MoSAIC: Mobile System Availability Integrity and Confidentiality

ACI SI 2004 Project Proposal

LAAS-CNRS, 7 avenue du Colonel Roche, 31077 Toulouse Cedex 4
Eurécom, 2229 Route des Cretes, Sohia Antipolis, 06560 Valbonne
IRISA, Campus Universitaire de Beaulieu, 35042 Rennes Cedex

Summary

We address the hitherto little-explored issue of fault tolerance in such networks. The first objective is to define an automatic data back-up and recovery service based on mutual cooperation between mobile devices with no prior trust relationships. Such a service aims to ensure continuous availability of critical data managed by mobile devices that are particularly prone to energy depletion, physical damage, loss or theft. The basic idea is to allow a mobile device to exploit accessible peer devices to manage backups of its critical data. The implementation of such a service by cooperation between devices with no prior trust relationship is far from trivial since new threats are introduced: (a) selfish devices may refuse to cooperate, (b) backup repository devices may themselves fail or attack the confidentiality or integrity of the backup data; (c) rogue devices may seek to deny service to peer devices by flooding them with fake backup requests; etc. Dealing with these threats is the second objective of the project. We intend to study mechanisms for managing trust in cooperative services between mutually suspicious devices. Of particular interest are mechanisms based on reputation (for a priori confidence-rating and a posteriori accountability) and reward (for cooperation incitation). In the sparse ephemeral networks of devices considered, these mechanisms can rely neither on accessibility to trusted third parties nor on connectivity of a majority of the considered population of devices. Self-carried reputation and rewards are therefore of prime interest.

Résumé

Le projet proposé vise l'étude de nouveaux mécanismes de tolérance aux fautes et de sécurité pour les dispositifs mobiles sans-fil dans des applications d'intelligence ambiante (l'informatique ubiquitaire, le support tactique pour les champs de bataille ou la sécurité civile, la domotique, etc.). Nous nous focaliserons sur les réseaux épars auto organisés, utilisant de façon prédominante des communications sans-fil à un seul saut, c'est à dire des réseaux composés d'un faible sous-ensemble d'une population importante de mobiles, réseaux qui se créent spontanément par le fait d'une certaine proximité et la découverte mutuelle, et qui cessent d'exister dès que la communication n'est plus possible.

Nous explorerons le problème peu étudié jusqu'à présent de la tolérance aux fautes dans ces réseaux. Le premier objectif consiste à définir un service de sauvegarde et de restauration automatique de données, basé sur la coopération entre mobiles n'ayant aucune relation de confiance pré-établie. Un tel service vise à assurer la disponibilité des données critiques gérées par des mobiles qui sont particulièrement vulnérables à l'épuisement des batteries, aux dommages physiques, au vol, … L'idée de base est de permettre à un mobile d'exploiter des pairs accessibles afin de gérer la sauvegarde de ses données critiques. L'implémentation d'un tel service par coopération entre mobiles n'ayant aucune relation de confiance préalable est loin d'être triviale du fait des nouvelles menaces introduites : (a) des mobiles « égoïste » peuvent refuser de collaborer, (b) les mobiles qui servent de sauvegarde peuvent également défaillir ou attaquer l'intégrité ou la confidentialité des données, (c) des mobiles malveillants peuvent chercher à provoquer un déni de service par l'inondation des pairs avec de fausses requêtes de sauvegarde, etc. Traiter ces menaces est le second objectif du projet. Nous avons l'intention d'étudier des mécanismes de gestion de la confiance dans les services collaboratifs entre mobiles mutuellement suspicieux. Dans ce contexte, des mécanismes basés sur la notion de réputation (pour une évaluation de la confiance a priori et une imputabilité a posteriori) et de récompense (pour l'incitation à collaborer) sont de premier intérêt. Dans les réseaux épars et éphémères que nous considérons, les mécanismes ne peuvent se baser ni sur l'accès à des tiers de confiance ni sur la présence d'une majorité des mobiles considérés, la réputation et la récompense autoportées semblent par conséquent particulièrement bien adaptées.

1 Goal and context

Partie à rédiger en Anglais.

On précisera, en particulier, les verrous scientifiques et technologiques à dépasser, l'état de l'art ainsi que les projets concurrents ou similaires connus dans le contexte national et international, en particulier ceux auxquels les équipes du projet participent.

The proposed project aims to investigate novel dependability and security mechanisms for mobile wireless devices, especially personal mobile devices, in ambient intelligence applications (ubiquitous computing, tactical support for battlefield and emergency operations, virtual classrooms, home automation/entertainment, etc.). The mobile devices of interest include, for instance: personal digital assistants (PDAs), laptop computers, mobile telephones, digital cameras, etc., and extend to systems embedded within vehicles. Despite their heterogeneity, we suppose that each device contains at least a processor, some memory and a means of wireless communication. The focus is on sparse ephemeral self-organizing networks, using predominately single-hop wireless communication, i.e., networks of a small number of a potentially large population of mobile devices that come into existence spontaneously by virtue of physical proximity and mutual discovery, and that cease to exist as soon as communication is no longer possible.

Personal mobile devices are undergoing considerable development, and can broadly be classified into the following groups:

- **Laptops**, which are standard computers built as a compact and portable package. They support all the standard computing applications (edition, messaging, software development, internet access, database applications, image editing, etc.). They can carry large quantities of data (up to several tens of gigabytes), stored on a relatively fragile medium (disk drive), which is prone to failure. Their battery life is also limited (1-4h), and they usually do not offer a very low-consumption stand-by mode.
- **PDAs** are pocket computers with limited data input capability, used mainly for managing personal information, accessing databases, and navigation applications. Typical context-aware applications that make use of PDAs are concerned with collecting or viewing location-dependent notes or media. Battery life ranges from 6 to 12h of continuous usage, but they are typically used intermittently during short time periods (information lookup, note taking); the operating system is optimized for extended running time in standby mode. Local storage is ensured by dynamic RAM, and in some cases by static flash RAM, which allows data survival over battery outages.
- **Capture devices** capable of acquiring multimedia data, such as pictures, sound or video. Such devices are an important evolution, since mobile devices are thus becoming data sources instead of being mostly "reader" devices. There is also an increasing trend towards devices that combine the functions of PDAs and mobile phones with capture devices.

