A Survey of Survivability in Mobile Ad Hoc Networks

Michele Nogueira Lima [a,1] Aldri Luiz dos Santos [b] Guy Pujolle [a]

[a] *Laboratoire d'informatique de Paris 6 (LIP6), Université Pierre et Marie Curie, 104, Avenue du Président Kennedy, 75016, Paris, France*

[b] *Department of Informatics, Federal University of Paraná, 81531-990, Curitiba, Paraná, Brazil*

Abstract

Considerable improvements have been made towards providing ad hoc network security. However, conventional lines of defense are inefficient to put all attacks and intrusions off. In view of security limitations, we present a survey of the most relevant survivable initiatives for MANETs. Survivability is defined as the network ability to fulfill correctly its functions even in the presence of attacks or intrusions. We propose a new classification of the defense lines taking into account the resiliency-oriented approach and we identify survivability properties. Survivable initiatives are described and categorized into three groups: routing discovery, data transmission and key management. We observed that security solutions focus still on one network layer or one type of attack, using essentially preventive or reactive mechanisms.

Key words:
Survivability, Intrusion Tolerance, MANETs, Security, Dependability

1 Introduction

The increasing popularity of wireless portable devices, such as laptops, PDAs, wireless telephones or wireless sensors, has highlighted the importance and the potential of mobile ad hoc networks and ubiquitous computing. Currently, due

Email addresses: Michele.Nogueira@lip6.fr (Michele Nogueira Lima), aldri@inf.ufpr.br (Aldri Luiz dos Santos), Guy.Pujolle@lip6.fr (Guy Pujolle).

[1] This work was supported by CAPES/Brazil, grant 4253-05-1.

to Internet service facilities and the convenience of portability, many people employ mobile networking in their professional and domestic activities.

Mobile ad hoc network (MANET) is a network formed by a set of mobile hosts which communicate among themselves by means of the air. Those hosts establish dynamically own network without relaying on a support infrastructure or a central administration, and cooperate to forward data in a multi-hop fashion [1–3]. MANETs were initially proposed for military applications and currently their use has been enlarged. Examples of application include emergency disaster relief, digital sensors positioned to take measurements in a region, battle field communication, people sharing information during a lecture or conference, and so on [4].

MANET's hosts must ensure functionalities and guarantees provided by support structures in wired networks. Routing, access control and node authentication are examples of network functionalities that must be done by node cooperation. Nevertheless, those hosts present characteristics as constraint resources (processing, memory, bandwidth, energy and others), mobility and wireless communication that limit their capacity on performing dense activities, increasing the dynamism of the network topology and the complexity on providing network management, control and security.

Due to their mean of communication and constraint resources, MANETs are critically vulnerable to diverse types of attacks. Wireless communication, for example, is susceptible to interferences and interceptions. Portability has made devices each time smaller, with resource limitation, and thus easy targets for overload attacks [1, 5]. The fully network decentralization, absence of support infrastructure and the dynamic topology increase the vulnerability to many attacks as impersonation attacks, Sybil attacks [6], selective forwarding, blackhole, wormhole attacks [7, 8], among others.

Many solutions have been proposed for security problems on ad hoc networks [1, 3, 8, 9]. In general, these solutions work in the preventive or reactive way and apply mechanisms and techniques to protect basic protocols and applications. Essentially, the solutions use specialized hardware, cryptographic primitives, mechanisms for overhearing neighbor communication or protocols designed for path diversity [10]. However, techniques and mechanisms are used for a specific goal, being effective to one given case, but inefficient to others. Moreover, all existent techniques and mechanisms are themselves incapable of individually defending against all types of attacks and intrusions.

Due to solution restrictions and MANETs characteristics, researchers have focused on designing security mechanisms for network survivability. Survivability is commonly defined as the ability of a system to fulfill its mission, in a timely manner, in presence of attacks, failures or accident [11]. The term

system has a wide sense and could characterize networks, means of communication or services, and *mission* represents the abstract goals and requirements of the system.

The contributions of this survey are the following. A definition of survivability to attacks, considering a design perspective resiliency-oriented. A new classification of defense lines, suggesting that survivability to attacks can be reached when all defense lines work cooperatively. A description of survivability key properties and requirements for MANETs. An investigation of survivable initiatives organized on three groups: route discovery, data transmission and key management. The work concludes that current initiatives continue emphasizing the use of preventive and reactive mechanisms, being specialized to one network layer, protocol or attack, without exploring well some survivability properties and requirements.

The rest of the survey is organized as follows. Section 2 defines survivable systems, presenting survivability concepts and key properties, as well as a classification of defense lines considering those concepts. Section 3 summarizes MANETs characteristics, security issues and conventional countermeasures. Section 4 analyzes the survivability requirements for MANETs, taking into account their essential services. Section 5 describes and categorizes in three groups the survivable initiatives for MANETs. Finally, Section 6 concludes the survey and gives future directions.

2 Background

Security mechanisms, in general, follow two defense lines: one preventive and another reactive [8]. The former provides mechanisms to avoid any type of attack as firewall and cryptographic systems. The latter consists in taking action on demand to mitigate intrusions, as intrusion detection systems (IDS).

Nevertheless, preventive and reactive solutions are not fully efficient against all types of attacks and intrusions [12, 13]. Thus, research groups have built security mechanisms toward one third line of defense, called **intrusion tolerance** (IT) [14], as illustrated in Figure 1. The tolerance approach complements the other ones and its goal is the development of mechanisms to make systems (networks, means of communication, services and others) tolerant to attacks and intruders, and to guarantee the network operation in presence of malicious actions [14–17].

Systems using techniques for tolerating intrusions and attacks are called **intrusion tolerance systems**. In a broad sense, these techniques can provide certain survivability key properties, supporting the development of survivable

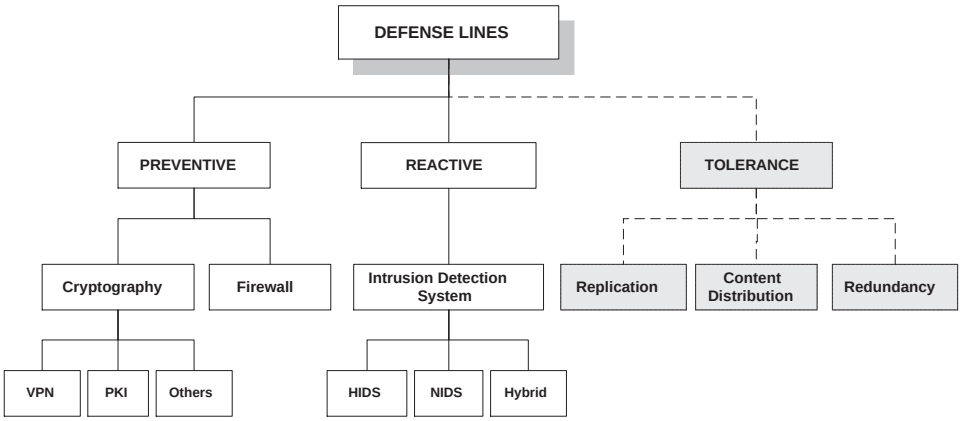

Figure 1. New classification: lines of defense

systems. Survivability refers to a system capability of completing its goals and requirements in a timely manner, even in the presence of attacks, intrusions, failures or accident [11].

Laprie *et. al* [18] consider survivability similar to **dependability** in terms of goals and addressed threats. Dependability goals consist of the system ability in delivering trusted services and in avoiding service failures that are more frequent or more severe. This work addresses **survivability** as a special case of dependability, where the network is capable of completing its goals in the presence of malicious faults. These faults bring different conditions and specific necessities that can only be efficiently treated when analyzed individually [17]. Hence, survivability aims to increase effectiveness of solutions, and to assist dependability and security integration.

