# Towards Mobile Ad-Hoc WANs: Terminodes

J.-P. Hubaux, J.-Y. Le Boudec, S. Giordano,
M. Hamdi, L. Blazević, and L. Buttyán, M. Vojnović
Swiss Federal Institute of Technology - Lausanne

*Abstract*— **Terminodes are personal devices that provide functionality of both the terminals and the nodes of the network. A network of terminodes is an autonomous, fully self-organized, wireless network, independent of any infrastructure. It must be able to scale up to millions of units, without any fixed backbone or server. In this paper we present the main challenges and discuss the main technical directions.**

## I. Introduction

The Terminode Project is a 10-year-long research program (2000-2010) [ter] that investigates wide area, large, entirely wireless networks that we call *mobile ad-hoc wide area networks*. In this project, we follow a radically distributed approach in which all networking functions are embedded in the terminals themselves [Hub99]. Because they act as nodes and terminals at the same time, we call these devices *terminodes*. A network of terminodes is an autonomous, self-organized network, completely independent of any infrastructure or other equipment. A previous paper presented the first technical options of terminodes [HBGH99].

Our vision of the Terminode Project can be illustrated by a scenario of a free, wireless network covering a wide area. In this scenario, terminodes are small personal devices owned by everyone in a given area (city, region or country). The set of terminodes constitutes a large network where multi-hop wireless communications allow voice and data messaging among all users. The whole network operates at unlicensed frequencies. It can be considered a free amateur wide area wireless network. The terminode users can be human or equipment, depending on the application. A terminode network can be of any size. In particular, in regions of high-density population, the size could reach several million devices. In the following, we summarize the main design points of the project.

*The Spectrum is the Infrastructure:* To eliminate the need for any additional device or network equipment, all networking functions (typically performed in backbone routers/switches and servers) are distributed in the terminodes. The only external resource needed by users is the frequency bandwidth that is assumed to be allocated by regulation authorities. The fact that routing/switching functions are performed in the terminodes dramatically changes the routing paradigm. A backbone of routers or switches typically looks like a tree, sometimes augmented with few redundant links. In the terminodes approach, the backbone is identical to the set of terminodes and looks more like a strongly connected graph with a very high level of redundancy.

*Scalability to Large Numbers:* Scalability to a very large number of terminodes is central to our research. In the Internet or Telecom networks, this issue is efficiently addressed using centralized and/or hierarchically organized routers and servers. This approach is inappropriate in our context.

*Decentralization and Self-organization:* Terminodes are designed to be self-organizing: any number of terminodes that form a connected graph can constitute a network. Therefore, all terminodes have a common, minimal set of functions that are necessary and sufficient for the network self-operation (*peer-to-peer* [Ver98]). Compared to current networks, the mechanisms that include centralized storage or processing must be substituted with completely distributed solutions. However, this does not imply that all terminodes are identical. A terminode can be individually extended with large processing, storage or internetworking capabilities that could be a benefit for entire community of terminodes – under the condition that these extensions are not necessary to run the network.

*CB Business Model:* The terminodes introduce an original business scenario in multimedia communication services. In today's networks, most multimedia communication services, including those supported by the Internet, are seen by the end user as commercial services that include a service contract and regular fees. In the scenario we consider, the paradigm is radically different: terminodes are goods that people purchase once and use forever, without service contracts or per-use-basis fees. This is similar to the business model of citizen band, amateur radio, and talkie-walkie systems.

## II. Related Work

Research in mobile ad-hoc networks was initiated in DARPA Packet Radio projects [JT87]. The research on wireless networks has been mainly focused on cellular systems that are, in principle, single-hop wireless systems. Within the framework of the multi-hop wireless systems, research communities worked on projects that addressed mainly Medium Access Control (MAC) and routing issues.