Usually, mobile devices are backed up on a server, and only use their local storage as a cache for offline use. For example, the contact database of a PDA is synchronized with a desktop computer application. This reduces the impact of failure of such devices. However, in the case of capture devices, large quantities of data are generated on the mobile device, without being recoverable. This highlights the need for new ways of ensuring data availability. Because the "density" of these devices is increasing (as mobile devices are becoming more and more popular), there is an opportunity for cooperatively backing up data by using neighborhood devices. The first objective of the proposed project is therefore to define an automatic data back-up and recovery service based on mutual cooperation between mobile devices with no prior trust relationships. Such a service aims to ensure continuous availability of critical data managed by mobile devices that are particularly prone to energy depletion, physical damage, loss or theft. The basic idea is to allow a mobile device to exploit accessible peer devices to manage backups of its critical data. To our knowledge, no work has already exploited this principle of cooperative backup for mobile devices. Indeed, relatively little work appears to have been devoted to tolerance of device failures in a mobile self-organized network scenario [N00]

[BI03a] [BI03b][1], although there has been considerable work on checkpointing in cellular mobile computing environments (see, e.g., [PKV96] [PS96] [YSF99] [CS01] [PWY01] [PR02]).

The implementation of such a service by cooperation between mobile nodes with no prior trust relationship is far from trivial since new threats are introduced: (a) selfish devices may refuse to cooperate; (b) backup repository devices may themselves fail or attack the confidentiality or integrity of the backup data; (c) rogue devices may seek to deny service to peer devices by flooding them with fake backup requests; etc. Dealing with these threats is the second objective of the project. We intend to study trust management mechanisms to support cooperative services between mutually suspicious devices. Of particular interest are mechanisms based on reputation (for prior confidence-rating and posterior accountability) and rewards (for cooperation incitation). In the sparse ephemeral networks considered, these mechanisms can rely neither on accessibility to trusted third parties nor on connectivity of a majority of the considered population of devices [ZH99]. Self-carried reputation and rewards are therefore of prime interest. This approach contrasts to most existing approaches to mobile system security, which have mainly focused on key management and distribution (see, e.g., [ZH99] [KKA03] [LNS03]) and on secure ad-hoc network routing (see, e.g., [BB01] [DLRS02] [PH02] [ZA02]).

Achieving dependability and security despite accidental and malicious faults in networks of mobile devices is particularly challenging due to their intrinsic asynchrony (unreliable communication, partitioning, mobility, etc.) and the consequent absence of continuous connectivity to global resources such as certification and authorization servers, system-wide stable storage, a global time reference, etc. Furthermore, the threats to dependability and security are particularly severe: device lifetime and communication severely limited by scarcity of electrical energy; use of wireless links causing susceptibility to link attacks ranging from passive eavesdropping to active impersonation, message replay, and message distortion; poor physical protection of mobile devices (especially in a hostile environment) making them susceptible to physical damage, and vulnerable to theft or subversion.

There are a number of other projects that are addressing issues that partly address some topics of this proposal, although with different objectives (those marked by an asterisk include as partners one of the partners of the current proposal):

- DIT* (DARPA OASIS program) focuses on intrusion-tolerance for ensuring dependability and security of Internet web servers.
- e-Justice* (FP6-IST IP) studies security of online and offline administration and justice workflows, in particular the design and use of certificate standards adapted to authorization management in environments with devices of different computation power (most notably PDAs and other mobile devices).
- MobileMAN* (FP5-FET) studies the security of mobile ad-hoc networks, in particularly through a reputation mechanism for enforcing cooperation.
- MOSQUITO* (FP6-IST STREP) focuses on context-aware security for business applications in ubiquitous computing environments, in particular new types of certificates and their use for configuring mobile networks.
- PRIME* (FP6-IST IP) is focused on identity management and the protection of privacy.
- SECURE (FP5-IST) is studying secure environments for collaboration between ubiquitous roaming entities; the emphasis is on self-configuring security mechanisms and a computational model for formally reasoning about trust.
- SPLASH* (ACI-SI) is focused on the security of communication protocols in mobile ad-hoc networks.

[1] External citations are given in the form [author-initials | 2-digit year] and are listed in Section 4. Internal citations are given in the form [institute-initial | serial digit] and are listed in Section 5.

- WiTNESS* (FP5-IST) addresses the security of communicating mobile devices using an extensible certificate infrastructure and application-level access control dependent on the security of the underlying execution platform.

The main features that distinguish the proposed MoSAIC project from most current and previous work are:

- Emphasis on spontaneous interaction between peer mobile devices with no prior trust relationships.
- Fault- and intrusion-tolerant collaborative data backup (with possible extension to checkpointing).
- Self-carried reputation and rewards for collaboration between sporadically interconnected and mutually suspicious peer devices without reliance on a fixed infrastructure and access to trusted third parties.

2 Project description

Partie à rédiger en Anglais sur 5 à 10 pages.

Entre autres, le caractère innovant du projet (concepts, technologies, expériences . . .) devra être explicité et la valeur ajoutée des coopérations entre les différentes équipes sera discutée.