Making a parallel with dependability, intrusion tolerance consists in applying fault tolerance mechanisms to the security domain. In contrast to survivability, intrusion tolerance consists of techniques and mechanisms to provide correct services in the presence of intrusions [19]. Intrusion tolerance emerged with Fraga and Powell's initiative [20], however, the development of such systems only had more attention in the last decade with MAFTIA (*Malicious- and Accidental-Fault Tolerance will be Internet Applications*) [15] and OASIS (*Organically Assured and Survivable Information System*) [16] projects. The MAFTIA project has designed wide scale distributed systems to tolerate many ordinary faults and malicious attacks in fixed networks. The OASIS project was developed by American Department of Defense (DARPA) to build a tolerant system for high-speed networks.

Survivability attributes are composed of guaranteeing reliability, availability, maintainability, confidentiality, integrity and safety [18]. Survivable systems are related with a subset of faults, called malicious or intentional faults, comprising of malicious logics and DoS attacks or intrusion [21, 22]. In general, these faults abuse of existent system vulnerabilities, introduced accidentally

or deliberately during the development of the system. An attack can successfully exploit system vulnerabilities resulting in an **intrusion**.

This work suggests that **survivability** should be reached by the use of preventive, reactive and tolerant approaches operating together. Figure 2 illustrates this behavior where preventive defenses will be the first obstacle for attacks, blocking certain ones and incapable of preventing others. Some attacks can succeed in intruding into system (or network) and reactive defenses will begin to work, trying to detect and stop them. However, reactive defenses have also limitations and intruders can be successful in compromising the system. In order to guarantee the system operation even in presence of intrusions, techniques of intrusion tolerance need to be applied, until preventive or reactive defenses can adapt themselves and take actions against the attack or intrusion.

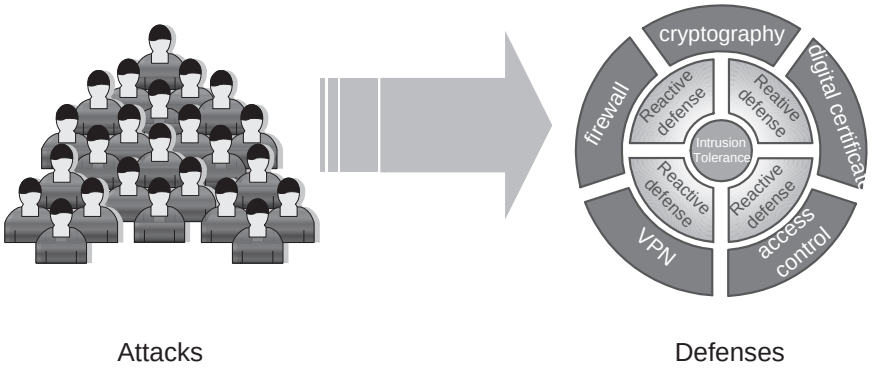

Figure 2. All defenses working together

The following properties are defined for survivable systems: resistance, recognition, recovery and adaptability [17]. **Resistance** is the capability of a system to repel attacks. User authentication, firewalls and cryptography are examples of mechanisms used to reach it. **Recognition** is the system capacity to detect attacks and evaluate the extent of damage. Examples of recognition mechanisms are intrusion detection by patterns and internal system integrity verification. **Recovery** is the capability of restoring disrupted information or functionality within time constraints, limiting the damage and maintaining essential services. In general, conventional strategies applied for achieving recovery are replication and redundancy. Finally, **adaptability** is the system capacity of quickly incorporating lessons learned from failures and adapting to emerging threats [11, 17]. Figure 3 illustrates the interaction among these key properties.

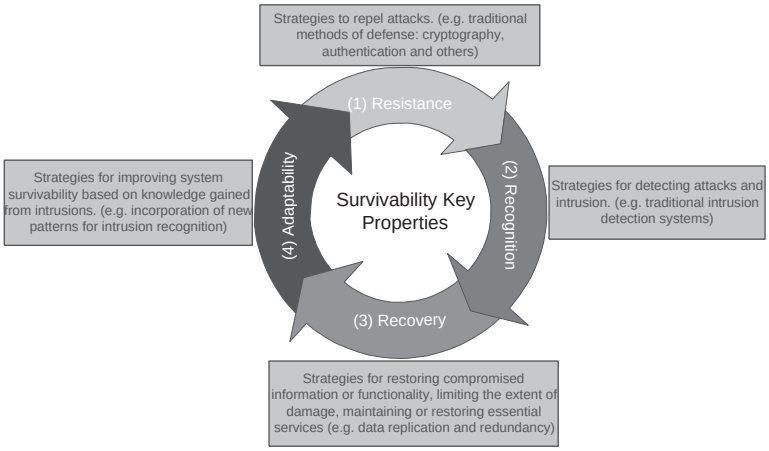

Figure 3. Survivability key properties

3 Issues and mechanisms for security in MANETs

MANETs are susceptible to many security issues. Characteristics as dynamic topology, resource constraint, limited physical security and no centralized infrastructure make those networks vulnerable to passive and active attacks [8]. In passive attacks, packets containing secret information might be eavesdropped, violating the confidentiality principle. Active attacks include injecting packets to invalid destinations, deleting packets, modifying contents of packets, and impersonating other nodes.

Classifing attacks by network protocol stack is the more frequent. Table 1 summarizes the main attacks for MANETs according to network layers. Some attacks are also categorized as byzantine or misbehavior attacks, being generated by network node whose actions cannot be trusted or do not conform to protocol specifications. Blackhole, wormhole, rushing, Sybil, sinkhole, HELLO flooding and selective forwarding are examples of byzantine attacks. Moreover, these attacks are also related to selfishness problem. The goal of a selfish node is to make use of the benefits of participating in the ad hoc network without having to expend its own resources in exchange [23].

Researches have actively exploring many mechanisms for securing mobile ad hoc networks. These mechanisms are based essentially on customized cryptographic primitives, protocols for path diversity, protocols that overhear neighbor communication, and protocols that use specialized hardware [10].

Cryptographic primitives have been used to provide authentication, integrity and confidentiality of secure routing protocols [26–28]. In general, HMAC (message authentication code used for authentication [29]), digital signatures and symmetric or asymmetric cryptographic operations are applied with these purposes. However, this mechanism generally increases the network overhead.

Layer	Attack	Description
Physical	Jamming	deliberates interference with radio reception to deny the target's use of a communication channel
Link	Exhaustion	attacker induces repeated retransmission attempts in order to exhaust target's resources
	Collision	deliberates collisions or corruption induced by an attacker in order to deny the use of a link
Network	Wormhole	adversaries cooperate to provide a low-latency side-channel for communication by means of a second radio with higher-power and long-range link
	Blackhole	adversaries advertise zero-cost routes to every other node, forming routing black holes
	Sinkhole	an attempt is made to lure traffic from the network to pass through an adversary in order to facilitate other attacks
	Flooding	overwhelms victim's limited resources: memory, processing or bandwidth
	Selective forward	malicious nodes behave like normal nodes in most time but selectively drop sensitive packets for the application. Such selective dropping is hard to detect
	Sybil	multiple fake identities will be created for adversary nodes, meaning that an attacker can appear to be in multiple places at the same time
	Rushing	adversaries quickly forward their route request (RREQ) messages when a route discovery is initiated, in order to participate any route discovery. This attack can be carried out against on-demand routing protocols, as AODV [24], DSR [25] and others
Transport	SYN Flooding	classic TCP SYN flood where an adversary sends many connection establishment requests to a target node, overwhelming its resources

Table 1. Attacks by network layers

MANET constraint resources prevent the usage of complex encryption methods. Furthermore, no existence of infrastructure and dynamic topology increase the difficulty for the key management and distribution, and mainly these mechanisms cannot defend against internal attacks.

