Trusted Ambient community for self-securing hybrid networks

Véronique Legrand, D. Hooshmand, Stéphane Ubéda

INRIA

INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Trusted Ambient community for self-securing hybrid networks

V. Legrand — D. Hooshmand — S. Ubéda

N° 5027

Decembre 2003

THÈME 1

ISSN 0249-6399 ISRN INRIA/RR--5027--FR+ENG

Trusted Ambient community for self-securing hybrid networks

V. Legrand* , D. Hooshmand , S. Ubéda†

Thème 1 — Réseaux et systèmes
Projet ARES

Rapport de recherche n° 5027 — Decembre 2003 — 21 pages

Abstract: An ad-hoc network is a group of wireless terminals that possess the ability to automatically organise themselves into a radio network, in which each terminal can perform the duties of both end node as well as router. A network so formed has the particular characteristics of being dynamic by nature, being inherently incapable of relying on any pre-existing infrastructure or centralised administration system as well as being unique in that it uses Hertzian transmission with air as its medium.

This ad hoc communication capacity, together with multi technology support and more classical cellular access to networks - or to the Internet - is the fundamental network architecture for what is nowadays called *Ambient Networks*. This architecture is sometimes denoted hybrid networks. These are the characteristics that render hybrid networks particularly vulnerable to attack. The security models employed in other infrastructure based networks (wireless or otherwise) are inapplicable in ad hoc networks, due to their design based on the fundamental principle of a reliable, fixed trusted third party or an established addressing system. We propose, in this paper, a solution that addresses the specific needs of ad hoc networks.

First, we describe the paradox presented by the contrasting needs for mobility as well as strong security in ad hoc / hybrid networks. Second we describe our proposed solution, a ***trust seed***, which uses the concept of trust transmission to form a mobile version of an infrastructure: an ***ambient community***. As the ambient community grow in terms of members, the trust seed becomes capable of distributing trust to more and more entities. However, the originality of our contribution resides in the proposition of a new key agreement protocol, conceived to distribute a secret between ad-hoc nodes without ever transmitting it via a non-secure channel, and without any prior configuration. We conclude the document

* veronique.legrand@insa-lyon.fr
† stephane.ubeda@insa-lyon.fr

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier (France)
Téléphone : +33 4 76 61 52 00 —Télécopie +33 4 76 61 52 52

by presenting some perspectives that will allow us to further our work and approach the concept of adaptive trust and ambiances.

Key-words: hybrid networks, security, self organization.

Notion d'ambiance pour la sécurité des réseaux hybride

Résumé :

Un réseau ad hoc est composé d'un ensemble de terminaux sans fil capables de s'organiser pour constituer un réseau radio, dans lequel ils jouent chacun le double rôle de nœud et de routeur. Cet ensemble ainsi formé constitue une géométrie fortement dynamique sans possibilité d'appui sur une infrastructure ou une administration centralisée. Les échanges sont basés sur les technologies de transmission hertzienne, et l'air devient le vecteur de propagation. Ce sont ces caractéristiques, nœuds/routeurs, forte dynamique, absence d'infrastructure, et enfin l'interface air qui rendent les réseaux ad hoc particulièrement vulnérables.

Les modèles de confiance, éprouvés dans les autres réseaux filaires ou sans fil en mode infrastructure, sont inopérants pour de tels réseaux parce que ces modèles sont construits pour employer comme référence un tiers de confiance ou un système d'adressage stable. Ces réseaux ne disposent donc pas de protocoles de confiance adaptés à leurs spécificités.

Ce rapport propose une solution pour un environnement couplant des terminaux aux capacités de communications en mode ad hoc, avec des communications de type cellulaire : c'est ce que nous appelons un réseau hybride. Après un rapide état de l'art dans le domaine de l'établissement de la confiance dans les réseaux ad hoc, nous détaillons notre solution. Notre architecture est basée sur la notion de *germe de sécurité*, un ensemble d'informations et d'algorithmes, permettant de construire une notion d'*ambiance*, c'est-à-dire de nœuds en accord sur un niveau de sécurité commun. L'orignalité de notre approche réside dans la capacité de ce protocole à générer une clé de session sans transmission de partie de la clé sur un canal non sécurisé.

Mots-clés : réseaux hybrides, sécurité, auto-organisation

1 Introduction

Wireless communications are rapidly becoming a critical aspect of computer networks, and offer open solutions for providing mobility, even essential network services where wire installations are unfeasible. More and more portable devices are seen equipped with communication capabilities, of which the dominant species are those that use radio transmission. The number of mobile phones has also increased significantly, and the combination of a standard 2G/3G interface with short range radio capacities is rapidly becoming commonplace. The phone terminal that was the centre of a Personal Area Network will remain a major device in an environment where many objects will play similar roles. This concept is what some authors already call "'fourth generation networks"' [16]. Finally, we observe that networks are becoming ubiquitous, and that communication and computing are both becoming increasingly personal.