Consider the following scenario:

> *Alice is attending an important symposium. Before leaving her office, she takes care to synchronize her wireless personal digital assistant (PDA) with her desktop computer. During this synchronization, all her critical personal and professional data (address book, calendar, notes, presentations, etc.) on her PDA are safely backed up.*
>
> *During the journey to the symposium, Alice continues to work on her presentation using her PDA. When she reaches her destination, Alice registers and loads the latest version of the symposium program onto her PDA. She selects the sessions she wants to attend and goes from one room to another, chatting with colleagues during the breaks and occasionally taking notes on her PDA. As she moves around, her PDA wirelessly interacts with those of the colleagues she meets or that pass nearby, automatically looking for data that they wish to make available concerning, for example, their centers of interest and their latest papers, presentations and reference citations, etc. Each physical encounter is seen as an opportunity for Alice's PDA to gather data pertinent to her research. At the end of the symposium, Alice attends a meeting of the steering committee to discuss and decide on how to organize the next event. During the meeting, the minutes are written in common by a computer-supported collaborative work application, running on the steering committee members' PDAs.*
>
> *On her way back home, Alice uses her PDA in the taxi to the airport to start writing a paper on the brilliant new idea she had while listening to one of the presentations at the symposium. Deep in thought while emptying her pockets at the airport security check, she carelessly forgets her PDA on the luggage belt. She is jolted back to reality by the metallic thud of her PDA bouncing of the tiled airport floor, shortly followed by the crunching sound of her PDA being shattered under the heavy boots of Hiro, the Sumo wrestler who happened to be following her. With dismay, she realized that she had effectively lost all the work she had done since leaving home. How she wished she had done her work with old-fashioned paper-and-pen.*
>
> *Luckily however, Alice's PDA had taken advantage of its chance encounters with other devices to automatically back-up the latest revisions to its data. So, after purchasing a new PDA in the airport gizmo shop, Alice was able to reload at least some of her recent data from devices of people she had happened to encounter earlier in the day. Some of them could be contacted directly in the airport lounge, others could be found by searching throughout the airport via an ad-hoc network of PDAs and other wireless devices. When she reached her office the following day, she was glad to realize that the remaining data had been automatically sent back to her office machine, which meant that the next synchronization brought her new PDA almost up-to-date with the state her previous one had before the unfortunate incident at the security check.*
>
> *Of course, since conference attendees and chance traveling companions move around frequently, the duration of each backup opportunity was unknown and relatively brief, which meant that only small amounts of data could be backed up each time. Moreover, many encounters were with people that Alice had never met before, including some shady persons of doubtful character, so care had to be taken that Alice's PDA did not reveal private or other sensitive data, nor that it was corrupted by data sent with malicious intent, nor that her data was backed-up only on rogue devices. Also, Alice was glad that her PDA had altruistically offered to share its resources with the devices encountered so that they too had been generous in return.*

This admittedly somewhat-contrived scenario illustrates the need for the proposed work: to use cooperation between peer wireless mobile devices, with no prior trust relationship, in order to ensure

device data availability, while providing guarantees of integrity and confidentiality (including privacy). Other scenarios, with varying prior trust models, can be imagined in military applications (e.g., recovery and redistribution of critical command and control data during battlefield operations), civilian emergency operations, home automation and entertainment, etc.

The project aims to investigate and develop prototype middleware services to support the dependability and security of mobile ambient intelligence applications. We consider highly dynamic systems consisting of wireless-equipped mobile devices that communicate with each other mostly by direct, single-hop communication. However, we do not preclude extensions to include indirect communication via a multi-hop ad-hoc network or occasional access to a fixed communication infrastructure. We do not intend to address mobile ad-hoc routing protocols, or dependability and security issues at the wireless network level, which are largely covered in other projects.

The remainder of this project description is composed of four sections. In section 2.1, we discuss the specific constraints imposed by characteristics of the considered ambient intelligence environment. In sections 2.2 and 2.3 we outline the two complementary research themes that we plan to develop in the context of sparse ephemeral networks of mobile devices, namely: fault-tolerance through secure cooperative backup and trust management for cooperative services. Section 2.4 concludes by outlining the expected contributions of each partner and discussing the added value of cooperation.

2.1 Characteristics of considered ambient intelligence environment

The problems we intend to consider arise from the specific characteristics of ambient intelligence applications based predominately on sparse ephemeral networks of mobile devices:

- **Disconnected mode or absence of fixed infrastructure**: traditional dependability and security functions depend on service offered by dedicated entities, as is the case for networking functions dedicated to routing. A typical security example is that of a public key certification service, which is usually a prerequisite for many basic security services such as authentication, key exchange, non-repudiation, etc. An example from the dependability viewpoint is that of a system-wide stable storage facility on which data and process checkpoints might be stored. Here, due to the highly dynamic nature of the considered networks and the predominant mode of operation without access to a fixed infrastructure, we aim to adopt a peer-to-peer approach without any such reliance on dedicated entities.
- **Absence of prior organization**: ambient intelligence applications rely on flexible communication and openness to facilitate interactions between devices with no pre-established organizational relationships. Classic security mechanisms are inapplicable in this context since they attempt to reproduce at a logical level the relationships that exist at the organizational level. In particular, entity authentication consists of demonstrating the link between an operational entity and an identity or role within an organization. The absence of such links means that classic security mechanisms cannot be used for ambient intelligence applications and that new mechanisms must be invented that allow the dynamic construction of trust relationships between entities that do not share a common organizational reference.
- **Ephemeral interactions**: wireless communication and mobility mean that entities can only interact for brief periods. Consequently, the implementation of dependability and security protocols based on durable interactions, using notions of state or session, become problematic.
- **User transparency**: one of the objectives of ambient intelligence applications is to make the underlying computer systems as transparent as possible to the user, to the extent that they become invisible. To reach this objective, availability, integrity and confidentiality need to be guaranteed by built-in dependability and security mechanisms, with minimal user interaction**.**
- **Privacy**: the danger that ambient intelligence applications might reveal data concerning user identity, location, behavior or other personal characteristics is of growing importance since society is becoming increasingly concerned by issues of personal rights and privacy. The protection of private data, which is far from being ensured in classic distributed applications, is exacerbated in ambient intelligent applications by virtue of the required transparency and their dependency on physical location.

- **Energy, computation and storage constraints**: most devices in an ambient intelligence environment are severely restricted by the autonomy of their batteries. The need to economize electrical energy means that wireless communication must be kept to a minimum. Furthermore, energy, space and cost limitations all construe to limit the device computation power and storage capacity. Consequently, protocols and mechanisms (e.g., cryptography) must be designed under severe energy, computation and storage constraints.

