defenses work efficiently against well-know intrusions, being vulnerable to unknown intrusions. IDSs, for example, require extensive evidence gathering and comprehensive analysis in order to detect intrusions based on anomalies or predetermined intrusion patterns.

Therefore, reactive defenses also present limitations. Some intruders can be successful in compromising the network. In order to guarantee the operation of essential services, intrusion tolerance techniques have been applied [10]. These techniques aim to mitigate intrusion effects, and stimulate preventive and reactive defenses to adapt against attacks or intrusions. Next section details the SAMNAR architecture that was designed considering this approach.

5 The SAMNAR Architecture

This section describes a survivable architecture for self-organizing wireless network called SAMNAR. Architectures include concepts, rules and models, in which rules describe how to use concepts, whereas models show the application of both rules and concepts. SAMNAR designs security management functions and guides the development of survivable protocols and services. Security management functions consist of controlling and monitoring security services and mechanisms, distributing security-relevant information, reporting security-relevant events, controlling the distribution of cryptographic

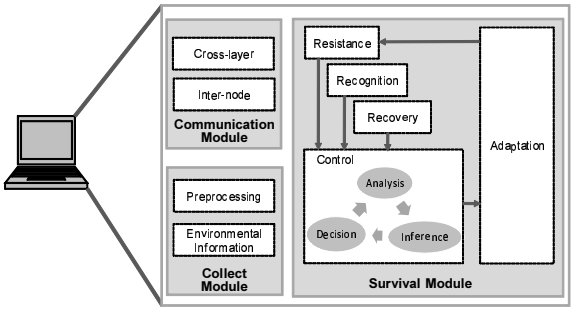

Figura 2: The architecture modules

keying material, and authorizing subscriber access, rights, and privileges.

The main objective of SAMNAR is to present a new approach for security management in order to make viable survivable self-organizing wireless networks. SAMNAR is inspired on the human body immune system in which different types of defenses cooperate adaptively. The architecture intends to offer prevention, reaction and mitigation of damages, as well as recovering of compromised services in a timely manner after the occurrence of intrusions. SAMNAR focuses on increasing the network capability of supporting essential services, as link-layer connectivity, routing and end-to-end communication, even in face of attacks and intrusions. Moreover, it proposes a cross-layer approach.

SAMNAR characteristics result from the requirements and properties of survivability. Thus, each node is responsible for reaching its survivability by the management of security mechanisms, following the bio-inspired approach presented in Section 4. Each node in the network is also self-managed meaning that no central entity in the network provides management functionalities.

The SAMNAR architecture is illustrated in Fig. 2. It is composed of three major modules named **survival**, **communication** and **collect**. The main module is the survival one employing our survivability approach, whereas communication and collect modules provide support for the first one. These modules are respectively detailed below.

5.1 The survival module

The **survival module** holds five independent components, being four of them related to the survivability properties, resistance, recovery, recognition and adaptability, and the control component. The properties represent respectively the network capability of repelling attacks; detecting attacks and evaluating the extent of damage; restoring disrupted information or func-

tionalities; and quickly incorporating lessons learned from failures and adapting to emerging threats.

The *resistance component* consists of preventive mechanisms such as firewall, access control, authentication and cryptography. This component works in a self-protection and self-adjusting fashion where preventive mechanisms and their configuration can be changed depending on the network or environmental conditions. The rule of a distributed firewall, for instance, can be more rigorous in certain environments, while simpler rules can be applied in more secure environments. Another example is the cryptographic key size that can be larger depending on the environment.

The *recognition component* is composed of reactive mechanisms to identify malicious behaviors, such as IDSs, reputation systems, anti-malwares and anti-spammers. Recognition mechanisms can also have the capability of reacting and stopping intrusions. All the mechanisms can be reconfigured if necessary by the adaptation component. New configurations as IDS rules will depend on the network and environmental conditions. This component provides to the control component information about detections, trustworthiness of neighbor devices, among others.