The MAC layer specified in the IEEE 802.11 standard [80299], or its variants, is typically assumed in the existing ad-hoc network projects. The standard is based on the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) scheme that is extended with short channel allocation and acknowledgment control messages. Apart from IEEE 802.11, there have been many extensions to the basic CSMA/CA protocol, including MACA, MACAW, FAMA, and CARMA. Their common objective is to resolve contention to a single-channel for a limited number of transceivers.[1] To probe further on these protocols, the reader is referred to [GLAF99] and the references therein. The wireless LAN technology is already widely available commercially. More recently, the Bluetooth standard has been defined [Blu99] as a low cost pico-cell wireless technology suitable for purposes such as cable replacement. However, it is still unclear how profitable it can be for mobile ad-hoc networks. Nevertheless, none of these protocols are targeted to deploy a wide-area mobile ad-hoc network such as the Terminodes network.

In the last few years, projects such as Monarch, Wins, etc., produced several routing protocols, simulation tools, simulation analysis, and performed trials. Mobile ad-hoc networks are becoming accepted as a valid commercial concept, which is confirmed by the creation of the MANET working group in IETF [Mob99]. Past work has focused on small networks. Based on the existing routing protocols, significant

This paper is accepted in the IEEE WCNC'2000 conference, Chicago, Sep. 2000. The authors are with the Institute for computer Communications and Applications (ICA), EPFL. Email: {Jean-Pierre.Hubaux, Jean-Yves.LeBoudec, Silvia.Giordano, Maher.Hamdi, Ljubica.Blazevic, Levente.Buttyan, Milan.Vojnovic} @epfl.ch

[1] An exception is CARMA, which has been extended to a multi-channel setting.

effort is currently being made in order to achieve scalability [ICP+99],[MZ99],[MBJJ99],[HP99]. Rather than following an evolutionary approach, we decided to investigate a different type of routing based on the physical location of the destination. A similar idea is used in [KV98], [BCSW99], [BCS99], but we combine it with new location and packet forwarding algorithms, designed specifically for networks with several million nodes.

## III. Basic Mechanisms

In this section we outline the fundamental mechanisms that we envision. The following sections will address the mobility management, security and incentive to collaborate. Finally, we will sketch some application scenarios.

### A. Packet Switching and Burnt-In Addresses

We envision a terminode network based on packet switching. Although circuit switching is an advantage for supporting voice (very small delay in relaying terminodes), the complexity associated with establishing, maintaining, and releasing circuits, or any form of connection, is at odds with the requirement that intermediate systems are user equipment, and may operate quite irregularly. Thus, we use connection-less packet switching. Delay will be minimized by supporting cut-through operations: routing information is placed at the beginning of the packet header and forwarding starts as soon as valid routing information has been analyzed.

Terminodes must be identified by some means of addressing. We need an address that a terminode can use without configuration; every terminode has a burnt-in 64 bit End-system Unique Identifier (EUI), as is planned today in the replacement of MAC addresses for any communication equipment. Note that terminodes are able to work with the Internet protocol (see below), however it is not a good idea to use IP addresses as the unique identifiers because, as long as IPv6 is not really deployed, there are not enough IPv4 addresses that could be set-aside for the exclusive use of terminodes.

### B. Radio System Architecture

The concept to design a wide-area radio network with no fixed infrastructure raises several technical issues, which have not been of concern with the existing systems (e.g., cellular systems and wireless LANs). In this section we discuss the radio system architecture, including physical and MAC layers. Currently, the predominant radio access technology considered for the third-generation cellular systems is Code Division Multiple Access (CDMA) [OP98], [umt97]. This is mainly due to an intrinsic flexibility of CDMA systems in terms of the radio resource planning. We envision the terminodes to use one, or several, non-operated frequency bands to be allocated for that purpose.

How should the radio system be architectured for terminodes? This question is raised bearing in mind that the system has to be decentralized and self-organizing, that it should cover a wide-area, support a potentially enormous number of terminodes, with a high diversity of terminode density. Architecturing the radio technology is a part of our ongoing research efforts, and our current considerations are centered around CDMA. Below, we address some of the technical issues involved.

We consider two tentative (global) radio system architectures that do not exclude other potential approaches.