In such a context, the communication capabilities of smart objects will not be restricted simply to accessing fixed networks, rather, their peer-to-peer communication capabilities will necessarily receive more attention. Devices within radio range can potentially establish self-organised networks of two or more objects. Mobility during the use of more complex services is becoming commonplace, and is addressed by means of ad-hoc communication capabilities. In this paper, this capability means that when two nodes are out of radio range, other devices can be used as relays through an ad-hoc routing service. Mobile users can join or leave the ad hoc network at any time, and the dynamically changing topology is handled in a distributed manner. Terminals in these networks can play the role of routers that discover and maintain routes to other nodes belonging to the network. Since the early days of research into ad-hoc networks in the 1970s, numerous protocols have been developed for ad-hoc routing. Most of them fall into one of two categories: (1) demand driven or reactive protocols, where routes between specific nodes are created only when desired and maintained only for the duration of the communication, and (2) table driven or proactive protocols, where nodes of the network attempt to maintain consistent, up-to-date routing information.

The notion of communicating objects and ambient networks, in which interactions between network elements are spontaneous and transparent ot the end user, significantly complicates the deployment of services. Security is the most important basic service to offer if we want such an approach to become a reality. The lack of fa ixed framework is already a strong constraint in building a security architecture, and so the self-organised aspect is probably a much more restricting constraint. In an environment where every user is the administrator of their own terminal and the associated services that their terminals provide, security could be seen as impossible to build between a collection of inherently untrustworthy nodes. Solutions for security in ad-hoc networks are essentially peer-to-peer solutions, and centralised trusted agents are inherently unsuitable.

Wireless ad-hoc networks are by nature very vulnerable to various forms of attack. First and foremost, wireless links are exposed to attacks that take advantage of the medium itself, ranging from passive eavesdropping to active radio interference. Classical problems include the leaking of secret information, message contamination and node interposition, otherwise

known as man-in-the-middle attacks. The most important security holes, however, stem from the decision-making processes that are by nature decentralised and based entirely upon cooperative algorithms.

Trust is an important element of any security architecture, particularly in such an environment where the active compromisation of nodes is a real threat. Many existing works on specifically ad-hoc security management assume a pre-existing trust relationship. This assumption can be acceptable in a large range of potential applications - such as military contexts - but does not correspond to the most common scenarios that one would come across in everyday life. In ambient networks, whether comprised of devices having ad-hoc capabilities or not - the term used to define security is *context awareness*. "Ambient awareness is the process of a personal computing device in acquiring, processing and - in the background, possibly unattended by the user - acting upon application-specific contextual information, taking the current user preferences and state of mind into account"' [13].

In this paper we propose a trust management scheme matching this definition of context awareness. The solution does not make any assumptions concerning the presence of any fixed infrastructure (the terminal can be in full ad-hoc mode), while the proposed architecture could take advantage of any encountered access points to contact fixe servers. We believe that trust cannot be attributed a Boolean value (trusted terminals versus compromised terminals), but must entail various levels of trust belonging to various levels of offered services. For example, a smart device equipped with a web cam can probably offer the ad-hoc routing service to most of the nodes in its environment as long as the behaviour of the nodes is not suspicious. The same device could allow terminals attributed with slightly more trust to access the video flux. And the same terminal will probably require a strong level of trust before allowing a foreign node to access the web cam's configuration interface. Trust is created starting from a low level, and grows during the establishment of what we term an ambient community. We propose an architecture based on self-organised communities of terminals with simple mechanisms to accept nodes in an existing ambient community, to establish the appropriate levels of trust, and also to reject or detach a suspicious node. Our solution is a mixture of context awareness and recommendation schemes. The basic mechanism is based on the notion of *node history*, which is used to build a specific shared secret. Then, nodes aggregate when exchanging data and services into an ambient community, which is the ultimate level of organisation.

In this paper, Section Two presents the view of the network architecture that we imagine. The notion of a hybrid network and the capability constraints of nodes in such a context are discussed. Mobility management is clarified and basic pre-supposed security concepts are also described. A large part of the section is devoted to the notion of a node's *history* in a hybrid environment. Section 3 describes all the mechanisms necessary to build trust between two nodes, as well as between a node and a pre-existing ambient community. Specific cases, such as that of a ***long-lost node*** (i.e., a node that has been accepted by the ambient community in the past and that has returned) are also addressed. Section Four will include our notion of ambient communities in a global security architecture - with other concepts like the imprinting of nodes, and gives a discussion on the applicability of the resulting

architecture. At the end of the paper, a conclusion is given together with some possible future developments that are envisaged with relation to the ambient community concept.

2 Previous work

Trust is a key issue of networks of the future, which will include ad-hoc networks both in themselves through to their application in the eventual Ambient Internet. However, it is difficult to imagine how one might be able to provide useful services in this new framework without somehow guaranteeing its future users their privacy, their confidentiality and the integrity of their information. In such a dynamic network environment, it will ultimately be the role of each network node to adapt itself to its changing environments, a concept which will in itself entail a new and more detailed set of exchanges and network structures than those currently used. It will clearly require new paradigms, in which trust will be an unavoidable element.

Current trust models address this situation with a centralised hierarchy that guarantees authenticity, at the cost of imposing the need for services that must be provided by a reliable trusted third party. However, such architecture is incompatible with the concepts on which ad-hoc networks are founded, and so a more specifically suitable model must be found. Note that in the ad hoc framework, it has been shown that security models based on trusted third parties - suck as PKI - are not sufficiently flexible nor scalable. New models of both certificates as well as architectures are proposed, including the Simple Distributed Security Infrastructure [19]and Simple Public Key Infrastructure [9].