Path diversity techniques aim to increase route robustness by discovering multipath routes and using these paths to provide redundancy in data transmission [10, 30, 31]. Multipath routing protocols can use all routes found simultaneously and transmit the same data more than one time; or can use them on demand, as an alternative. However, many of those protocols do not apply mechanisms to authenticate intermediary nodes in routes, making them vulnerable to impersonation and Sybil attacks.

Techniques for monitoring neighbor communication and behavior in wireless channel have been proposed to detect and minimize misbehaving nodes [10, 32, 33]. Generally, these techniques assume that wireless interfaces support promiscuous mode operation. Promiscuous mode means that if a node A is within range of a node B, it can overhear communications to and from B even if those communications do not directly involve the node A. By means

of this mechanism, nodes can monitor others and announce those that have misbehavior as dropping or tampering packets.

Finally, hardware, as GPS (*global position system*) [34] or directional antennas, has been used to help in preventing and detecting wormhole attacks [35, 36]. Pering *et. al*, for example, introduce the notion of *packet leash* as a general mechanism for detecting and defending against them [27]. A leash is any information added to a packet and designed to restrict its transmission distance. Leashes are classified as geographical or temporal. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender, and to take localization positions, the GPS can be used. In [36], a directional antenna scheme was proposed to also detect those attacks. The scheme restricts the communication among nodes based on distance information, which is calculated according to received signals. Unfortunately, these schemes are specific to wormhole attacks.

4 Survivability requirements for MANETs

MANET introduce diverse functions, operations and services influenced by the context, applications and basic characteristics. In a critical situation, where parts of a system are compromised by attacks or intrusions, priority is given to maintain correct functionality of essential services. Essential services demand capacities and guaranties to assure their correct delivery in presence of attacks, failures or accidents. Such capacities and guaranties are identified as survivability requirements and they can diverge significantly depending on the system characteristics, its scope, and the consequence of the service interruption. Despite of Linger *et. al* [37] to define those requirements in terms of essential and non-essential services, this section discusses survivability requirements for MANETs considering only and network characteristics.

Essential services in MANETs can be classified in two types: *specific service* and *general service*. The former represents those services designed by application or network context. The latter denotes fundamental services that are independent of applications or context as routing, connectivity and communication. Since specific essential services can vary with application or context, this work analyzes only the survivability requirements related to general essential services.

Survivable MANET's must maintain a connected network, since that service allows efficient routing and end-to-end communication. Consequently, survivable systems must (i) work on heterogeneous networks; (ii) be self-configurable (mainly for node's addressing and service discovery); (iii) adjust transmit powers of nodes adaptively in response to mobility, activities, environments and

attacks; and (iv) use node's energy and other resources efficiently when the system suspects that it is under attack.

Routing is other essential service, whose cooperative work way brings many security weaknesses. For this reason, survivable systems need to apply mechanisms (i) to control the access of nodes in the network; (ii) to protect the wireless communication at physical and data link layers as well as user/data acquisition; (iii) for integrity, confidentiality and authentication principals; (iv) for robust and efficient routing; and (v) to work with redundant approaches - multipath, double routing protocol and others.

Communication is the main purpose of any network and mobility issues make MANET's communication a challenge. In this way, its survivability requirements consist of (i) designing protocols that work normally on different conditions; (ii) making functional end-to-end communication without needing a reliable return channel for acknowledgments; (iii) using multiple communication channels; and (iv) proceeding during eventual disconnection and along with partial segments of paths. Table 2 summarizes MANETs survivability requirements taking into account these general essential services.

Essential services	**Survivable system requirements**
Connectivity	working on heterogeneous networks
	self-configuration (mainly, for naming and service discovery)
	self-adaptation of node transmit powers in response to mobility, activities, environments and attacks
	the efficient use of node's energy
Routing	node access control
	protection of wireless communication at physical, medium and data link layers
	integrity, confidentiality and authenticity principals
	efficiency and robustness
	the use of redundant approaches
Communication	working in different and variable conditions
	the use of asymmetric and unidirectional links
	end-to-end communication without considering a reliable return channel
	the use of multiple communication channel
	working even on eventual disconnections

Table 2. Survivability requirements

Certain survivability requirements are consequence of network characteristics. Decentralization and self-organization requirements, for example, are indispensable due to network organization and inexistence of central points. Scalability requirement comes from the great variability on the total number of nodes and the dynamic topology. Self-managed and self-controlled survivable systems are required to guarantee the network efficiency and functionality. Figure 4 illustrates the integration among all mentioned requirements, highlighting those yielded by general essential services (light gray) from those pro-

duced by network characteristics (dark gray). The requirements dependent of the context or application are not considered, making this incomplete view in the figure.

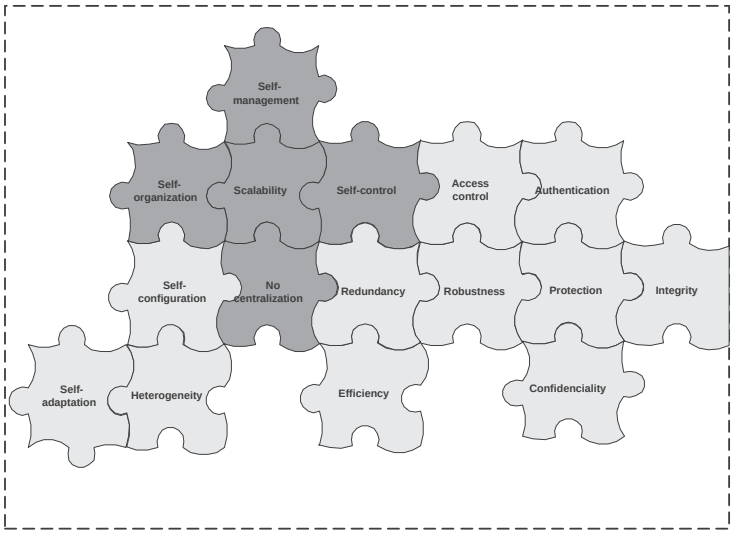

Figure 4. Integration among survivability requirements

Each requirement, as depicted in Figure 4, is connected to others that together can improve the network survivability. Robustness, for example, will be more effective for survivability when redundancy, access control and protection are also applied. Protection is often reached by authentication, integrity and confidentiality. Access control applies generally authentication mechanisms and self-controlling characteristic enhances it. Scalability requirement will be reached by means of self-management, self-organization and self-controlling. These integrations only illustrate some possibilities for together improving the survivability, without extinguishing all of them.

Nowadays, each essential service in Table 2, connectivity, routing and communication, is treated and associated to three different layers, respectively, link, network and application layers. This is not sufficient for archieving a complete survivable system due to multi-layer attacks. Further, the use of multi-layer information can make security mechanisms more robust, resistant and survivable. Routing layer, for example, can use energy or bandwidth information present in link layer to take better choices and to be more adaptive. Routing layer can inform the others about attack detection and in this way, those layers can start an alert procedure. In summary, the survivability existent on the layers can mutually provide guarantees and support.

Based on previous considerations, it is identified three view plans for survivability as shown in Figure 5. The first plan is related to survivability key properties described in Section 2. This plan analyzes survivability considering the existence of key properties. The second plan observes the system based on survivability requirements achieved. Finally, the third plan correlates key

properties and requirements with protocol layers. The figure also emphasizes that the two first plans can be analyzed considering separately one layer, without forgetting multi-layer cooperation aspect explained before.