- *Terminodes are self-organized into communities.* A community would be defined as a set of terminodes accessible by at least one of them in a single hop. This concept is fairly similar to the existing systems (cells of the cellular systems or individual wireless LANs). The basic distinction is that the communities are not assumed to be fixed to a given geographical region, and there is no notion of a base-station. The radio resource allocation could be done differently in intra- and inter-community communication. This is also inline with the packet forwarding discussed in section 3.3.
- *A terminode is not a member of any specific community.* In this approach, there is in fact no defined community. This concept is inspired by Shepard's paper [She96], which proposes an architecture based on CDMA. The author conducts a feasibility study to operate a dense packet radio network, where most of the radio resource allocation is resolved through CDMA, and only a simultaneous transmission and reception of a given station is alleviated through the MAC protocol. It is shown that the system is feasible assuming that the minimum energy routes are used, where each station directly communicates only with a few of its closest neighbors. However, it is demonstrated that localization of the traffic is necessary to avoid congestion, and this remains to be resolved. The paper, also, does not cover the mobility and code assignment problem. The latter may be needed to avoid the *hidden-terminal* problem [TK75], and can be solved through either *transmitter*, *receiver*, or *pair-wise oriented* code assignment [Hu93].

Indeed, one could argue whether the former or latter concept should be favored, which goes beyond the scope of the present paper. In general, common to all CDMA systems is the necessity for the transmission power control to reduce interference and to achieve a certain level of QoS (typically expressed in terms of a signal-to-interference ratio). Although, there is substantial work on the power control, most of the results are derived for the cellular systems setting. Hence, this is a potential direction of future work. Nevertheless, advanced concepts have to be evaluated to a full extent in order to define an architecture viable in the long-term (e.g. multi-user detection, rate adaptation, adaptive antennas).

Another issue of interest for the Terminodes is reduction of the power consumption in order to extend the battery longevity for battery supplied terminodes. There has been some work on designing power-aware protocols. For a recent overview of this issue the reader is referred to [WESW98].

### C. Packet Forwarding

A packet sent by a terminode contains, among other fields, the destination LDA and EUI, and possibly some source routing information. Our solution is based on a combination of the following ingredients (see [LB00] for more details). (1) Path Discovery and Maintenance, (2) Packet Forwarding.

Every terminode builds its personal view of the network. The personal view of the network is composed by two level views: local and remote view. Large scale routing is the terminode network is based on the combination of those two level views.

The local view of a terminode consists of information about other terminodes in its local vicinity (e.g a few hops away). It is based on the *Terminode Local Routing (TLR)* method, which provides the following functions:

- Discover the identities (EUIs) of the terminodes that are reachable by TLR. Such terminodes are a few hops away, and are said to be *neighbours*. This mechanism that is inspired by the IERP part of ZRP[HP99].
- Discover paths to neighbours. Source routing is used to reach neighbours, much like DSR[MBJJ99].
- Discover location (LDA) of neighbours. This is used in support of the remote view. However, TLR does not use locations for itself, and like DSR, routes are based only on fixed identities (EUIs).

In addition, a terminode builds its remote view by acquiring information about non-neighbour terminodes.

• The remote view is used by *Anchored Geodesic Packet Forwarding (AGPF)*, which is the method that allows to send data to non-neighbour terminodes. Unlike TLR, AGPF is heavily based on locations. In its simplest form, geodesic packet forwarding would consist in sending a packet in the direction of the destination, identified by its LDA. When an intermediate node receives such a packet, it checks whether the destination EUI is within reach of its TLR method, and if so, it uses this latter method. Else, the packet is sent to a neighbour in the direction of the destination LDA. The direction is computed as the shortest path (geodesic) on earth. In this simplest form, geodesic packet forwarding will not often work. If there is no connectivity along the shortest line, then the method would fail, typically because a relaying terminode would find no neighbour within the angle towards the destination. Our solution to this problem is to use *anchors*. An anchor is a point, described by geographical coordinates; it does not have to correspond to any terminode location. Anchors are computed by source nodes, using the methods described above. A source terminode adds to the packet a route vector made of a list of anchors, which is used as loose source routing information. Between anchors, geodesic packet forwarding is employed. When a relaying terminode receives a packet with a route vector (list of anchored points), it checks whether the convex hull of its set of neighbours includes the first anchor in the list. If so, it removes the first anchor and sends it towards the next anchor or the final destination, using geodesic packet forwarding. If the anchors are correctly set, we conjecture that there is a good chance that the packet will arrive at destination.