In addressing this problem, we have analysed currently used trust models in legacy networks. Trust is established on the foundation of common knowledge that each party can verify, traditionally a shared secret. In wireless networks all transmitted data can be intercepted, and so hybrid schemes that incorporate both the secure advantages of asymmetric cryptography as well as the efficiency and strength of symmetric cryptography are often used. Asymmetric key cryptography is ideal for guaranteeing authenticity, since in encrypting data with a public key one can be sure that only the possessor of the corresponding private key will be able to decrypt it [8]. The question of how to be sure of the association of a public key with one identity is what has driven us towards the notion of a *trust seed* associated with one entity, with semi-autonomous mechanisms that allow seeds to interact with each other as trust is established between nodes, developing their trustworthiness as more and more interconnected bonds are established.

Evidently, the question of how to establish a trust network in ad hoc environments has been addressed by current research, and while we are not satisfied that any suitable framework has been established, the concepts proposed have solved some questions and brought up others. The end of the section presents some existing solutions.

2.1 The Distributed CA Model

In this model [23], rather than attributing the responsibilities to one node, an ad-hoc certification authority is established between the spontaneous members of an ad-hoc network to govern the certificate services described above. This CA is governed by a quorum of n nodes representing the member nodes of the network, the private key of the CA being evenly distributed between the nodes, using a threshold cryptographic algorithm [21] that requires $t+1$ nodes (a quorum) to cooperate and provide $t+1$ out of n individual shares of the private key in order to form the entire key. An attack may therefore be made on up to t nodes without revealing the value of the secret. The key is then formed from the pieces by an elected combiner node in the network, which uses it to provide certification services, such as signatures or authorisation. Furthermore, the partial secrets distributed between the nodes are updated on a regular basis, so as to confound attacks that take place over long periods of time.

Though interesting, the model lacked definition in some degrees. Firstly, the obvious weakness is that were a combiner node to be attacked or its identity spoofed by an attacker, the key could either be obtained or falsified by a spoofing node. This problem was addressed in a later document, the COCA protocol [24], which required a quorum of combiners, to each form their own CA key from partial secrets. The combiners, too, were described as being inherently more stable and trustworthy. However, this latter approach was not oriented towards ad-hoc networks, being primarily drastically more exigent in its network resource consumption - the number of data requests would increase proportionally to the square of the number of trusted combiners. Secondly, the placement of a higher degree of trust and the relying upon a number of servers as *stable combiners* is not coherent with the spontaneity of ad-hoc networks. Another problem that this model had was that it was not scalable - one network key would be distributed to one quorum of members of a global CA, and the quorum nodes or combiners would always have to be mutually accessible. Furthermore, the certificate used a X.509 structure, which we have shown to be unsuitable for ad-hoc networks, due to its reliance on fixed services and network attributes.

2.2 The Neighbourhood CA Model

This model [15] shares some elements with that proposed by Zhou - both use threshold cryptography in order to distribute a CA key between members of a local ad-hoc CA that provides the same services as an infrastructure CA. However, Kong's model differs fundamentally in structure to the model proposed by Zhou in that there are several, possibly many certificate authorities, all addressing only their immediate neighbourhoods. Furthermore, since the CAs' domains of authority are restricted only to their immediate neighbours, the key is broken up between all N members of the neighbourhood, with K portions necessary to reconstitute the key. Thus, K = 1 would effectively configure the network for a centralised CA (with all its associated disadvantages), whereas setting K = N would implement the strongest safeguard possible, at the cost of requiring every node in the CA to be constantly

contactable. It is of note that a node could also belong to several CAs - for example, one to its north, and one to its south.

In order for a node to address the CA, it formulates a request, using a fixed identifier, such as a hardware address. A coalition of K nodes is formed on the fly (according to unspecified criteria), from which a combiner is chosen to process the partial secrets. The identity of the newcomer, however, must be verified by using *out of band* means - using a certificate provided beforehand by an external, trusted CA. If the node is accepted, it must necessarily become a member of the CA, and so the secrets are shuffled, joined and redistributed between the new group including all members, both old and new.

This model also leaves some questions unanswered. For example, if authentication services are only provided locally, trust can only be established on a hop-by-hop basis, which may ultimately be unsatisfactory. It would mean that a highly secure transaction could not take place on a low security network, for it would only take one *bad seed* along the routing path for all security to be lost. Furthermore, the reliance upon a hardware identification code opens the system to hardware spoofing, and the reliance on an external CA for any kind of authentication is fundamentally undesirable.

2.3 The Terminodes Project

This project, to be completed by 2010, is based on a network of entities that behave both as network nodes and routers in a CDMA-based radio environment. Thus, they perform endpoint terminal services as well as routing services. Similar terminodes are collected into communities of one sole hop, similar to both Kong's model as well as cellular phone networks, and identification is based on burnt-in hardware MAC addresses and eventually IPv6 addresses as well. However, aside from suggesting community based implicit key authentication services [11] or identity-based systems [10], no final answer is provided with regards of the network's security. Nevertheless, an interesting concept was introduced in an associated paper based on the same project [4] that was designed to combat the important problem of the intentional misuse of network services, primarily (a) overuse or flooding, and (b) failure to forward or provide other services, by the use of *nuglets*, a form of *network currency* used as incentive to be both conservative in network usage as well as to provide essential network services such as routing.

In [12], a distributed key management model is used, based on the concept introduced by PGP of users storing and signing certificates in their own repositories. However, in contrast to the PGP system, their model does not rely on centralised servers for the distribution of certificates. In order for device a to establish a trust level with device b, they merge their certificate repositories, and a attempts to find a chain of trust between the two. Furthermore, a scalable model is established in which the probability that a chain will exist in the merged repository is high. Trust, therefore, is established between devices via intermediaries, and what is formed is termed a *trust graph*, where trust between all network nodes is illustrated as links of peer-to-peer connections.