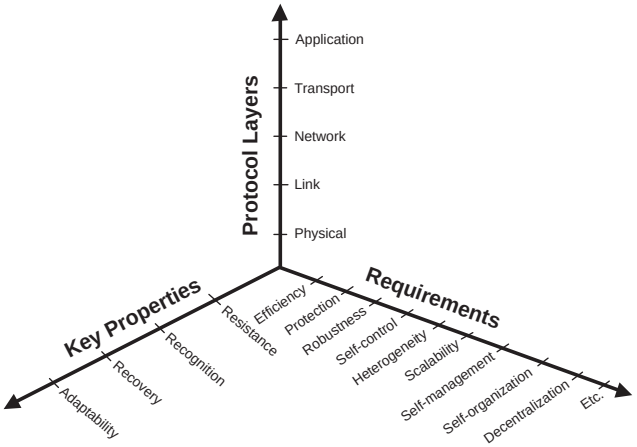

Figure 5. Plans of view for survivability

5 Survivable initiatives for MANETs

This section describes several initiatives on building survivable mobile ad hoc networks. Despite many of them do not present a complete survivable proposal, they have goals, characteristics and mechanisms more correlated to properties and requirements of survivability than just preventive or reactive schemes. Since some papers survey conventional security defense lines [3, 9, 38, 39], this work focuses on security propositions that aggregate more than one defense line and apply some technique of tolerance as redundancy or recovery.

Initiatives found in the literature are categorized on three main groups: *route discovery*, *data forwarding*, and *key management and access control*. The route discovery group consists of approaches trying to make route discovery phase of routing protocols more resistant and tolerant to different kinds of attacks and intrusion. The data forwarding group is composed of initiatives specialized on data forwarding using preventive or reactive security schemes and some tolerance techniques, as redundancy. The last one includes cryptographic key management and access control approaches built to be more tolerant to attacks.

Routing is essential for the correct operation of MANETs, and many routing protocols have been proposed in the literature, including proactive (table-driven), reactive (demand-driven), and hybrid solutions. Most of the existing protocols have assumed a MANET as a trust environment. However, as shown in previous sections, MANETs are highly vulnerable to attacks due to their characteristics.

Secure routing protocols have been proposed [27, 28, 40], such as SRP [30], SAODV [41], SAR [42]. These secure protocols are mostly based on authentication and encryption algorithms, being inefficient to put all intruders and attacks off. In this way, some research groups have built intrusion tolerant routing approaches as TIARA (Techniques for Intrusion-resistant Ad Hoc Routing Algorithms) [43], Best-Effort Fault Tolerant Routing (BFTR) [44], ODSBR (An On-Demand Secure Byzantine Routing Protocol) [45] and Boudriga's approach [13].

5.1.1 TIARA

TIARA defines a set of design techniques to mitigate the impact of Denial of Service attacks and can be applied on routing protocols to allow the acceptable network operation in the presence of these attacks. The main techniques established by TIARA are: *flow-based route access control (FLAC)*, *distributed wireless firewall*, *multipath routing*, *flow monitoring*, *source-initiated flow routing*, *fast authentication*, *the use of sequence numbers* and *referral-based resource allocation*. For its effective implementation, TIARA should be adapted to a routing protocol, being incorporated more easily into on-demand protocols, such as DSR and AODV.

FRAC technique and distributed wireless firewall are applied together to control packet flow and to prevent attacks based on resource overload. A flow is a sequence of packets, traveling from the source node to a destination node. Each node participating in the ad hoc network contains an access control list, where authorized flows are defined. Based on this list the node drops packets belonging to unauthorized flows, or forwards packets from an authorized flow.

The use of multipath routing has been proposed in order to tolerate attacks. The discovery and maintenance of many routing paths for a specific flow are enforced, but only one route is chosen initially to data forwarding. The flow monitoring technique checks the network failures sending periodic control messages, called *flow status packets*. If a path failure is identified, an alternative path found in the discovery phase will be selected. For the cases where source nodes wish to send data packets through a specific path, the source-

initiated flow technique will add a label to every packet indicating its path. A lightweight authentication mechanism is proposed for TIARA. It consists in placing the path label of the packet in a secret position. Each node can define a different position for the label within the packet, and this information is used for the node authentication. Sequence numbers are also inserted into secret locations of data packets, as well as path labels. This mechanism provides a counter measure for replay attacks. TIARA also considers a limited resource allocation in order to prevent authorized traffic flows that can exhaust network resources. In this technique, a routing node defines a threshold for the maximum amount of network resources allocated for a given flow.

5.1.2 BFTR

Best-effort fault-tolerant routing (BFTR) is a source routing algorithm exploring the ad hoc network path redundancy. Its goal is to maintain packet routing service with high delivery ratio and low overhead in presence of misbehaving nodes. BFTR never attempts to conclude whether the path, or any node along it, is good or bad. It takes into account existing statistics to choose the most feasible path, such as each one with the highest packet delivery ratio in the immediate past. By means of existing statistics and receiver's feedback, different types of attacks can be indistinctly detected as packet dropping, corruption, or misrouting.

BFTR is based on DSR flooding to retrieve a set of paths between source and destination nodes, whenever necessary, and it chooses the shortest path to send packets. The algorithm considers that the behavior of any good node is to delivery packets correctly with high delivery ratio. In this way, a good path consists of nodes with a good behavior pattern from the end-to-end point of view. Any path that deviates from such pattern is assumed a bad path, being discarded and replaced by the next shortest path.

In order to make the solution more generic and efficient than previous ones, BFTR requires no security support from intermediate nodes. Instead, the source node only relies on end-to-end performance observation to judge if a packet is successfully delivered. The source and destination nodes of connections are assumed well-behaved. A previous trust relationship between end nodes is required, being possible the authentication between them during data communication. It is not defined the way to establish the trust relationship, but it can be established by the knowledge of the public key through an off-line public key distribution such as PGP or via on-line public key infrastructure service.

The protocol has three routing components: route discovery, route selection, and route maintenance. Route discovery is similar to DSR except by RREP

packet to be sent along the reverse path of the RREQ packet. The destination sends multiple replies, so that the source can have multiple paths between the source and the destination. RREP packets are signed with the shared secret key between the source and the destination to prevent them from fabrication and replay attacks. Having multiple paths the source node will select the path using statistics information provided by signed acknowledgement packets and packet delay.

The route maintenance phase is identical to that defined by DSR. If a route failure report is received, the protocol will discard the current routing path and proceed with the next shortest path in the route cache. Moreover, if all paths in the current route cache have been rejected, BFTR will initiate new route discovery just as what DSR does, attempting to discover more paths. BFTR does not distinguish between route failure due to the mobility and test failure caused by misbehaving nodes.

5.1.3 ODSBR

ODSBR is a routing protocol that intends to provide a correct routing service even in presence of Byzantine attacks [45]. ODSBR operates using three sequential phases: (i) least weight route discovery, (ii) Byzantine fault localization and (iii) link weight management. The first phase is based on double secure flooding and aims to find lowest cost paths. Double flooding means that route discovery protocol floods with route request and response messages in order to ensure path setting up. In this phase, cryptography principals are used to authentication and digital signature operations. The second phase discovers faulty links on the paths by means of an adaptive probing technique. This technique uses periodic secure acknowledgments (acks) from intermediate nodes along the route and the integrity of the packets is assured by cryptography. The last phase of ODSBR protocol manages the weight assigned to a faulty link. Each faulty link has a weight to identify bad links, being this information stored at a weight list and used by the first phase of the protocol.

Results have shown the good performance of ODSBR in many scenarios for different metrics. However, some important points are not evaluated or well defined. For example, ODSBR assumes the use of RSA cryptography and digital signatures without considering open issues as public key distribution, node pair key initialization or the iteration among nodes to guarantee authenticity. These operations are essential for the good ODSBR functionality and can influence the results. Moreover, it is based also on acknowledgments that could not be assured due to mobility and dynamic topology.