• The remote view is created by a combination of path discovery methods called *Friend Assisted Path Discovery (FAPD)* and *Directional Random Discovery (DRD)*.

– FAPD is based on the concept of small world graphs[?]. A terminode $A$ keeps a list of terminodes that it calls *friends*. $B$ is a friend of $A$ if (1) $A$ thinks that it has a good path to $B$ and (2) $A$ decides to keep $B$ in its list of friends. $A$ may have a good path to $B$ because $B$ is a neighbour of $A$, or because $A$ managed to maintain one or several route vectors to $B$ which work well. When $A$ wants to discover a path to a destination $C$, then $A$ may require assistance from a friend $B$. This is done by sending a route request packet to $B$, which contains an offer (counted in beans). If $B$ accepts the offer, it has to find a path to $C$. When this path is found and authenticated by $C$, then $B$ keeps the beans and returns to $A$ the desired path. $B$ may in turn use his own set of friends to identify a path to $C$.

– Directional Random Discovery (DRD) is the last resort method. It consists in two mechanisms for forwarding a discovery packet towards the destination, and works as follows. When a terminode receives such a packet, it tries to send it to a good neighbour. As explained above, this is the most forward neighbour, inside a given angle, in the direction to the destination. When this first mechanism fails, i.e. there are no neighbours inside the given angle, the terminode applies the second mechanism. It determines the smallest angle towards the destination, which contains between 1 and 3 neighbours and sends to all neighbours within this angle. If there is an obstacle or a gap in the direction of the destination, then this angle may be large. Then the discovery packet is sent to these 1, 2 or 3 neighbours, who will forward it further, until the destination is reached. Every node accumulates its LDA into the packet, and consumes some beans. This method provides paths that tend to follow the boundary of holes in the terminode networks. The resulting paths are candidates to improvement.

• The remote view is constantly modified by *Path Maintenance*, which consists of three main functions: path simplification; path monitoring and deletion; congestion control and allows to improve paths, and delete obsolete or mal-functioning paths.

Mobility management, which is essential for routing, is performed by a combination of the following functions. Firstly, TLR allows a terminode to know who its neighbours are, and track them. Secondly, a location tracking algorithm is assumed to exist between communicating terminodes; this allows a terminode to predict the location (LDA) of corresponding terminodes. Thirdly, a distributed directory (VHR, as mentined previously in this paper) allows a terminode $A$ to obtain a probable location of terminode $B$ that $A$ is not tracking by any of the previous two methods.

Looping packets are discarded by the beans mechanism described below (similar to the TTL field in IP packets). Multicast packet forwarding in the Internet is already difficult enough and, thus for terminodes will be studied later.

.

## IV. Mobility Management

In a network of terminodes, two generally adopted solutions to manage mobile terminals (flooding within MANET networks [Mob99], and fixed server within GSM or Mobile IP) are not adequate and a new approach has to be found for mobility management. This is because the flooding operations have a dramatic effect in a very large network. In addition, no fixed infrastructure or servers can be assumed in the Terminodes network for the reasons mentioned above.

Few authors have already been studying the mobility management problem in ad hoc networks. The most relevant approaches are given in [LJC+00],[LH00]. The first approach defines a hierarchically distributed server and shows higher performances than MANET ad hoc routing algorithms. The second defines a virtual backbone as a subset of nodes that are responsible for replicating and maintaining location information of mobile nodes. We have developed a new and original approach for mobility management that avoids both flooding, and servers or directory services. It is called the Virtual Home Region (VHR) approach.