This system is well adapted to ad-hoc networks in that it captures the ad-hoc spirit well, even if not perfectly scalable due to individual trust paths having to be calculated for every node.

2.4 Zero knowledge authentication

Zero knowledge authentication is not a recent concept, having been established in the past in the guise of a variety of algorithms for determining whether the two parties wishing to verify each other's identity do indeed possess the common identifier (a password or otherwise) or not by only divulging information that would be computationally secure in preventing an attacker from determining the secret from which it was generated. In the context of ad-hoc networks, however, zero knowledge systems are characterised as being protocols that allow the establishment of a strong trust and security on the foundation of a possibly weak secret. The idea presented by [2] is to establish a group-wide secure channel by using a weak secret key - for example, a password distributed on paper in a meeting. The interest of the protocol is that it is a group zero authentication protocol, rather than a peer-to-peer one. Based on encryption using the shared password, a series of exchanges involving public keys, random challenges and responses assist in finally establishing a session encryption key. The two drawbacks of this protocol are that (1) a secret needs to be shared - though its value will ultimately not affect the final security of the session, and that (2) the fact that public keys are immediately encrypted by the secret key in the first phase of the transactions implies that in order for the operations to be unique, the public keys encrypted should change every time. This is impractical as well as being computationally inefficient.

2.5 Recommendation protocols

Recommendation protocols are based on the analysis of the establishment of trust in social, political, economic and other human communities.

The *distributed trust* model [1] describes a distributed recommendation protocol based on transactional trust. The mechanism interoperates between chains of nodes, and for this reason is suitable for the propagation of trust information within distributed architectures. In this model, exchanges are effectuated between two entities, named agents, described as being responsible for their own fate, and able to choose their own trust policies. They can consequently transmit an opinion on the quality of their trust policy, termed a recommendation. A table of reputations for each network entity (both with regards to the entity themselves as well as the trust placed in their recommendations), is combined with an algorithm (a function described in [3]) in order to obtain the overall trust value for a target using any given recommendation path. Trust refreshings enable trust both to be augmented as well as revoked entirely from one node, and the mechanisms described in the protocol allow such refreshings to propagate along the same paths along which the recommendations were propagated in the first place.

However, it should be noted that the revelation of trust information will encourage malicious usage - an attacker would more willingly attack a node in which a lot of trust

has been placed. Since these transmissions are open, it presents a weakness in the protocol. Otherwise, this scheme is suitable for ad-hoc networks due to its distributed and user-centred design, in that trust policies are managed by the owner.

3 Elements of networks architecture

The notion of an Ambient Community that we present in this paper is part of a global project to build an ambient network based upon terminals, a major capability of which will be ad-hoc networkability. Firstly, describe the architecture of what we describe as being a hybrid network [6], as some of its aspects will have an impact on the establishment of secure communication between nodes. Secondly, we will describe the elementary services that we assume to be present for our approach, notably mentioning the particular feature of the history of a terminal in such an environment. This notion is required to build common data bases, which will aid in building shared secrets with an associated level of trust. However, this concept is not described in detail as it is not intended to be the primary focal point of the paper, and the subject is left open to further investigation.

3.1 Hybrid networks

An ad-hoc network consists of a set of mobile terminals that possess wireless communication devices. Since an ad-hoc network is characterised by the absence of a backbone, most of the advanced network services are difficult to build. The infrastructures must be emulated, and services have to be obtained through the means of distributed elementary services [20]. The routing paradigm is the main factor driving the design of a network. The most elementary service that must be present in an ad-hoc network is the routing scheme. Ad-hoc routing schemes have been broadly studied in the past [17], and the IETF's MANet group propose an architecture in which the basic element is the MANet node - in contrast with an ad-hoc node, which is relatively unrestricted in comparison. According to the IETF's description, "'a MANet node principally consists of a router, which may be physically attached to multiple IP hosts (or IP-addressable devices), which has potentially multiple wireless interfaces - each interface using a different wireless technology"' [7]. Packets travel from node to node using an IP-level routing mechanism. Two families of routing protocols are debated upon in the MANet group, one called demand-drive or reactive protocols, in which routes between specific nodes are created only when required and are limited to the duration of the communication, and the other called table-driven or proactive, where nodes of the network attempt to actively maintain consistent, up-to-date routing information.

What we mean by *network architecture* is set of rules and mechanisms that allow the implementation of services and to enable networking. By *hybrid network architecture*, we refer to ad-hoc networks with the addition of several basic features. Firstly, we assume the presence of multiple network access in technologies in the hardware - a reasonable assumption considering the current trend of mobile devices being equipped with both WiFi and Bluetooth hardware, and sometimes even a 2G/3G connection. In the standard IP scheme,

an IP address is a link to an interface - a concept that is not very useful in the identification of a terminal. We will work with the supposition, therefore, that there exists some solution at the ad-hoc level [6] or by the use of IPv6 as in [5]. When in hybrid architectures, we also consider access points to be part of ad-hoc networks, playing the role of Internet access points. Merging the ad hoc capability with more classical cellular solutions has been studied and solutions exist that include Internet access in the ad hoc routing scheme when a access point is within reach [5, 14].