2.2 Theme 1 — Fault tolerance by cooperative backup

We consider the design and implementation of a prototype service for data backup and recovery by cooperation between ephemerously-connected and mutually-suspicious mobile devices. The need for such a fault-tolerance service is motivated by: (a) the increasing dependency of users on the availability, integrity and confidentiality of data carried by mobile devices and (b) the fragility of mobile devices and other risks relating to their use in a harsh or even hostile environment. We purposely limit ourselves to the issue of data backup, but note that such a service could serve as the basis for mobile device checkpointing and recovery, and for real-time tolerance of mobile device failure based on redundant devices.

The problems to be addressed include: resource allocation, garbage collection of obsolete backups, integrity and confidentially of backup data, resistance to denial-of-service (DoS) attacks, etc. The service is to be supported by negotiation between peer mobile devices with no prior trust relationship. Among the various approaches that might be considered, we intend to take inspiration from current work in the area of peer-to-peer (P2P) applications [Mnet] [LSB03], which have characteristics that are particularly well-adapted to the considered environment: absence of pre-established organization, service through cooperation, short-duration interactions, etc. We also plan to take inspiration from our know-how in the domain of fragmentation-replication-dissemination (FRD) techniques, which exploit distribution to increase availability, integrity and confidentiality in the face of accidental faults and malicious attacks [L4]. Until now, these FRD techniques have only been considered in the case of fixed infrastructure systems. We might also consider the advantages that could be drawn from occasional access to a common time reference (e.g., through the Global Positioning System (GPS)) or from exploiting mobility for data dissemination.

In the sequel, we use the terms "client" to refer to a device requesting its data to be backed up and "server" for a device hosting back-up data. Any device may be both a back-up client and a back-up server. However, to simplify our discourse, we usually consider a single client.

2.2.1 Threats

The data back-up service must face up to the following threats:

1. Permanent and transient accidental faults affecting a client device
2. Theft or loss of a client device.
3. Accidental or malicious faults affecting server device availability should recovery be required (i.e., on failure of the client).
4. Accidental or malicious modification of data backups that could violate data integrity if recovery should be required.
5. Malicious read access to data backups. Back-ups may contain sensitive confidential data that should be made unintelligible to the server device user.
6. Denial of service through selfishness. Cooperation may be thwarted if there is no incentive for devices to participate.
7. Denial of service through maliciousness. A malicious client could attempt to saturate servers by false back-up requests, and thereby deny service to other clients and to users of the attacked server devices. A malicious server may also choose to withhold backed-up data (cf. threat 3).

It will also be important to distinguish various contexts of utilization of the data back-up service according to the type of user community and appropriate prior trust model. For example, in a closed

(and non-infiltrated) military context, certain threats such as denial-of-service through selfishness or malicious attack may be considered negligible.

2.2.2 Back-up

The primary aim of the back-up service is to provide protection against permanent and transient accidental faults of client devices (threat 1). Depending on the utilization context, complete or partial back-up of client device data may be considered. Partial "delta" back-ups or update operation logs might be preferred to minimize the amount of data to be transferred to and stored on server devices, or even to provide some protection against confidentiality attacks on back-ups (threat 5).

The back-up service also provides protection of data availability in the face of loss or theft of the client device (threat 2). Confidentiality might be provided in such a situation by an "auto-delete" function triggered by a failed user-authentication challenge.

Unavailability and modification of back-ups (threats 3 and 4) are only of import if the client device should fail. Tolerance of multiple faults may be achieved by installing redundant back-ups on independent server devices. Malicious read access to back-ups (threat 5) may be prevented by cryptographic techniques, with appropriate trade-offs between the level of protection provided and the associated costs in energy and resource consumption. The strength (key length, degree of redundancy, etc.) and cost of the deployed techniques may be adapted according to the degree to which server devices may be trusted (e.g., devices of colleagues or those of strangers). The adaptation could also make use of a dynamic measure of the "reputation" of the server devices (see theme 2 below).

Fragmentation-replication-dissemination (FRD) techniques [L4] are also of interest here. Data confidentiality may be provided by cutting back-up data into fragments that are disseminated over different server devices. Fragments may also be replicated to ensure data availability and integrity (by voting on multiple replicas). Fragmentation, replication and dissemination may be modulated in both space and time according to the number of trustable devices available in a given place or at a given instant.

Denial of service through selfishness (threat 6) may be discouraged by the use of a "reward" scheme to motivate device participation, inspired from micro-economy approaches developed in peer-to-peer (P2P) applications. Devices acting as servers are rewarded for their participation and may redeem their earnings when acting as clients that wish to purchase back-up service. Denial of service through maliciousness (threat 7) may also be discouraged by an appropriate "reputation" mechanism. Devices with a history of detected maliciousness will have a poor reputation and will be spurned by client devices when negotiating to purchase back-up service. The related notions of reward and reputation are the subject of the cooperative service trust mechanisms to be investigated in the context of theme 2 of the proposed project.

2.2.3 Recovery

The second important aspect of the proposed data back-up service concerns the means by which back-up data may be re-installed when required on client devices, i.e., data recovery. This involves finding the data that has been backed up and transferring it back to the client device or its surrogate.

The recovery process will depend heavily on whether or not devices can occasionally connect to a fixed infrastructure. If access to a fixed infrastructure cannot be considered (e.g., in a battlefield scenario), then access to back-up data has to be based on establishing a wireless communication channel between client and server devices. If direct communication is not possible (which will be the usual case) then the solution may be to create an ad-hoc network with intermediate devices, or to wait until the devices are again within wireless range (by chance encounter or by planned rendezvous).

At least two recovery modes can be distinguished:

- "Push" recovery: the server devices automatically send data backups to the client device or its surrogate. The most appropriate way might be for server devices to trigger such a boomerang operation as soon as they have access to a fixed infrastructure. The data could be transferred

either immediately to the client device or its surrogate, or possibly through a trusted third party.

- "Pull" recovery: the client device searches for the data copies that it requires. Again, we may take inspiration from P2P systems that seek to develop totally distributed file search engines. Requests to the search engine might target the requested data by specifying particular places or times, e.g., "the data I backed up during the flight from Toulouse to Rennes on January 10, 2004".