5.1.4 Boudriga's approach

Boudriga *et. al* [13] propose a new approach for building intrusion tolerant MANETs. It consists in a multi-level trust model and a network layer mechanism for resource allocation, recovery and intrusion detection. The multi-level trust model assumes that the network is divided into two virtual sets: the resource's domain and the user's domain. Resources have many attributes as location, ownership, activities and trust level and user's attributes are its identity, activities and trust level. Each resource assigns a unique trust level for each type of activity that it is involved with and each location where it appears. Users or applications allocate resources based on activities and trust levels.

The distributed scheme of resource allocation proposed by Boudriga *et. al* aims to allocate available resources with the largest possible values and the smallest costs. For each application, only a fraction of a resource is allocated at a given node. The application demand specifies the set of requested resources, the total requested amount for each resource and the minimum trust level acceptable for each resource. Each network node has a resource manager, a security manager, and a trust manager that monitors and coordinates the resources and security functionalities.

Finally, intrusion tolerance on the Boudriga's approach is reached through the availability of a distributed firewall mechanism, a technique for detecting and recovering from intruder-induced path failures, a trust relation between all nodes, a IPsec-based packet authentication, and a wireless router module that enables survivability mechanisms to DoS attacks. The distributed firewall aims to protect the MANET against flooding attacks and each node maintains a firewall table containing the list of all packets passing through it and accepted by their destination. After a handshake between the sender and the receiver of a related flow, the entries in a firewall table will be maintained automatically and refreshed when failures are detected, intrusion occurrences or other abnormal behavior. Based on those entries, the node can forbid any flood of spurious traffic. Three parameters are managed by the nodes to detect anomalies in the behavior: packet loss rate, duplicate packet rate and authentication failure rate.

5.2 Data forwarding

Some works proposed secure routing mechanisms to defend against several attacks. However, those protocols ensure the correctness of the route discovery, but alone they can not guarantee secure and undisrupted delivery of data. Intelligent attackers can easily gain unauthorized access to the network, follow

the rules of the route discovery, place themselves on a route, and later redirect, drop or modify traffics, or inject data packets. In a nutshell, an adversary can hide its malicious behavior for a period of time and attack at the least expected time, complicating its detection. For these reasons, mechanisms to provide data confidentiality, data availability and data integrity are necessary for guaranteeing secure data forwarding.

Several mechanisms have been proposed for securing data forwarding. Lightweight cryptographic mechanisms as Message Authentication Code (MAC) [29], for example, are used to data integrity. Nuglets [46], Friends and Foes [47], Sprite [48] propose mechanisms to stimulate node participation in data forwarding, trying to guarantee data availability. CORE [49] and CONFIDANT [50] are examples of reputation systems that provide information to distinguish between a trustworthy node and a bad node. This information also encourages nodes to participate in the network in a trustworthy manner.

Some solutions to provide data confidentiality and data availability have tried to apply techniques as redundancy and message protection to be more resilient to attacks. In SPREAD [51], SMT [52] and SDMP [53], for example, the message is divided into multiple pieces by a *message division algorithm*. These pieces are simultaneously sent from the source to the destination over multiple paths. In [54], a cross-layer approach is investigated to improve data confidentiality and data availability, using directional antennas and intelligent multipath routing with data redundancy.

5.2.1 SPREAD

The Secure Protocol for Reliable Data Delivery (SPREAD) scheme proposes the use of some techniques to enhance data confidentiality and data availability. Initially, the message is splitted into multiple pieces by the source node, using the threshold secret sharing scheme. Each piece is encrypted and sent out via multiple independent paths.

SPREAD assumes link encryption between neighboring nodes, with a different key. The scheme supposes that an efficient key management scheme exists and focuses on three main operations: to divide the message, to select multiple paths and to allocate message pieces into paths. SPREAD selects multiple independent paths taking into account security factors as the probability that the path can be compromised. It allocates the pieces into each selected path with the goal of minimizing the probability of harm.

SPREAD uses (T,N) threshold secret sharing algorithm [55] where the system secret can be reconstructed from any T out of N shares. Thus, the secret message can be divided into N shares in order to harm the message. In this way, the enemy has to compromise at least T shares for recovering the original

message.

The SPREAD scheme works with multiple routing and its goal is to achieve the optimal share allocation way where the attacker should damage all the paths to recover the message. If the message could be divide into N pieces where N is the number of independent paths, the optimal data confidentiality could be achieved when the threshold, T, is equal to N. However, this trivial choice provides non-redundancy, being impossible the reconstruction of the message by the destination, if any packet loss occurs. Thus, SPREAD improves the reliability and fault-tolerance introducing some redundancy, being $T < N$.

A share allocation scheme is used to distribute the N shares into M most secure available paths. SPREAD formulates the share allocation as a constrained optimization problem in order to minimize the use of paths with great probability of being compromised and, in the same time, to allocate the N shares, guaranteeing a given security level and also providing the redundancy. It is found that the number of shares allocated for each secure path should be bigger than $N - T + 1$ and smaller than $T - 1$. Furthermore, the sum of the number of shares allocated for each secure path must be equal to N. These constraints will force the attacker to compromise all the paths to damage the original message, while at the same time, it can tolerate a certain number, $N - T$, of share lost during the transmission or caused by some types of attacks.

5.2.2 SMT

The goal of the secure message transmission (SMT) protocol is to ensure data confidentiality, data integrity, and data availability, safeguarding the end-to-end transmission against malicious behavior of intermediary nodes. SMT exploits four main characteristics: end-to-end secure and secure feedback mechanism, dispersion of the transmitted data, simultaneous usage of multiple paths, and adaptation to the network changing conditions.

SMT requires a security association (SA) [56] between the two end communicating nodes, so no link encryption is needed. This trust relationship is indispensable for providing data integrity and authentication of end nodes, necessary for any secure communication scheme. The two end nodes make use of a set of node-disjoint paths, called Active Path Set (APS), being a subset of all existing paths between them.

Data message is broken into several small pieces based on the information dispersal scheme [57]. It is also added limited data redundancy to allow recovery from a number of faults. Data redundancy is also divided into pieces. A ratio of N/M, where M out of N transmitted pieces, is needed to reconstruct the original message. All pieces are sent through different routes existent in APS,

enhancing statistically the confidentiality and availability of exchanged messages. At the destination, the dispersed message is successfully reconstructed only if sufficiently M pieces are received. Each piece carries a Message Authentication Code (MAC), allowing its integrity verification by the destination. The destination validates the incoming pieces and acknowledges the successfully received ones thought a feedback to the source. The feedback mechanism is also protected by cryptography and is dispersed to provide fault tolerance.

Each path of APS has a reliability rate based on the number of successful and unsuccessful transmissions on this path. SMT uses this rate to manage the paths in APS, trying to determine and maintain a maximally secure path-set, and adjusting its parameters to remain effective and efficient.

5.2.3 SDMP

The Secured Data based MultiPath (SDMP) protocol exploits also multiple paths between network nodes to increase the robustness and data confidentiality. The protocol assumes Wired Equivalent Privacy (WEP) link encryption/decryption of all the frames between neighboring nodes, which provide link layer confidentiality and authentication. SDMP can work with any routing protocol which provides topology discovery and supports the use of multipath for routing. The protocol makes no assumptions about the node-disjointness of the supplied path-set.

SDMP distinguishes between two types of path: signaling and data. The first is dedicated only for signaling and the second carries user data. Signaling type requires only one path of the path-set existent between source and destination nodes, being the other paths available for data transmission.