In summary, our notion of a hybrid network architecture defines each terminal as having an identity which may neither be persistent, nor secure. This identity is used for routing within the ad-hoc network, and may be linked with an IP address in order to reach the Internet. We also assume that a local broadcast scheme is present as well as a flooding scheme (non-local broadcast) that can be controlled, i.e. limited by parameters such as the number of hops or certain node characteristics.

3.2 Advanced hybrid network services

In this paragraph we describe the services required to set up the security architecture that we propose. Firstly, our security model is user-centred, and is based around the idea of a monadic user moving between terminals. We use the notion of a *trust germ* to set up trust between terminals, and so the establishment of trust between two users on two terminals becomes based on the common histories of the user-terminal couplings. This personal information on the terminal is assumed to be securely linked to one exclusive user of the terminal - so the two are considered one secure entity. This is envisioned ultimately to be a secure transient association, known as device imprinting [22]. We make no assumption regarding the trustworthiness of the owner of the terminal, but do assume that if trust is accorded to a terminal, then the imprinting of a user to a terminal can also be trusted.

The next subsection is devoted to the kind of information that a trust germ should contain in order to be able to effectively establish trust. We assume, at the very least, that the germs contain some public/secret key pairs (and the associated algorithms) that can be used by the network architecture to establish secure paths between nodes using asymmetric cryptographic techniques. This feature will be used to develop the Common History Exchange Protocol which is used as the basis in the setup of an Ambient Community.

3.3 Seed of trust of an terminal in an hybrid network

In our approach, each terminal has what we call a Seed of Trust. This seed is composed of an Algorithms part and a Knowledge part. At the *birth* of a smart device, the knowledge part is more or less empty. In fact, it can be initialised during the device's *birth* process with some very general information regarding its birth: date, country, company and so on. We will explain the information involved further along. The next step of reinforcement of the Knowledge part will occur when a user takes control of the smart device. This can be done with a process known as imprinting, which was studied in [22]. This operation is very important and has to be performed securely, though its details are beyond the scope

of this paper. We assume that the user and terminal are somehow linked, i.e. we will not differentiate between a user and their smart device.

The knowledge of a node will be reinforced with the notion of *history*. Each important event along the life of a node will be associated with some secure information and saved in the knowledge part of the seed of trust. We don't want to go too far in defining what kind of information could be relevant, although one could evisage such information as the IDs of encountered nodes, recently used access points (recalling that we are considering hybrid networks as well as just ad-hoc networks), elements pertaining to certified software, and so on. The duration of validity of that information is also something that should be studied.

It is easy to say that information would have different values depending on how it were obtained. The value of information originating coming from birth or imprinting will be very high. Elements of certified software or elements obtained through standard fixed network security concepts obtained via an access point will be of a medium level. Information obtained when exchanging data with other nodes in ad hoc mode should be considered less important. Again, this analysis is beyond the scope of this paper. We only bear in mind that the more securely the information is obtained the higher the value associated in the knowledge part of the seed of trust.

This seed of trust will be used spontaneously to build common secrets between nodes and to derive a value N corresponding to the Trust Level between these two nodes [18]. This process is described and analysed in the next section. The principle is very simple, requiring a statement such as "'I can strongly trust a node that has in its history records of prior interactions with 3 nodes present in my personal history, that has used 2 certified software packages that I have also used, that comes from the same country, that has a user with the same accreditation level in the same bank as me and that regularly visits the same cyber café"'. Naturally this is only an example and specific studies should be conducted depending on the usage context.

Our model uses this seed of trust and the idea that trust is only transitive. The seed of trust is the vector of trust transmission in the network and it is supported dynamically by the notion of an Ambient Community that corresponds to a group of nodes having the same Trust Level N.

The Algorithm part of the seed of trust is composed of standard processes such as MD5 and the Diffie Hellman cryptographic package. These algorithms are required in order to generate certificates and to encrypt exchanges. There is also list of processes specific to our model. The two major algorithms are the Common Knowledge Exchange algorithm which extract the common knowledge from two knowledge lists, and the Trust Engine which take as its input the result of the CKE from which it computes the Trust Level N. We can imagine this Trust Engine as a Trust Policy that can vary depending on the context. Those algorithms are accompanied by elementary algorithms used to manipulate date: the Data Engine. The last element of the seed is a unique ID of the user/terminal and a Secret Key Ks and an associated public key Kp to set up asymmetric cryptographic processes.

Finally, we assume that each element of the Knowledge part of the seed of trust is certified and thus has a fingerprint. During the establissement of trust, only the public part of the

knowledge is sent to the newly encountered node. This drasticaly reduces the possibilities of man-in-the-middle attacks. In the table 1, we summarise the attributes of a element of knowledge. Of course, those general attributes may be further specified with more sepcific information. The figure 1 summarises the information included in the seed of trust. This seed of trust will be noted $< ID, K_s, K_p, K_n >$.