When partial back-ups have been created, like when fragmentation-replication-dissemination is used, the recovery process will also need to tackle the problem of reconstructing the complete data from the various parts.

Many various optimizations of the proposed back-up service may be considered. For example, in the case of incremental back-ups, the optimal period of back-up creation may depend on several factors, including the relative size of the increments (deltas or update logs) and the performance of recovery based on those increments. The chosen solutions need to be flexible and adaptable to various application scenarios. Another important issue is that of garbage-collecting obsolete back-up data. This may depend on the notion of a contract set up between client and server devices, or be triggered when the client device announces that the earlier back-ups are obsolete. The appropriate solutions imply various business models associated with micro-economy mechanisms of various complexity: fines, contracts, leases, etc.

2.3 Theme 2 — Trust for cooperative services

With the development of short distance wireless communication technologies, in particular 802.11, Bluetooth, or more recently 802.15, and even RFID tags, it seems reasonable to assume the generalization of ad-hoc interactions to a large range of cooperative services that will complement cellular mobile systems.

A self-organizing ad-hoc network is built upon services that cannot be obtained without the cooperation of its constituent nodes. In order for such a cooperative service to be effectively implemented on a network as a whole, it is necessary to analyze how these nodes can be trusted to carry out their task. For instance, routing is a basic service in ad-hoc networks that is subject to non-cooperation from selfish nodes and deliberate attacks from malicious nodes. This service can only be achieved by isolating misbehaving nodes so that malicious nodes are simply ignored and selfish nodes receive a strong incentive to cooperate if they want to access the network at all.

The cooperative backup system presented under Theme 1 is another instance of such a cooperative service. In particular, it is likely that it will be quite frequently used in sparse and very dynamic ad-hoc networks, which will likely be in a situation where the user cannot reach his home network, even through multi-hop routing. In such disconnected operation scenarios, where mobile networks must be self-organizing, we contend that making devices accountable for their actions through a dynamic rating of their trustworthiness will foster effective cooperation. Trust management or trustworthiness rating must be based on mechanisms that fit with the assumptions made about the network topology and application requirements.

The cooperative backup service assumes that the user device will be in contact with many different devices during its journey. With an appropriate design of the backup service, a single malicious device will not able to totally disrupt the backup functionality as long as a sufficient number of non-malicious nodes can be given the incentive to participate in the cooperative backup service. In addition to fostering such cooperation, the trust-rating mechanisms developed in this theme may provide helpful hints for identifying such malicious devices, so that a device can judge which neighbors can be trusted to effectively store its critical data correctly. This will be especially useful in order to accordingly increase or reduce data dissemination, thus enabling the user to preserve his data, yet optimizing his device's energy consumption by reducing the number of messages exchanged.

Approaches for trust management

Three main approaches are generally recognized for managing or rating trust about the cooperation of other entities:

1. *Membership-based trust management*. This approach is the classic method of prior confidence, in which trust depends essentially on the entity being a member of a trusted group (e.g. allied army in a battlefield scenario). This membership can be established from the entity identity or public key by self-standing authorities or trusted third parties, as illustrated by public key infrastructures [ITU88] [EFL99] and trust management approaches [BIK01]. The trust in the entity cooperation is ensured the central authority and distrust is materialized by the revocation or timed invalidation of authority-issued credentials. The use of ad-hoc communications in this scenario however makes it necessary to add new security mechanisms when proof of the physical proximity of other entities is required [E7].
2. *Reputation-based rating*. In this approach, trust is estimated based on the evaluation of past interactions with the entity [E1] [LSB03]. The interest of reputation is that it may evolve positively or negatively and thus bring direct evidence of misbehavior. This approach is very well adapted to self-organized cooperative systems in which membership is meaningless since no trusted group is common to two communicating entities. The main issue of such schemes is the retrieval of reputation evaluations of a client entity. These evaluations may be computed either locally, based on present or past observations about the service completion, or obtained from "neighbors". In the latter case, the preservation of negative reputation evaluations is an important issue, as well as the forgery of positive reputation evaluations.
3. *Currency-based rating*. Trust in this approach is a micro-economic or currency-related notion [McC01]. Earning transferable credits (e.g., mojos, nugglets, brownie points, etc.) is a proof of a node's active participation in the system. This approach is less prone to malicious coalitions because rating someone positively costs credits. However, it involves the use of a significant infrastructure for currency exchange, in particular to prevent double or multiple spending of credits, and to bootstrap the system whenever a new entity enters. In addition, currency exchange also requires adequate security mechanisms to handle the exchange of credits against services fairly.

Rating mechanisms must be adapted to the characteristics of the network and cooperative service or application that is secured. In particular, the sparsely-populated networks that we envision make it difficult to obtain information about the exchanges of a neighbor node with the rest of the network. The ephemeral and highly dynamic nature of the interactions in the applications we target also makes it useless in general to build up trust from immediate observation only. The hybrid nature of the networks we want to secure, sometimes online with a global infrastructure, generally offline in the field, would also make it necessary to deal with disconnections if authorities are used to manage trust.

Self-carried reputation

Contrary to dense ad-hoc networks, the local observation of the behavior of neighboring nodes cannot be used as a general mechanism for evaluating reputation. Such an approach is the best to avoid denial of service attacks originating from fake neighbor recommendations, yet encourage self-organized participation to routing in a dense ad-hoc network [E2]. However, local observation can be achieved in these networks only because it is a side effect of the broadcast nature of the routing function on a wireless communication medium. This is not the case for most cooperative functions we consider, like for instance the storage of backup data.

Most reputation architectures for secure ad-hoc routing or for avoiding "freesurfing" in peer-to-peer services rely on an exchange of reputation information with other nodes or peers. However, the direct retrieval of information from remote nodes using one-hop communication technologies only, which we assume is the situation of the network most of the time, is simply impossible.

An alternative way of handling reputation is to have each device carry a summary of its reputation marks as established by the devices for which it performed services. Keeping one's own trust rating is generally performed through some credentials, often called "cookies" in P2P infrastructures [LSB03].