The *recovery component* consists of mechanisms to enhance the attack tolerance of network essential services. Mechanisms to restore disrupted information or functionality, such as replication or redundancy, have been employed as tolerant mechanisms. The application of two cryptography algorithms successively and the replication of message pieces are examples of redundancy. Sending redundant message pieces by different routes increases the probability of the message to be received by the destination node and the possibility of message recovery in case of piece losses. However, redundant strategies should consider resource limitations, as well as service and application requirements.

The *adaptation component* complements the previous ones. It is responsible for adapting preventive, reactive and tolerant mechanisms, as well as local or network configurations. It can replace a given protocol or a defense mechanism, such as changing a weaker cryptographic algorithm for a stronger one, depending on the necessities and requirements on time. Further, the adaptation component can change the key size of a cryptographic algorithm, the rules into an IDS or a firewall, the used route and others in accordance with the network condition or decisions taken by the control component.

The *control component* manages and coordinates all modules in the architecture. It receives information from communication and collect modules as well as from the resistance, recognition and recovery components. The control component correlates and analyzes all information in order to make inferences and take decisions. All decisions are sent to the adaptation com-

ponent that defines and sends satisfactory parameter values to other modules or components. Adaptation component learns with taken actions and later, it can take the same action if the node or network present a similar condition.

5.2 The communication module

The **communication module** is responsible by cross-layer and inter-node communications. The *inter-layer component* offers the exchange of information inter-layers. It supplies information from different network layers to control component so that it takes decisions based on all network layers and achieves the survivability for all of them.

The *inter-node component* provides communication, exchange and synchronization of information among the nodes aiming to guarantee the survivability of the whole network. Example of such information is the node configuration or network intrusion detections. Techniques for inter-node communication must consider the limitations and heterogeneity of the network resource capacities, such as memory, bandwidth and processing, and must be efficient in using these resources.

5.3 The collect module

The **collect module** holds mechanisms to gather all data required by the survival module. The collect module is composed of the *preprocessing component* and the *environmental information component*. The first one is exploited when gathered data need to be treated before sending to the survival module. Normalizations, previous calculations and others are examples of preprocessing used for facilitating analyses and inferences of the survival module. The second component stores information gathered periodically about the network conditions, sending it to the survival module when required.

6 Security and Performance Management Framework

Since SAMNAR is a conceptual architecture, we designed a more practical framework for security and performance management towards survivable wireless mesh networks (WMNs). They comprise two node types, mesh routers and mesh clients, communicating among them in a multi-hop way. WMNs present some advantages in relation to other networks, such as easy deployment, low cost of equipments and fast configuration. These networks

can be implemented using different wireless communication technologies including IEEE 802.11, IEEE 802.16, cellular technologies or a combination of them [5].

Fig. 3 illustrates the layout of our framework. A set of **management operations** runs on each node, interacting with networking functionalities directly, or through the node's databases or information stores. The **management entity** and **managed agents** execute management operations. The **management entity** represents an application running in the node for controlling the data collection, processing, analysis and decisions. Further, it controls **managed agents** that consist generally in a daemon running in background to effectively collect statistics, cooperate with other nodes, provide cross-layer communication and others. Two different settings are possible for placing management entities in the network. In the first setting, only mesh routers execute management entities whereas in the second setting both kinds of nodes execute them. The former results in a partially distributed organization of the framework, and the latter results in a fully distributed organization.

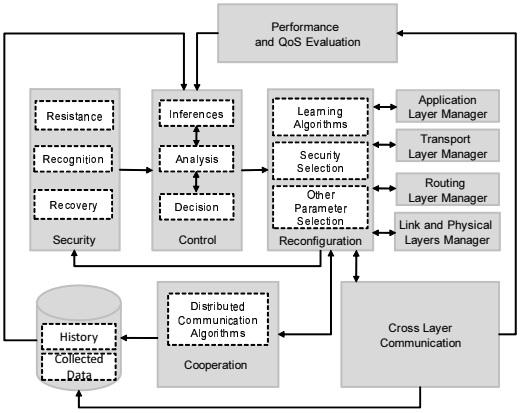

Figura 3: Framework for Security and Performance Management on WMNs

Our framework includes different functional blocks, representing management operations. We describe in this section each one of these blocks and we present research challenges related to each one of them.