Identity	Node ID, IP address, Package ID...
Trust Level	associated with this specific information
Date	of assimilation into the Seed
Duration	before expiration
Public Key	if one exists
Fingerprint algorithm	e.g. MD5
Signature	for certification

Table 1: Certificate Information in Seed of Trust

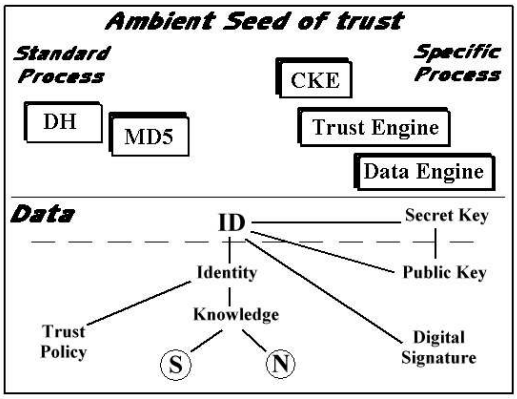

Figure 1: Seed of trust information model - this must be securely stored on the terminal (a smart card could be used).

4 The Trust Ambient Communutity model

Authentication is the core requirement for integrity, confidentiality and non-repudiation, none of which can be set up without a trust management tool between terminals. Though basic trust features will be based on one-to-one exchange protocols, most existing work uses the notion of distributed security services. In those approaches, a collection of nodes is grouped in order to build an *authority* of some kind. In ad hoc networks, the high dynamicity

of the topology strongly induces the need for automatic group organisation. Therefore, security policy outside of *military contexts* need not be too restrictive if spontaneous exchanges are ever to occur!

In the Trusted Ambient Community model, nodes will spontaneously group in communities based on the rule that *a friend of my friend is a friend of mine.* Since the TAC model allows for the quick establishment of communication, only weak trust is required for initialisation. The TAC Model introduces the notion of different trust levels, and so naturally the level of services between two nodes at the weakest trust level will be very poor - possibly only ad hoc routing and other basic network services. The nodes consolidate their trust level during data exchanges or when the nodes are idle at the application level. This consolidation operation is based on the collective *history* of the nodes, this history denoted as knowledge of the node. Each node implementing the Trusted Ambient Community modelis supposed to have an ID associated with a secret key and a public key. This information, together with the Knowledge is denoted as a Seed of Trust: $< ID, K_s, K_p, K_n >$ (see 3.3). The intialisation of interaction between two nodes begins with the Common Exchange algorithm which is described below.

4.1 Common Knowledge Exchange algorithm

The principle of the Common Knowledge algorithm is the following:

- Two ad hoc terminals discover each other in an non secure environment.
- During an initial phase the terminals exchange their public keys K_p. One of the nodes is the initiator (the one sending the request packet) and the other is the receiver. Note that only the public key of the initiator has to be sent in plaintext while the one pertaining to the receiver can be encoded using the public key of the initiator.
- Next, terminals exchange all or part of their personal Knowledge K_n using an asymmetric cryptographic algorithm. Only the public parts of the each element of knowledge are sent at this point of the algorithm (information without their associated fingerprints).
- Using a specific algorithm, common knowledge is determined and built independently on each terminal. The elements of the common knowledge are completed with their fingerprint (no more exchanges are need to do so) and a common secret is build in parallel on each side
- Nodes exchange the generated common secret to verify the identity of both.
- Depending on the size and the quality of this common knowledge, an initial Trust Level is established between the two nodes.
- In further exchanges, the knowledge already sent to a specific node can be consolidated by new elements (because not all the knowledge was not completely transferred or because the personal knowledge of a node has been reinforced by its recent activity).

- A group of nodes with a sufficient common knowledge will be a group in an Ambient Community.

This process is what we call the Common Knowledge Exchange (CKE) algorithm. In the next paragraph we will discuss possible scenarios of terminals encountering one another and how the CKE is applied. The use of Ambient Communities will be discussed in the last paragraph of this section.

4.2 Encounter scenarios and trust management

When two nodes interact with each other in the TAC Model, we can distinguish four cases. In this discussion, each node is assumed to be in an Ambient Community, even if this group is reduced to the node itself. Figure 2 shows all four interaction scenarios. Each of them needs specific operations.

- (a) A node wants to establish a level of trust with an Ambient Community and interact with one participant. Both nodes apply the CKE algorithm, sending only the already built common knowledge of the Ambient Communities to which they belong. As a result, both nodes obtain a level of trust between the two communities and not only the two nodes. If all the trust levels of the three components (the two pre-existing communities and the result of the CKE applied on the common knowledge of the two communities) is the same, the communities merge into a bigger community. If this is not the case, a candidate can choose to leave its original community and try to achieve access to the other one using its own knowledge instead of the common knowledge of its former community. This operation may fail, leaving the terminal on its own, excluded from every community.
- (b) A node is already included in a community and interacts with another member of this community. It can participate in the reinforcement of the common knowledge of the community by broadcasting new elements of knowledge.
- (c) The node is a member of a community and it leaves the community, voluntarily (see case (a)) or not - because of interference, mobility or another kind of networking partitioning. Because the node belongs to the community, its knowledge includes a community membership certificate with a time span.
- (d) The last case is of a node that was a member of a specific Ambient Community in the recent past and asks to rejoin the community. This case is denoted as the *long-lost node* scenario. If the original membership certificate for this specific community has not expired, the node is quickly reintegrated. If the certificate has expired, the procedure described in case (a) is applied except that this expired certificate is now part of the knowledge of the candidate and thus contributes to the CKE procedure.

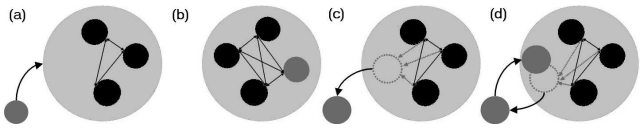

Figure 2: Illustration of all the possible encounter scenarios of a node with an Ambient Community.