The content of such cookies is extremely important for designing trust-rating enforcement mechanisms. First of all, trust may depend on the criterion considered for an application: for instance, is this PDA often synchronized online, or did the owner of this PDA effectively store my latest backup? Second, if rating may be negative, it is likely that a selfish or malicious user will simply not present such cookies unless he is somehow forced to do so, for instance because he does not even know what the cookie contains. Finally, privacy is at stake since, for instance, a device might be traced based on the interactions testified by its cookies.

Designing security cookies for cooperative services thus very much depends on the considered adversary model. It may already be anticipated that some adversary models make it necessary to resort to membership-based trust to prevent the creation of selfish node cartels or simply to prevent an attacker from forging his own recommendations. Thus, even though cooperation is self-organized, there may be a need for some limited prior trust in a set of recommending devices. Part of the work done in this theme will be to find out which adversary models are relevant for the applications we consider and to define matching cryptographic primitives. The possible routes of exploration that we foresee for these primitives are histories of past actions of an entity based on signatures of knowledge using group signatures or group-blind signatures if privacy is required [E3], or based on certification chains [E6], or even on threshold cryptography. The computation power necessary to create and evaluate a cookie is an important issue for certain classes of devices, especially the ones we target, and thus has to be evaluated with care.

Currency-based incentives

Currency-based incentives seem to offer a fine way to deal with selfish nodes since nodes must provide service to earn credits so that they may themselves obtain some service. In addition, the evaluation of trust in such schemes only relies on the simple exchange of credits and not on a complex valuation of the entity behavior. Currency-based incentives are also quite interesting for preserving user privacy since only the currency issuer needs be named. Finally, since credit is a positive valuation, it makes no sense for an attacker to hide the credits he receives. On the other hand, attacks on currency-based incentives exist: they essentially revolve around the currency exchange phase.

Multiple spending of some credit the attacker has acquired, just like checks in real life, is a first form of attack. In the context of the applications we consider, it is clearly impossible to solve this problem at the level of mobile devices. However, as previously indicated, performing backup recovery generally requires occasional connection to a fixed infrastructure. This phase or any connection to such infrastructure may be used to force each user to reveal the credits received from other devices. This would make it possible for a central authority, most probably the currency issuer, to eventually locate any cheating party. The one-time certificate technique [E4] illustrates how financial compensations may be obtained out of multiple spending of a currency incentive. Similar mechanisms might be developed for fostering participation in cooperative services. Alternately, the identity of a cheating user might simply be revealed with similar techniques. The central authority might then simply stop distributing currencies to that particular user. New protocols are however required in that case so that currencies would carry a validity period, and even a multiply-spent credit would stop circulating after some time.

One major issue of such schemes is the enforcement of a fair exchange of credits against services. One way to deal with attacks of this kind might be to opt for micro-payment techniques. If communication cost in terms of autonomy is the main reason for selfishness, it may be possible to break up a backup transaction into small slices, even if we risk losing the last part of it. Another solution is to use tamper-proof or tamper-resistant hardware, like a smartcard, acting on behalf of a trusted third party like the currency issuer. Such hardware would for instance make it possible to enforce the exchange of a credit against the storage of some data, and release the credits earned only after some time is elapsed or a recovery has been requested.

We plan to develop protocols based on such incentives for the cooperative backup service of theme 1 and to simulate such systems in order to gain some insight about the behavior of such a scheme, and in particular its stability with respect to credit distribution.

Hybrid trust infrastructure

We foresee that a major contribution of this theme will be the elaboration of a hybrid trust infrastructure, in the sense that we will try to find out if synergies can be established:

- Between reputation and currency schemes: in particular, is it possible to use the rich semantics of reputation schemes and benefit from the apparently better adaptation of the currency scheme to self-organization?
- Between self-organized and authority-based trust management: since at one moment or another, mobile devices will be reconnected to a fixed (or mobile) infrastructure.

We plan in particular to develop protocols mixing a centralized management of reputation schemes like in the eBay auction system and a decentralized management through currency incentives or by allowing mobile deices to fetch reputation data based on a prediction of their future encounters. For instance, an infrastructure of offline stations may act as a repository for trust information and, based on current device mobility patterns, supply certificates to devices about other devices they are likely to meet. This would make it possible to avoid carrying too many credentials on a mobile platform, and instead develop heuristics for certificate look-up and fetching adapted to a given cooperative service.

2.4 Cooperation and added value

The proposal gathers researchers from three organizations: LAAS-CNRS (Toulouse), IRISA (Rennes) and Eurécom (Sophia Antipolis). The team at LAAS has extensive experience regarding computer security and fault tolerance applied to a wide spectrum of faults. They pioneered the notion of intrusion-tolerance in the mid-1980's. The participating researchers from IRISA have several years of hands-on experience with system-level support for mobile ambient intelligence applications. They are at the origin of the innovative notion of spontaneous information systems and have recently set up a joint competence center with Texas Instruments for deploying Java applications on mobile devices. The group at Eurécom has considerable expertise in the field of computer security and mobile computing. They have made several innovations regarding the use of reputation mechanisms in ad-hoc networks. We believe that the combined forces of these three experienced teams constitute a unique melting pot from which significant innovations will emerge.

The two planned themes of work will be developed as two co-advised PhD theses:

1. ***Fault Tolerance by Cooperative Backup***: this thesis will be co-advised by IRISA and LAAS. IRISA brings to this theme its experience on spontaneous information system architectures and ambient computing [I1, I2, I4], recovery-based fault tolerance [I4] and information gathering [I3]. LAAS contributes its expertise on fault-tolerance [L1, L2, L3], fragmentation-redundancy-scattering [L4] and state capture mechanisms [L5].
2. ***Trust for Cooperative Services***: this thesis will be co-advised by Eurécom and LAAS. Eurécom has a considerable relevant background on areas such as reputation mechanisms for ad-hoc routing [E1] and their validation using simulation or game theory [E2], and collaboration mechanisms based on history for trust relationship establishment (networks with infrastructure [E6], extended to offline use [E3, E4, E5]). In addition to the expertise mentioned above for theme 1, the relevant LAAS security expertise concerns authorization schemes [L6, L7] and role-based access control mechanisms [L8].