6.1 The control block

The control block corresponds to the core of our framework comprising functions as the management of agents and the analysis of data, information

and statistics from the network. Other functional blocks supply evidences for analysis, inferences and decisions about the best configuration that the node should follow on specific network situation. Decisions consider security aspects as well as requirements of performance and Quality of Service (QoS). Further, realtime collected data or history of events, as logs, feed the control block intending to enhance decisions. The control block can employ different algorithms to analyze, infer and take decisions, such as those supported by probabilistic approachesand by artificial intelligence techniques (fuzzy logic, neural networks, swarm intelligence and others). The control block sends taken decisions to the reconfiguration block.

Research directions

Developing efficient mechanisms for analyzing, inferring and taking decisions is the main challenge for this functional block. Decisions must consider many kind of information, and they also request real time processing. In general, artificial intelligence techniques request high processing, being in contrast with portable devices characteristics. Hence, it is necessary to develop mechanisms that take efficient decisions and optimize the use of network resources. This consists in modifying artificial intelligence techniques to fit the characteristics of self-organizing wireless networks, including aspects related to resource limitations.

6.2 The reconfiguration block

The reconfiguration block aims to adapt security mechanisms and network layers towards survivability and based on the control block decisions. The reconfiguration block comprises of learning algorithms, a set of security mechanisms that can be employed, and a set of other parameters that can be chosen. The reconfiguration block defines how to adapt protocols, algorithms, network layers and security mechanisms following taken decisions. Since reconfigurations must be executed quickly, learning algorithms gain knowledge of previous decisions and actions, and then change faster the configuration of layers and security mechanisms. Changes include adjusts on parameter values as well as the replacement of protocols or even security mechanisms. Further, the reconfiguration block knows the set of security mechanisms that the node can employ as well as the set of options to change on network layers, such as possible routes to use, communication spectrum, channels and radios, routing protocols and others. Replacement of protocols, security mechanisms or channel, for instance, must require an agreement of other nodes in order

to keep the communication. This process must be performed by means of algorithms in the cooperation block.

Research directions

Defining how the self-reconfiguration of network nodes is worth. Choosing the best technique for node adaptation or learning algorithm is a first step to achieve this goal. In general, self-adaptive mechanisms must evaluate the global network behavior and change node configuration when the evaluation indicates that the network is not accomplishing what it was intended to do, or when better functionality or performance is possible. Solutions have applied multi-agent systems to self-adaptation of nodes. However, agents have only a limited view on the evaluation of the global behavior, being a challenge to employ them in a dynamic environment as that of self-organizing wireless networks. Learning techniques must be improved considering changing environments. It is always a challenging situation to learn with environments lacking of global knowledge, with a great dynamism and nondeterminism.

6.3 The cooperation block

The cooperation block owns algorithms for distributed communication among nodes. Cooperation is worth collecting data and managing information that require some kind of interaction with other nodes. Such data represents network state in terms of physical layer, radio interferences and channel conditions. Also, cooperation block assists in collecting data from distributed security mechanisms such as reputation systems or intrusion detection systems. The cooperation block supports the reconfiguration block when the agreement among different nodes is requested to select a protocol or security mechanism.

Research directions

In [11], authors emphasize the high communication cost for sampling/probing channels and exchanging information in WMNs, and [12] provides insights for designing effective cooperative communication protocols and algorithms. Different algorithms based on clustering or quorum sensing systems try to minimize the overhead generated by control messages used to time synchronization among nodes, and maximize power savings [13]. Power control mechanisms can also be employed to minimize overhead controlling the range of communication among nodes and being more efficient [14]. Some other solutions have been proposed to improve data collection in self-organizing wireless

networks based on mechanisms like data aggregation. However, it is still a challenge to design a universal data collection method whose time-complexity, message-complexity and energy-complexity are all within constant factors of the optimum.