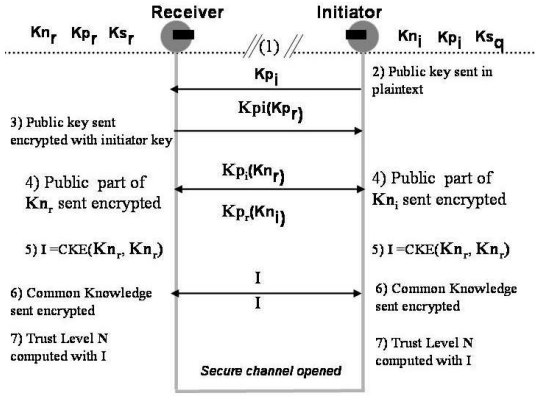

Figure 3: Common Knowledge Exchange algorithm

4.3 Role of ambient communities

The purpose of an Ambient Community is to group nodes into a close *social community*. We define a potential social community as a collection of users/terminals sharing a strong common history. The originality of our Trusted Ambient Community model is first that it can be set up very quickly and obtained purely through local computation. The second advantage is that the model can be applied to small groups (starting from 2!) and also potentially zero initial knowledge. In this case, an Ambient Community created on the basis of zero common knowledge base would be assigned with a low Trust Level, allowing participants to reinforce their common knowledge. Of course, the update of common knowledge over a large-scale ambient community has to be managed carefully in order to be scalable. This is a common drawback of any structuring techniques applied to highly dynamic groups. The advantage of our model is that communication can be initialised very quickly at a low level and the inclusion of a new node in an ambient community with a high level of trust is postponed until the level of trust between the candidate and one element of the Ambient Community is enough. Since a member of an Ambient Community uses the community's common knowledge, acceptation of a new member can be performed locally.

It is important to discuss the global security architecture that we will be able to build on top of the Trusted Ambient Community model. We can imagine the organisation as permitting each node to be part of more than one ambient community, but that each of these communities should be attributed with a different level of trust. Remember that for each level of trust there exists a list of associated services. To reduce the scalability problem, we could limit the number of Trusted Ambient Communities above Trust Level 3 to only 1. Doing so, each node can be part of 3 ambient communities. We can attribute Trust Level 1 to ad hoc networks. A Level 1 community would not really be a community, since we suppose that any node encountering another one even with only little common knowledge would be accepted in this virtual community and thus have access to the basic ad hoc services (at least routing services). Figure 4 gives an illustration of the kind of organisation that may occur in the Trusted Ambient Community model.

It is also possible to conceive specific distributed services that might be set up inside a particular Ambient Community, such as name services, software updates, data caches... but the most important feature of an Ambient Community is its associated notion of Trust Level which allows risk to be managed directly. The trust level may also decrease when the resulting trust turns out to have diminished after an update of the common knowledge. It is also possible to add specific security oriented services within an Ambient Community (such as recommendation) in order to expedite the integration of nodes, or to facilitate compartmental analysis and intrusion detection, which would be used to speed up the isolation of a suspicious node.

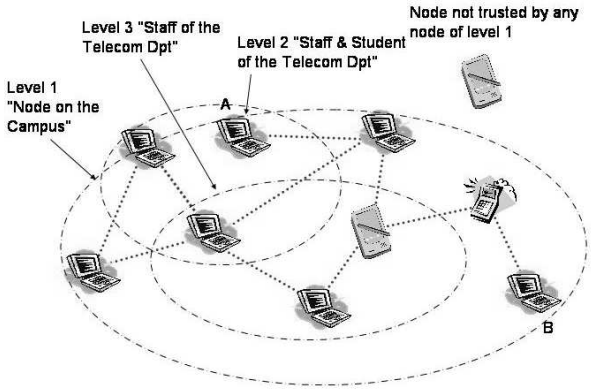

Figure 4: Nodes belonging to communities with different trust levels. Note that although node A communicates with node B in the context of a low security network, the data in fact traverses connections through higher security communities.

5 Discussion and conclusion

Ad hoc networks environments are open to a variety of possible security threats for which currently there is no global solution. Trust management is a key issue, its implementation being not only a technological problem but also a philosophical problem. Various policies for trust establishment may exist around the world and the choice of one of them clearly depends upon the context of usage. An ideal solution for a trust management architecture, therefore, would need to be flexible in order to be easily adaptable to any context - perhaps incorporating the possibility of the coexistence of various trust policies within the same architecture. Solutions attempting to implement such characteristics are described as being *self-organised* public-key infrastructures, a category into which the Trusted Ambient Community model neatly falls.

The Trusted Ambient Community model agglomerates groups of nodes with shared secrets and associated trust levels. The model supposes that in order to communicate, a node must be considered to be *honest*, what ever the definition of honesty for an ad hoc terminal might be. This assumption is clearly necessary an for ad hoc environment where terminals do not necessarily belong to the same usage context (no centralised authority has necessarily certified the terminals). The Ambient Community model could be implemented using already existing standards (ISAKMP and IPsec) but an evaluation of the overhead cost introduced by such a model has to be carried out. In our model, trust can clearly be given to an adversary. Therefore, in order to obtain a high level of trust - and thus penetrate an Ambient Community with high trust level - it could take a long time to obtain sufficient

common knowledge through only sniffing the networks. By the time the hacking is done, we could easily suppose that the context has changes, or some certificate expired.