The protocol divides the message into shares using the Diversity Coding approach [58]. Each share has a unique identifier and those shares are combined in pairs through an XOR operation related to a random integer number generated. Each pair is sent along a different path. This message division approach is essentially a non-redundant version of Diversity Coding, although redundancy could be easily added to provide data availability. Information necessary for message reconstruction at the destination is sent by the signaling path.

Unless the attacker can gain access to all of the transmitted parts, the probability of message reconstruction is low. That is, to compromise the confidentiality of the original message, the attacker must get within eavesdropping range of the source/destination, or simultaneously listen on all the paths used and decrypt the WEP encryption of each transmitted part. However, note that it is possible to deduce parts of the original message from only a few of the transmitted pieces, especially since one piece of the original message is always sent in its original form on one of the paths.

5.2.4 Cross-layer approach

In contrast to previous solutions, a cross-layer approach is investigated in [54] to improve data security in MANETs. The solution uses directional antennas and intelligent multipath routing to enhance end-to-end data confidentiality and data availability. Unlike an omni-directional antenna that transmits or receives radio waves uniformly in all directions, a directional antenna transmits or receives radio waves in one particular direction. Directional antennas make eavesdropping more difficult and reduce the areas covered by packet transmissions, minimizing the overlap of message pieces sent by multiple paths. Thus, the use of directional antennas is justified by the reduction on the likelihood that an adversary is able to simultaneously gather all of the message pieces at the source or destination nodes.

A self-adaptive transmission power control mechanism is used together with directional antennas to reduce the message interception probability. This mechanism allows the transmitter to use only enough transmission power in order to reach the intended receiver, minimizing the radiation pattern for a given radio transmission and the possibility of an attacker to intercept the message transmission. Dynamically the transmission power is adjusted depending of the data packet type exchanged between neighboring nodes. For example, to send data packets, the minimum power is required for reliable communication, while maximum power is used to transmit request-to-send/clear-to-send (RTS/CTS) and to control packets of IEEE 802.11 Medium Access Control (MAC) protocol.

Multipath routing is also used to statistically enhance data availability. Thus, messages are divided based on threshold secret sharing algorithm, and then the shares are sent by multiple node-disjoint paths. Two intelligent routing schemes are proposed to reduce message interception probability: (i) minimizing the physical distance of hops and (ii) minimizing the path-set correlation factor. Knowing that the area covered by the antenna lobe augments with the increase of the physical distance of hops, and that attackers have better chance to intercept messages on large covered areas, the first scheme intends to minimize the physical distance of hops. Edge weights equal or proportional to their corresponding physical distance are set and a shortest-path routing algorithm is run to find paths with shortest physical distance of hops.

The second scheme is based on the correlation factor of the node-disjoint paths. This factor represents the number of links connecting the paths. The total correlation factor of a set of paths is the sum of the correlation factor of each possible pair of paths. Thus, it is proposed to minimize the message interception probability in order to reduce the total correlation factor of the path-set used for message exchange.

Security solutions have relied on cryptography and suppose the existence of an infrastructure for providing and managing keys. Some MANET's characteristics, as the lack of any central infrastructure, make key management a challenge. Despite of this, distributed and self-organized key management system for MANETs have been proposed. Basically, there are two types of key infrastructure [3, 9]. The first involves the private key infrastructure, which establishes common private keys used for symmetric cryptography, such as symmetric group keys used for securing group communications. The second considers the public key infrastructure, which provides a couple of keys (public/private) used for asymmetric cryptography, as in digital signatures. This subsection addresses the below initiatives.

5.3.1 PGP-like

One of the survivable key management initiatives for MANETs is called PGP-like [59]. This system handles the public key management problem and proposes a fully distributed self-organizing public key management infrastructure. PGP-like is based on the PGP (Pretty Good Privacy) functionality [60] and each node is responsible for creating its public and private keys. Unlike PGP, where certificates are mainly stored in centralized certificate repositories, certificates in PGP-like are stored, distributed and managed by the nodes in a fully self-organized manner. In this system, key authentication is performed via chains of public-key certificates. When a node x wants to verify the authenticity of the public key of node y, both nodes, x and y, initially combine their local certificate repositories. Then, the first node tries to find an appropriate certificate chain from x or y.

As public and private keys are created locally by a node itself, public-key certificates are issued based on the trust existent among the nodes. In this way, if a node x believes that a given public key K_z belongs to a given node z, then x can issue public-key certificate in which K_z is bound to z by the signature of x. The trust among nodes is based on the way that public keys are exchanged. For example, if nodes x and y have exchanged their key through a channel like an infrared, the node x can believe that K_y belongs to y.

Initially, each node holds in its repository certificates issued by it and the certificates that other nodes issued to it. However, PGP-like defines a mechanism that provides periodic exchanges of certificates between neighbor nodes. This mechanism aims to distribute the certificates and become more efficient to find a chain of public-key certificates. Moreover, mechanisms to update and to revoke keys are used to prevent conflicts.

PGP-like presents functionalities to deal with misbehavior nodes. It provides operations to cross-check the keys existent in certificates and to detect inconsistencies. The certificates are inconsistent when two or more of them are related to the same user, but they present different keys or relate the same public key to different users.

5.3.2 Joshi's approach

Joshi *et. al* propose a fully distributed certificate authority scheme based on secret sharing and redundancy [61]. In secret sharing mechanism, the certificate authority's private key is first divided into parts. These parts or key shares are then distributed among the nodes in the network. To communicate, nodes have to recreate the key. The certificate authority (CA) key can be recreated by combining a minimum number of key shares from the total number of shares. The critical situation is when the number of nodes required to recreate the key are not found in the communication range of the node trying to communicate.

The number of key shares per node is more than one by incorporating redundancy into the network. Since each node stores more than one key share, then the number of nodes required to recreate the CA key is reduced, increasing the chances of a legitimate node for recreating the CA key. On the other hand, the redundancy poses a challenging since the chances of an intruder entering in the network and compromising the CA key are increased. When an intruder accesses the network and compromises one node, it becomes as good as a valid node. To overcome this problem, it is proposed the use of a intrusion detection system (IDS), which should identify the misbehavior/compromised nodes and remove them from the network.

5.3.3 URSA

URSA is a ubiquitous and robust access control solution for mobile ad hoc networks, where no single node monopolizes the access decision or is assumed to be completely trusted [62]. Instead, multiple nodes jointly monitor a local node and certify/revoke its ticket. Tickets performs the same functionality of conventional digital certificates, having expiration time, personal public key of the node, signature and identifier. Tickets are certificated and updated periodically to resist conspiracy of attacks by multiple misbehavior nodes. Certifications are based on RSA cryptosystem [62] and on threshold cryptography-based signature [55].

URSA handles a localized group trust model where a node is considered trust if it is trusted by any k trusted nodes. The trust relation is defined within a certain period T, which is defined by ticket's expiration time. Based on this

model, URSA keeps a general RSA key pair denoted as SK, PK. The SK key is used to sign tickets for all nodes; and the certificates signed by SK can be verified by PK. However, no single node in the network has a full information of SK. Instead, each node holds a share of SK to sign the partial tickets.

When a node moves to a new location, for example, it exchanges tickets with its new neighbors, as the first step to verify each other. After receiving the ticket from its neighbors, the node verifies the ticket signature with PK. After this procedure, certified neighbors help each other one in routing and forwarding packets. Neighbor nodes also monitor each other to detect possible misbehaviors. If a misbehavior node is detected, ticket revocation can be done to prevent the attack propagation. Tickets are also periodically renewed to improve the resilience of the system.

URSA presents important characteristics to survive attacks in MANETs, being decentralized, self-controlled, robust and present aspects for providing access control, authenticity, integrity, and confidentiality. A critical point is the definition of the amount K of secret share holders to be used in the system operations. This amount must balance between service availability and intrusion tolerance. However, URSA is vulnerable to $K + 1$ collaborative nodes.