6.4 The security block

The security block comprises of security mechanisms that can be employed by the node. They follow the three lines of defense, prevention, reaction and tolerance, representing, respectively, survivability properties as resistance, recognition and recovery. A node holds different security mechanisms for each defense line. Depending on the control block decision and reconfiguration block selection, a set of security mechanisms is used. The node applies simultaneously at least one security mechanism of each defense line. Security block also manages the integration among applied security mechanisms.

Research directions

Issues related to different security mechanisms have been handled for self-organizing wireless networks. Despite of many solution proposals for trust models, intrusion detection systems or reputation systems, the majority of them use some kind of threshold. However, defining thresholds in a dynamic and nondeterministic environment lacks of accuracy or precision. A direction for improving those proposals lies in making dynamic and adaptable threshold values. However, achieving such feature requires the development of mechanisms that consider a changing environment.

6.5 The layer block

Our framework defines a functional block for each layer of the protocol stack, such as **link and physical layer manager**, **routing layer manager**, **transport layer manager** and **application layer manager**. These functional blocks manage and adapt characteristics, protocols and configurations of those layers as response to the control block decisions and reconfiguration choices. Managed agents execute operations of these functional blocks. The management entity launches specific layer agents only when some reconfiguration is required. Agents act until they finish their task. After that if a new reconfiguration in the layer is necessary, the management entity launches a new agent.

Research directions

Since layer agents are launched only when some reconfiguration is required, proposing an optimized way to execute this operation is worth. In order to trigger the creation of layer agents, information supplied by reconfiguration block is requested. What and when layer agents will be created must to be defined for achieving survivable goals. Hence, efficient methods to learn with the dynamic environment, and take quick and efficient decisions are worth. This integration between reconfiguration block and layer block is still an open research issue.

6.6 The cross-layer communication block

The cross-layer communication block provides communication among layers of the protocol stack. It monitors and collects data related to these layers. Collected data and the algorithm used to collect them are defined indirectly by the control block decisions and directly by the reconfiguration block. The cross-layer communication block observes data on these layers by predefined evaluation metrics, including performance metrics, and it feeds node's database with such information. Examples of this data can be interferences on channel or radio, latency on application layer, packet loss ratio and others. The cross-layer block can just collect data or it can process it, e.g., it can characterize the behavior of communication channels and store only the result of this process. Further, this block can send values related to performance metrics directly to the performance and QoS evaluation block.

Research directions

Defining which data will be collected from other layers of the protocol stack is a first issue. Such data is related to application requirements, and features of the network that should be analyzed to provide an overview of network context and situation. Further, how to collect this data from other layers in an efficient and optimized way without compromising network behavior is another issue.

6.7 The performance and QoS evaluation block

The performance and QoS evaluation block aims to examine if requirements of performance and Quality of Service (QoS) are being reached. In general, applications define the requirements of performance and QoS, and evaluations detect changes on the network's performance and statistical data (as

timer and counter values) collected. Results of these evaluations assist the control block to take decisions in accordance with performance requirements. Depending on the network situation, the control block can give priority or not for the requirements of performance and QoS requested by an application. In a critical situation of the network, as a disaster, for instance, in which the connectivity is worth for data transmission, the control block can decide not consider the QoS requirements of a video application and give priority to keep the network connected. In another way, if the network is being used for a video transmission of a medical operation of emergency, the QoS requirement must be reached.

Research directions

First, the requirements of applications related to QoS, performance and survivability must be established. Models that can represent these requirements need to be designed in order to facilitate the operations of the performance and QoS evaluation block. Those models must consider not only application requirements, but also different aspects related to users and their behavior in order to assist in accurate evaluations. Since survivable networks will give priority for critical services and applications, it is essential to distinguish them. For the moment, critical services for self-organizing wireless networks are those necessary to guarantee network connectivity. However, depending on the requirements of applications other services must be assured in the presence of faults, attacks or intrusions.