The PhD students will be located at one of the co-advising institutions (respectively LAAS for theme 1, and Eurécom for theme 2), but will spend approximately one month per year at the other institution. Joint two-day working meetings uniting all three teams are planned once every four months.

3 Intended results

Partie à rédiger en Anglais.

On détaillera l'échéancier des résultats et réalisations intermédiaires et finaux attendus. On précisera les risques scientifiques qui seront pris. On discutera de l'impact potentiel de ce projet sur les scènes européenne et internationale.

It is clear that the matters tackled by this project will be of tremendous interest in the next 5 to 10 years as portable devices of the type considered here become more and more common, and people tend to rely on them for organizing their life and their critical data. Being able to ensure the security and dependability of applications based on these devices is thus of prime importance.

The project revolves around actual PhD thesis work, with the budget for these theses included in the project's indirect funding. The results will be described in an intermediate report (and the projected PhD theses) and demonstrated through the joint implementation of an experimental platform.

Schedule of due dates:

- 18 months: report on dependability and security mechanisms adapted to self-organizing ephemeral networks of mobile devices, definition of experimental platform based on laptops and PDAs.
- 36 months: experimental platform of an architecture illustrating the use of the defined mechanisms – application to backup of critical data for mobile devices.

Since the planned research is exploratory, MoSAIC inherits the inherent risks of any long-term research project. Particularly challenging difficulties are:

- How to collect data backups from peer devices with which communication has been lost and how to reconstruct useful information from a potential sub-set of the backed-up data.
- How to establish trust relationships between mutually suspicious devices without any trusted third parties.

Through the teams participating in MoSAIC, the project will allow France to increase its impact during future European and other international projects. We envisage common international publications, as well as release to the scientific community of the results and software components of the developed demonstration platform.

4 References

On donnera ici les références bibliographiques citées dans la description scientifique

[AN02] J. Arkko, P. Nikander. "How to Authenticate Unknown Principals without Trusted Parties", In *Security Protocols Workshop*, (Cambridge, UK), 2002.

[BIK01] M. Blaze, J. Ioannidis, A. Keromytis. "Offline Micropayments without Trusted Hardware." In *Financial Cryptography 2001*. Grand Cayman, February 2001.

[BB01] Sonja Buchegger, Jean-Yves Le Boudec. "The Selfish Node: Increasing Routing Security in Mobile Ad Hoc Networks". IBM Research Report RR 3354, May 2001

[BI03a] M. Boulkenafed, V. Issarny. "A Middleware Service for Mobile Ad Hoc Data Sharing, Enhancing Data Availability", In *4th ACM/IFIP/USENIX International Middleware Conference*, (Rio de Janeiro, Brazil), LNCS, 2672, pp.493-511, Springer, 2003.

[BI03b] M. Boulkenafed, V. Issarny. "AdHocFS: Sharing Files in WLANs", In *2nd Int. Symp. on Network Computing and Applications*, (Cambridge, MA, USA), pp.156-63, IEEE CS Press, 2003.

[CS01] G. Cao, M. Singhal. "Mutable Checkpoints: a New Checkpointing Approach for Mobile Computing Systems", *IEEE Transactions on Parallel and Distributed Systems*, 12 (2), pp.157-72, February 2001.

[DLRS02] B. Dahill, B.N. Levine, E. Royer, C. Shields. "A Secure Routing Protocol for Ad Hoc Networks". In *10th Conference on Network Protocols (ICNP)*, November 2002.

[EFL99] C.M. Ellison, B. Frantz, B. Lampson, R. Rivest, B.M. Thomas, T Ylönen. "SPKI Certificate Theory – RFC 2693". September 1999.

[ITU88] ITU-T. "Recommendation X.509: The Directory – Authentication Framework", 1988.

[KKA03] A. Khalili, J. Katz, W. A. Arbaugh. "Toward Secure Key Distribution in Truly Ad-Hoc Networks", In *Symp. on Applications and the Internet Workshops (SAINT'03 Workshops)*, pp.342-46, 2003.

[LSB03] S. Lee, R. Sherwood, B. Bhattacharjee. "Cooperative peer groups in NICE". In *INFOCOM'03*, April 2003.

[LNS03] D. Liu, P. Ning, K. Sun. "Efficient Self-Healing Group Key Distribution with Revocation Capability", In *10th ACM Conf. on Computer and Communications Security (CCS'03)*, (Washington D.C., USA), pp.231-40, 2003.

[McC01] Jim McCoy. "Mojo Nation Responds". http://www.openp2p.com/pub/a/p2p/2001/01/11/mojo.html.

[Mnet] Mnet, http://mnet.sourceforge.net.

[N00] P. Nikander. "Fault Tolerance in Decentralized and Loosely Coupled Systems", In *Ericsson Conference on Software Engineering*, (Stockholm, Sweden), Ericsson, 2000.

[PH02] P. Papadimitratos, Z. J. Haas. "Secure Routing for Mobile Ad hoc Networks", In *SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS 2002)*, (San Antonio, TX, USA), 2002.

[PKV96] D. K. Pradhan, P. Krishna, N. H. Vaidya. "Recoverable Mobile Environment: Design and Trade-off Analysis", In *26th IEEE Int. Symp. on Fault-Tolerant Computing (FTCS-26)*, (Sendai, Japan), pp.16-25, IEEE CS Press, 1996.

[PR02] C. Pedregal-Martin, K. Ramamrithan. "Support for Recovery in Mobile Systems", *IEEE Transactions of Computers*, 51 (10), pp.1219-24, October 2002.

[PS96] R. Prakash, M. Singhal. "Low-Cost Checkpointing and Failure Recovery in Mobile Computing Systems", *IEEE Transactions on Parallel and Distributed Systems*, 7 (10), pp.1035-48, October 1996.

[PWY01] T. Park, N. Woo, H. Y. Yeom. "An Efficient Recovery Scheme for Mobile Computing Environments", In *Int. Conf. on Parallel And Distributed Systems (ICPADS)*, (KyongJu City, Korea), pp.53-60, IEEE CS Press, 2001.