Other works follow the same idea of URSA and apply threshold approach as [5] and [63]. Although they present similar characteristics to URSA, they deal with a public key management problem. In fact, Zhou and Haas [5] are the first to address public key management in MANET, and also applied threshold approach to make it decentralized and robust.

6 Conclusion

The use of MANETs has increased and, consequently, the security issues have become more important. Traditional defense lines are not sufficient for such networks, since they present different characteristics and properties that require new approaches. This article introduced survivability concepts and its correlation with preventive, reactive and tolerance defense lines. Survivability enables MANETs to fulfill their goals even in presence of attacks or intrusions by means of the cooperation among those three defense lines.

Key properties of survivability as resistance, recognition, recovery and adaptability were detailed, and survivability requirements for MANETs were analyzed. Those requirements comprise self-organization, self-control, self-configuration, self-management, access control, protection, authentication, scalability, redundancy and others.

Existent survivable initiatives are categorized in three groups: route discovery, data transmission and key management. These initiatives are described emphasizing survivable characteristics and the use of different defense lines. Based on those initiatives, we can conclude that (i) security solutions for MANETs are still based on a few set of preventive and reactive techniques; (ii) solutions stay specialized either on attacks or one layer of the stack protocol; (iii) adaptability property is almost unexplored; (iv) requirements as heterogeneity, efficiency, robustness and self-management are not yet reached and initiatives consider them of low importance.

Finally, this work highlights that a full survivable MANET needs to consider a multi-layer and multi-attack solution, beyond being heterogeneous to diverse environments and adaptable on the fly to unexpected situations. Further, survivable MANETs should apply cooperatively the three defense lines instead of only one or two independently.

References

[1] P. Papadimitratos and Z. Haas. *Handbook of ad hoc wireless networks*, chapter Securing mobile ad hoc networks. CRC Press, 2002.

[2] F. Adelstein, S. K. S. Gupta, and G. G. Richard III. *Fundamentals of mobile and pervasive computing*. McGraw-Hill, 2005.

[3] D. Djenouri, L. Khelladi, and A. N. Badache. A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications surveys & tutorials*, 7(4):2–28, 2005.

[4] C. E. Perkins. *Ad hoc networking: an introduction*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 2001.

[5] L. Zhou and Z. J. Haas. Securing ad hoc networks. *IEEE network*, 13(6):24–30, 1999.

[6] J. Douceur. The sybil attack. In *Proceedings of the international workshop on peer-to-peer systems (IPTPS)*, Cambridge, MA (USA), March 2002.

[7] H. Yang, H. Luo, J. Kong, F. Ye, P. Zerfos, S. Lu, and L. Zhang. *Ad hoc network security: challenges and solutions*. CRC Press, 2004.

[8] B. Wu, J. Chen, J. Wu, and M. Cardei. *Wireless/mobile network security*, chapter A survey on attacks and countermeasures in mobile ad hoc networks. Springer, 2006.

[9] P. Argyroudis and D. O'Mahony. Secure routing for mobile ad hoc networks. *IEEE Communications surveys & tutorials*, 7(3):2–21, Third Quarter 2005.

[10] I. Khalil, S. Bagchi, and C. Nita-Rotaru. DICAS: detection, diagnosis and isolation of control attacks in sensor networks. In *Proceedings of the international conference on security and privacy in communication networks (SECURECOMM)*, pages 89–100, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[11] R. Ellison, D. Fisher, R. Linger, H. Lipson, T. Longstaff, and N. Mead. Survivable network systems: an emerging discipline (cmu/sei-97-tr-013). Technical report, Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, 1997.

[12] P. E. Veríssimo, N. F. Neves, and M. P. Correia. Intrusion-tolerant architectures: concepts and design. Technical Report DI-FCUL TR-03-5, University of Lisbon, Department of Informatics, University of Lisbon, Portugal, 2003.

[13] N. A. Boudriga and M. S. Obaidat. Fault and intrusion tolerance in wireless ad hoc networks. In *Proceedings of IEEE wireless communications and networking conference (WCNC)*, volume 4, pages 2281–2286, Washington, DC, USA, 2005. IEEE Computer Society.

[14] Y. Deswarte and D. Powell. Internet security: an intrusion-tolerance approach. *Proceedings of the IEEE*, 94(2):432–441, 2006.

[15] Malicious- and accidental-fault tolerance for internet applications, 2006. Access: August 2006.

[16] Organically assured and survivable information system (OASIS), 2006. Access: August 2006.

[17] J. P. G. Sterbenz, R. Krishnan, R. R. Hain, A.W. Jackson, D. Levin, R. Ramanathan, and J. Zao. Survivable mobile wireless networks: issues, challenges, and research directions. In *Proceedings of ACM workshop on wireless security (WiSe)*, pages 31–40, New York, NY, USA, September 2002. ACM Press.

[18] J.-C. Laprie and B. Randell. Basic concepts and taxonomy of dependable and secure computing. *IEEE transaction dependable security computer*, 1(1):11–33, 2004.

[19] P. Veríssimo. Intrusion tolerance: concepts and design principles. a tutorial. DI/FCUL TR 02, Department of Informatics, University of Lisbon, July 2002.

[20] J. Fraga and D. Powell. A fault- and intrusion-tolerant file system. In *Proceedings of the international conference on computer security*, pages 203–218, 1985.

[21] J. C. Laprie. *Dependability: basic concepts and terminology in English, French, German, Italian, and Japanese (Dependable computing and fault-tolerant systems)*. Springer-Verlag, December 1991.

[22] A. Avizienis, J.-C. Laprie, and B. Randell. Dependability and its threats - a taxonomy. In *IFIP congress topical sessions*, pages 91–120, 2004.

[23] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. Mitigating byzantine attacks in ad hoc wireless networks. Technical report, Center for Networking and Distributed Systems, Computer Science Department, Johns Hopkins University, 2004.

[24] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of IEEE workshop on mobile computing systems and applications (WMCSA)*, page 90, Los Alamitos, CA, USA, 1999. IEEE Computer Society.

[25] D. Johnson, D. Maltz, and J. Broch. *DSR - the dynamic source routing protocol for multihop wireless ad hoc networks*, chapter 5, pages 139–172. Addison-Wesley, 2001.

[26] A. Perrig, R. Canetti, J. D. Tygar, and D. Song. The TESLA broadcast authentication protocol. *RSA CryptoBytes*, 5(2), 2002.

[27] Y. Hu, D. Johnson, and A. Perrig. SEAD: secure efficient distance vector routing for mobile wireless ad hoc networks. *Ad hoc networks*, 1:175–192, 2003.

[28] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: a secure on-demand routing protocol for ad hoc networks. *Wireless networks*, 11(1-2):21–38, 2005.

[29] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-hashing for message authentication. RFC 2104, Internet Engineering Task Force, February 1997.

[30] P. Papadimitratos and Z. Haas. Secure routing for mobile ad hoc networks. In *Proceeding of communication networks and distributed systems modeling and simulation (CNDS)*, 2002.

[31] P. Kotzanikolaou, R. Mavropodi, and C. Douligeris. Secure multipath routing for mobile ad hoc networks. In *Proceedings of the conference on wireless on-demand network systems and services (WONS)*, pages 89–96, Washington, DC, USA, 2005. IEEE Computer Society.

[32] S. Marti, T. J. Giuli, K. Lai, and M. Baker. Mitigating routing misbehavior in mobile ad hoc networks. In *Proceedings of the international conference on mobile computing and networking (MobiCom)*, pages 255–265, New York, NY, USA, 2000. ACM Press.