6.8 Node's database

Information used by performance manager block and other blocks comes from **node's database**. It owns information collected in that moment and also history of logs. We highlight that the amount of information or data stored by the node is limited depending on its capabilities. When the node reaches a predefined threshold of stored bytes, it replaces stored information or data by new one following some data replacement policy. Various data replacement policies have been proposed and analyzed for wireless network, e.g., [15], providing insights for a data replacement policy to be employed by our framework.

Research directions

How to store collected data considering resource limitations of nodes and make it available in an optimized way is an issue. Data fusion techniques

have been employed in order to efficiently distribute data among network nodes. Other kind of data distribution and storage could be applied always considering resource limitations.

7 Conclusion

This article presented SAMNAR, a conceptual architecture for security management in self-organizing wireless networks. SAMNAR is inspired on the human body immune system and provides survivability of essential network services. The architecture comprises three main modules, survival communication and collect modules. We have designed a framework for security and performance management, where each SAMNAR's module is developed. We offer some research directions highlighting main issues for each functional block proposed in the framework in order to guide future works.

Referências

[1] P. E. Heegaard and K. S. Trivedi, "Network survivability modeling," *Computer Networks*, vol. 53, no. 8, pp. 1215–1234, 2009.

[2] F. Martignon, S. Paris, and A. Capone, "Design and implementation of MobiSEC: a complete security architecture for wireless mesh networks," *Computer Networks*, vol. 53, no. 12, pp. 2192–2207, 2009.

[3] J. Dong, K. Ackermann, and C. Nita-Rotaru, "Secure group comm. in wireless mesh networks," *Ad Hoc Networks*, vol. 7, no. 8, pp. 1563–1576, 2009.

[4] Y. Yuan, S. Wong, S. Lu, and W. Arbaugh, "ROMER: resilient opportunistic mesh routing for wireless mesh networks," in *IEEE WiMesh*, 2005.

[5] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communication Magazine*, vol. 43, no. 9, pp. 23–30, 2005.

[6] A. Keromytis, J. Parekh, P. N. Gross, G. Kaiser, V. Misra, J. Nieh, D. Rubenstein, and S. Stolfo, "A holistic approach to service survivability," in *ACM SSRS*. New York, NY, USA: ACM, 2003, pp. 11–22.

[7] F. Wang and R. Upppalli, "SITAR: a scalable intrusion-tolerant architecture for distributed services," in *DISCEX*, vol. 2, 2003, pp. 153–155.

[8] J. Wylie, M. Bigrigg, J. Strunk, G. Ganger, H. Kiliççöte, and P. Khosla, "Survivable information storage systems," *IEEE Computer*, vol. 33, no. 8, pp. 61–68, 2000.

[9] T. Aura and S. Mäki, "Towards a survivable security architecture for adhoc networks," in *International workshop on security protocols*. London, UK: Springer-Verlag, 2002, pp. 63–73.

[10] Y. Qian, K. Lu, and D. Tipper, "A design for secure and survivable wireless sensor networks," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 30–37, 2007.

[11] P. Kyasanur, J. So, C. Chereddi, and N. Vaidya, "Multichannel mesh networks: challenges and protocols," *IEEE Wireless Communications*, vol. 13, no. 2, pp. 30–36, 2006.

[12] J. Yackoski, L. Zhang, C.-C. Shen, L. Cimini, and B. Gui, "Networking with cooperative communications: holistic design and realistic evaluation," *IEEE Communication Magazine*, vol. 47, no. 8, pp. 113–119, 2009.

[13] V. Cicirello, M. Peysakhov, G. Anderson, G. Naik, K. Tsang, W. Regli, and M. Kam, "Designing dependable agent systems for mobile wireless networks," *IEEE Intelligent Systems*, vol. 19, no. 5, pp. 39–45, 2004.

[14] Z. Yang, S. Liao, and W. Cheng, "Joint power control and rate adaptation in wireless sensor networks," *Ad Hoc Networks*, vol. 7, no. 2, pp. 401–410, 2009.

[15] H. Chen, Y. Xiao, and S. V. Vrbsky, "Scalability study of cache access mechanisms in multiple-cell wireless networks," *Computer Networks*, vol. 52, no. 15, pp. 3017–3027, 2008.