[YSF99] B. Yao, K.-F. Ssu, W. K. Fuchs. "Message Logging in Mobile Computing", In *29th IEEE Int. Symp. on Fault-Tolerant Computing (FTCS-29)*, (Madison, WI, USA), pp.294-301, IEEE CS Press, 1999.

[ZA02] M.G. Zapata, N. Asokan. "Securing Ad Hoc Routing Protocols". In *ACM Workshop on Wireless Security (WiSe 2002)*, September 2002.

[ZH99] L. Zhou, Z.J. Haas. "Securing Ad Hoc Networks". *IEEE Network Magazine*, 13(6): 24-30, November/December 1999.

5 Bibliographical references of the researchers involved in the project

Pour chaque (enseignant-)chercheur participant, lister de 3 à 5 publications, logiciels ou brevets les plus significatifs, en relation avec la thématique du projet proposé.

[E1] P. Michiardi, R. Molva. "Core: A Collaborative Reputation Mechanism to Enforce Node Cooperation In Mobile Ad Hoc Networks", In *6th IFIP Communications and Multimedia Security Conference*, (Portorosz, Slovenia), September 2002.

[E2] P. Michiardi, R. Molva. "Game Theoretic Analysis of Security in Mobile Ad Hoc Networks", In *WiOpt Workshop*, Mars 2003, Best Student Paper Award.

[E3] L. Bussard, Y. Roudier, R. Molva. "Untraceable Secret Credentials: Trust Establishment with Privacy". In *Workshop on Pervasive Computing and Communications Security (PerSec'04) at PerCom 2004*, (Orlando, FL, USA), March 14-17, 2004.

[E4] L. Bussard and R. Molva. "One-time Authorization for Off-line Interactions". In *PerCom 2004*, (Orlando, FL, USA), March 14-17, 2004.

[E5] L. Bussard, R. Molva, Y. Roudier. "History-Based Signature or How to Trust Anonymous Documents". In *2nd International Conference on Trust Management (iTrust 2004)*, (Oxford, UK), Springer Verlag, 2004.

[E6] L. Bussard, Y. Roudier, R. Kilian-Kehr, S. Crosta. "Trust and authorization in pervasive B2E scenarios". In *6th Information Security Conference (ISC 2003)*, (Bristol, UK), October 1st-3rd, 2003.

[E7] L. Bussard, Y. Roudier. "Embedding distance bounding protocols within intuitive interactions." In *1st International Conference on Security in Pervasive Computing (SPC'2003)*, (Boppard, Germany), March 12-13, 2003.

[L1] J. Arlat, Y. Crouzet, Y. Deswarte, J.-C. Laprie, D. Powell, P. David, J.-L. Dega, C. Rabéjac, H. Schindler, J.-F. Soucailles. "Fault Tolerant Computing", In *Encyclopedia of Electrical and Electronic Engineering* (J. G. Webster, Ed.), 7, pp.285-313, Wiley-Interscience, 1999.

[L2] D. Powell (Ed.). *A Generic Fault-Tolerant Architecture for Real-Time Dependable Systems*, 266p., Kluwer Academic Publishers, Dordrecht, 2001.

[L3] J.-C. Ruiz, M.-O. Killijian, J.-C. Fabre, P. Thévenod-Fosse. "Reflective Fault-Tolerant Systems: From Experience to Challenges", *IEEE Transactions on Computers*, 52(2), pp. 237-254, 2003.

[L4] Y. Deswarte, L. Blain, J.-C. Fabre. "Intrusion Tolerance in Distributed Systems". In *IEEE Symposium on Security and Privacy*, (Oakland, CA, USA), pp. 110-121, IEEE CS Press, 1991

[L5] M.-O. Killijian, J.-C. Ruiz, J.-C. Fabre. "Portable Serialization of CORBA Objects: a Reflective Approach", In *17th ACM Conference on Object-Oriented Programming, Systems, Languages, and Applications (OOPSLA'02)*, (Seattle, WA, USA), pp. 68—82, ACM Press, 2002.

[L6] E. Totel, J.-P. Blanquart, Y. Deswarte and D. Powell, "Supporting Multiple Levels of Criticality", In *28th IEEE Int. Symp. on Fault-Tolerant Computing (FTCS-28)*, (Munich, Germany), June 1998, pp.70-79.

[L7] Y. Deswarte, N. Abghour, V. Nicomette and D. Powell, "An Internet Authorization Scheme using Smart Card-Based Security Kernels", In *International Conference on Research in Smart Card (e-Smart 2001)*, (Cannes, France), LNCS 2140, pp.71-82, Springer Verlag, 2001.

[L8] A. Abou El Kalam, Y. Deswarte. "Security Model for Health Care Computing and Communication Systems", In *Security and Privacy in the Age of Uncertainty, 18th IFIP Int. Conf. on Information Security (IFIP/Sec'2003)*, (Athens, Greece), pp.277-88, 2003.

[I1] M. Banâtre, F. Weis. "SIS a New Paradigm for Mobile Communication Systems". In *IST 99*, (Helsinki, Finland), November 1999.

[I2] P. Couderc, M. Banâtre. "Ambient Computing Applications : an Experience with the SPREAD Approach". In *HICSS*, (Hawaii, USA) January 2003.

[I3] D. Touzet, P. Couderc, J.M. Menaud, F. Weis, M. Banâtre. "Side Surfer: Enriching casual Meeting with Spontaneous Information Gathering". In *ACM SigArch Computer Architecture Newsletter*, 29 (5), December 2001

[I4] P. Couderc, M. Banâtre. "SPREADing the Web". In *Personal Wireless Communication (PWC 2003)*, (Venice, Italy),. September 2003.

[I5] M. Banatre, G. Muller, M. Hue, N. Peyrouze, B. Rochat. "Lessons from FTM: an Experiment in the Design and Implementation of a Low Cost Fault Tolerant System", in *IEEE Transactions on Reliability*, 45, pp. 332-340, June 1996.