[33] M. Just, E. Kranakis, and T. Wan. Resisting malicious packet dropping in wireless ad hoc networks. In *Proceedings of the international conference on AD-HOC networks & wireless (ADHOC-NOW)*, pages 151–163, Montreal, Canada, 2003.

[34] B. Hofmann-Wellenhof, H. Lichteneeger, and J. Collins. *Global Positioning System: Theory and Practice*. Springer, New York, 2001.

[35] Y. C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: a defense against wormhole attacks in wireless networks. In *Proceedings of the IEEE computer and communications societies (INFOCOM)*, volume 3, pages 1976–1986, 2003.

[36] L. Hu and D. Evans. Using directional antennas to prevent wormhole attacks. In *Proceedings of the network and distributed system security symposium (NDSS)*, pages 89–96, Washington, DC, USA, 2004. IEEE Computer Society.

[37] R. C. Linger, N. R. Mead, and H. F. Lipson. Requirements definition for survivable network systems. In *Proceedings of the international conference on requirements engineering (ICRE)*, pages 00–14, Washington, DC, USA, 1998. IEEE Computer Society.

[38] T. Anantvalee and J. Wu. *Wireless/mobile network security*, chapter A survey on intrusion detection in mobile ad hoc networks. Springer, 2006.

[39] A. Mishra, K. Nadkarni, and A. Patcha. Intrusion detection in wireless ad hoc networks. *IEEE Wireless Communications*, 11(1):48–60, 2004.

[40] R. B. Bobba, L. Eschenauer, V. Gligor, and W. Arbaugh. Bootstrapping security associations for routing in mobile ad-hoc networks. In *Proceedings of the global telecommunications conference (GLOBECOM)*, volume 3, pages 1511–1515, 2003.

[41] M. G. Zapata. Secure ad hoc on-demand distance vector routing. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3):106–107, 2002.

[42] S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. In *Proceedings of the ACM international symposium on mobile ad hoc networking & computing (MobiHoc)*, pages 299–302, New York, NY, USA, 2001. ACM Press.

[43] R. Ramanujan, S. Kudige, and T. Nguyen. Techniques for intrusion-resistant ad hoc routing algorithms TIARA. In *DARPA information survivability conference and exposition (DISCEX)*, volume 02, pages 98–100, Los Alamitos, CA, USA, 2003. IEEE Computer Society.

[44] Y. Xue and K. Nahrstedt. Providing fault-tolerant ad hoc routing service in adversarial environments. *Wireless personal communications: an international journal*, 29(3-4):367–388, 2004.

[45] B. Awerbuch, R. Curtmola, D. Holmer, H. Rubens, and C. Nita-Rotaru. On the survivability of routing protocols in ad hoc wireless networks. In *Proceedings of the international conference on security and privacy in communication networks (SECURECOMM)*, pages 327–338, Los Alamitos, CA, USA, 2005. IEEE Computer Society.

[46] L. Buttyán and J.-P. Hubaux. Stimulating cooperation in self-organizing mobile ad hoc networks. *Mobile network application*, 8(5):579–592, 2003.

[47] H. Miranda and L. Rodrigues. Friends and foes: preventing selfishness in open mobile ad hoc networks. *Proceedings of international conference on distributed computing systems workshops (ICDCSW)*, 00:440, 2003.

[48] S. Zhong, J. Chen, and Y.R. Yang. SPRITE: a simple, cheat-proof, credit-based system for mobile ad-hoc networks. In *Proceedings of the IEEE computer and communications societies (INFOCOM)*, volume 3, pages 1987– 1997, 2003.

[49] P. Michiardi and R. Molva. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In *Proceedings of the IFIP TC6/TC11 sixth joint working conference on communications and multimedia security*, pages 107–121, Deventer, The Netherlands, 2002. Kluwer, B.V.

[50] S. Buchegger and J.-Y. Le Boudec. Performance analysis of the CONFIDANT protocol: cooperation of nodes – fairness in dynamic ad-hoc networks. In *Proceedings of IEEE/ACM symposium on mobile ad hoc networking and computing (MobiHoc)*, Lausanne, CH, June 2002. IEEE.

[51] W. Lou, W. Liu, and Y. Fang. SPREAD: enhancing data confidentiality in mobile ad hoc networks. In *Proceedings of the IEEE computer and communications societies (INFOCOM)*, 2004.

[52] P. Papadimitratos and Z. J. Haas. Secure data transmission in mobile ad hoc networks. In *Proceedings of the 2003 ACM workshop on wireless security (WiSe)*, pages 41–50, New York, NY, USA, 2003. ACM Press.

[53] R. Choudhury, X. Yang, R. Ramanathan, and N. H. Vaidya. On designing MAC protocols for wireless networks using directional antennas. *IEEE transactions on mobile computing*, 5(5):477–491, 2006.

[54] V. Berman and B. Mukherjee. Data security in MANETs using multipath routing and directional transmission. In *Proceedings of IEEE international conference on communications (ICC)*, volume 5, pages 2322–2328. IEEE Computer Society, 2006.

[55] A. Shamir. How to share a secret. *Communications of the ACM*, 22(11):612–613, 1979.

[56] D. Maughan, M. Schertler, M. Schneider, and J. Turner. Internet security association and key management protocol (ISAKMP). RFC 2408, Internet Engineering Task Force, November 1998.

[57] M. O. Rabin. Efficient dispersal of information for security, load balancing, and fault tolerance. *Journal ACM*, 36(2):335–348, 1989.

[58] E. Ayanoglu, Chih-Lin I, R. D. Gitlin, and J. E. Mazo. Diversity coding for transparent self-healing and fault-tolerant communication networks. *IEEE Transactions on Communications*, 41(11):1677–1686, november 1993.

[59] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-organized public-key management for mobile ad hoc networks. *IEEE transactions on mobile computing*, 2(1):52–64, 2003.

[60] P. R. Zimmermann. *The official PGP user's guide*. MIT Press, Cambridge, MA, USA, 1995.

[61] D. Joshi, K. Namuduri, and R. Pendse. Secure, redundant, and fully distributed key management scheme for mobile ad hoc networks: an analysis. *EURASIP Journal on Wireless Communications and Networking*, 2005(4):579–589, 2005.

[62] W. Stallings. *Cryptography and network security - fourth edition.* Prentice Hall, 2006.

[63] S. Yi and R. Kravets. MOCA: Mobile certificate authority for wireless ad hoc networks. In *Proceedings of the PKI research workshop (PKI)*, 2003.

Vitae

Michele Nogueira Lima is a Ph.D. student at University Pierre et Marie Curie, Laboratoire d'Informatique Paris 6 (LIP6). Michele received her M.Sc in Computer Science at Federal University of Minas Gerais, Brazil, 2004. She has worked at security area for many years, her interest domain is security, wireless network, intrusion tolerance and dependability.

Aldri Luiz dos Santos is a professor at the Department of Informatics of Federal University of Paraná and was a visiting researcher at the Department of Computer Science of Federal University of Ceará. Aldri received his Ph.D. in Computer Science from Department of Computer Science of Federal University of Minas Gerais, Belo Horizonte, Brazil. Aldri received both his M.Sc. and B.Sc in Informatics from Federal University of Paraná, Curitiba, Brazil. From July to October 2001 he was an invited researcher at Cyber Solutions Inc., Sendai, Japan. He is member of the SBC (Brazilian Computing Society).

Guy Pujolle received the Ph.D. in Computer Science from the University of Paris IX in 1975. He is currently Professor at the University Pierre et Marie Curie and member of the Scientific Advisory Board of the France Telecom Group. Pujolle is chairman of IFIP Working Group on "Network and Internetwork Architectures". His research interests include wireless networks, security, protocols, high performance networking and intelligence in networking.