Most attacks would be variants of man-in-the-middle, or ID usurpation. Attacks are made more difficult due to the fact that knowledge is sent over the air without the associated fingerprint, which would be needed to establish the trust. An ad hoc node in our model should reinforce its knowledge, and would therefore need some time to receive the associated fingerprint of new information elements. This has only been touched upon lightly in this paper, and is clearly a weak point of the model. In an ad-hoc environment, it would not be convincing to work on the assumption that the knowledge elements will always be obtained through physical imprinting (i.e., through physical transport) or by secure connection to a trusted server through an access point. Elements of the history of a node need to be obtained during ad hoc interaction. This problem has not yet been studied and the first answer is that a node transfers the associated fingerprint of its ID only to nodes participating in its Ambient Community and possessing a minimum level of trust. It is evident that depending on the trust policy, we could fall into the extremes either of an organisation with such weak security that any node could join and use services, to a system where security is so strict that the only allowed devices are those that follow very non ad hoc-like guidelines, such as the requirement for special hardware or otherwise.

Another drawback of the Trusted Ambient Community model is the potential cost induced by the management of the seed of trust. Depending on the context, the knowledge of a node could grow very quickly and the data management could easily put a high load on the CPU. Another problem is that when the knowledge grows large in size, it becomes difficult to transmit in one shot and only significant elements must be chosen to be sent during initialisation. How must this list be built? What would be the significant information?

Currently we are continuing our investigations related to the Trusted Ambient Community, both with regards to the basic elements as well as the global architecture. We are refining the model and plan to implement part of it to perform some performance evaluation.

References

[1] A. Abdul-Rahman and S. Hailes. A distributed trust model. In *New Security Paradigms Workshop, ACM*, pages 48–60, 1997.

[2] N. Asokan and P. Ginzboorg. Key-agreement in ad-hoc networks. *Computer Communications*, 18(23):1627–1637, 2000.

[3] T. Beth, M. Borchedring, and B. Klein. Valuation of trust in open networks. In *European Symposium on Research in Computer Security*, pages 3–18, 1994.

[4] L. Buttyan and J.-P. Hubaux. Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks. Research report, Swiss Federal Institute of Technology - Lausanne, Department of Communication Systems, 2001.

[5] G. Chelius, E. Fleury, and S. Ubeda. Issues in merging ad hoc, cellular and ip mobility. *IEEE Communication magazine*, 2003.

[6] Guillaume Chelius and Eric Fleury. Ananas: A new adhoc network architectural scheme. INRIA Research Report 4354, 2002.

[7] S. Corson and J. Macker. Mobile ad hoc networking (MANET): Routing protocol performance issues and evaluation considerations. IETF RFC 2501, January 1999.

[8] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Inform. Theory*, (22):644–654, 1976.

[9] C. Ellison and al. SPKI certificate theory. IETF RFC 2693, September 1999.

[10] A. Fiat and A. Shamir. How to prove yourself: Practical solutions to identification and signature problems. In LNCS Springer-Verlag, editor, *Advances in Cryptology - CRYPTO'86*, pages 186–194, 1987.

[11] M. Girault. Self-certified public keys. In Springer-Verlag, editor, *dvances in cryptology - Eurocrypt'91*, pages 490–497, 1991.

[12] J. Hubaux, L. Buttyan, and S. Capkun. he quest for security in mobile ad hoc networks. In *ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC)*, October 2001.

[13] P. Jonker, S. Persa, J. Caarls, F. de Jong, and I. Lagendijk. Philosophies and technologies for ambient aware devices in wearable computing grids. *Elsevier Computer communications*, (26):1145–1158, 2003.

[14] U. Jönsson, F. Alriksson, T. Larson, P. Johansson, and G.Q. Maguire Jr. MIPMANET - Mobile IP for Mobile Ad hoc Networks. In *IEEE/ACM Workshop on mobile and ad hoc networking and computing*, 2000.

[15] Jiejun Kong, Petros Zerfos, Haiyun Luo, Songwu Lu, and Lixia Zhang. Providing robust and ubiquitous security support for mobile ad-hoc networks. In *International Conference on Network Protocols (ICNP)*, pages 251–260, 2001.

[16] J. Pereira. Fourth generation: now, it is personal! In *IEEE International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1009–1016, 2OOO.

[17] C. Perkins and P. Bhagwat. Routing over Multi-hop Wireless network of Mobile Computers. In *SIGCOMM'94: Computer Communications Review*, October 1994.

[18] P.R.Zimmermann. *PGP Source Code and Internals*. MIT Press, Boston, 1995.

[19] R. L. Rivest and B. Lampson. SDSI - a simple distributed security infrastructure. version 1.1. Manuscript, available from(http://theory.lcs.mit.edu/cis/sdsi.html), October 1996.

[20] E. Royer and C. Toh. A review of current routing protocols for ad-hoc mobile wireless networks. *IEEE Personal Communications*, pages 46–55, 1999.

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

[22] F. Stajano and R. Anderson. he resurrecting duckling: Security issues for ad-hoc wireless networks. In LNCS Springer-Verlag, editor, *7th International Workshop on Security Protocols*, pages 172–194, April 1999.

[23] L. Zhou and Z.J. Haas. Securing ad hoc networks. *IEEE Network*, pages 24–30, 1999.

[24] L. Zhou, F. B. Schneider, and R. van Renesse. COCA: A secure distributed online certification authority. Cornell University, Research Report, 2002.

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399