### A. Principle

A virtual home region is a set of terminodes located near to each other. The VHR is in charge of keeping some of the information generated by a terminode. This terminode is called *the owner terminode* (because it owns the information stored in the VHR). The VHR is defined by a point in the space, $C$, and a radius $R$. The terminodes that belong to a VHR are those located in the disk ($C$,$R$). Each terminode defines a single VHR that we refer to as "its VHR"; the relation between a terminode and its VHR is defined by a well-known hash function $H$. The function $H$ operates on the EUI space and gives images in the LDA space: $H(EUI) = C$ with $C$ being the center of the VHR of terminode EUI. The owner does not need to be in its VHR (in general it is not).

When the owner terminode $A$ moves to a new location, it stores its new LDA coordinates in its VHR, using a simple SNMP-like protocol[2]. If a terminode $B$ is willing to send packets to $A$, it sends a query to $A$'s VHR and retrieves its LDA. The VHR associated to $A$ is known to $B$ because $H$ is known to all terminodes (see Figure 1).

To make this approach work, terminodes are provided with the capability of storing short information, serving as temporary distributed memory for other terminodes. This cooperation is mandatory for a self-operating network.

[2]We also consider additional protocols for direct source-destination mobility tracking that are not discussed in this work.

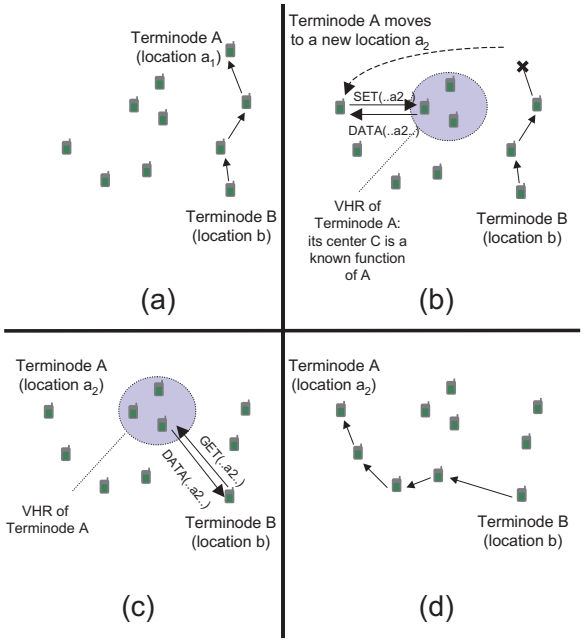


Fig. 1. The VHR mobility management; (a) terminodes $A$ and $B$ are communicating directly, (b) terminode $A$ moves and uses the VHR protocol to publish its new position, (c) if $B$ does not directly keep track of $A$'s movement, it uses the VHR protocol to retrieve the new location of $A$, (d) finally, $B$ re-establishes communication with $A$.

The advantage of this approach is that it requires a reasonable amount of communication to find a new position, in addition to the fact that no external devices or servers are necessary. There are several technical issues that are being solved to implement this solution; in particular the radius setting is discussed hereafter.

### B. The Radius Setting

The VHR needs management procedures in order to ensure that it contains a sufficient number of terminodes. This number is appropriately chosen to ensure enough redundancy of the stored information and at the same time to be small enough to minimize communications inside the VHR. The expected VHR size is between 4 and 20 terminodes, mainly depending on the packet loss probability. The radius has then to be dynamically set to reach this size. Currently, two schemes are being evaluated to estimate the VHR size. In the first, the VHR is managed in a centralized mode (by the owner); in the second, it is managed in a distributed way (by the terminodes inside the VHR with self-organization functions). If the VHR is managed by its owner, it is the responsibility of the owner itself to estimate, monitor and manage the radius of its VHR. On the contrary, if the VHR is self-organized, this becomes a task of the terminodes in the VHR. The radius is increased when the VHR size falls under its minimum value and decreases when it exceeds its maximum value. A *VHR Protocol* is used to store and retrieve location information from the VHR, as illustrated in Figure 1.

## V. Security

Security in networks (including wireless ad-hoc networks) is concerned with confidentiality and integrity of information, as well as legitimate use and availability of services [For94]. In military applications, confidentiality is considered to be the most important security objective. In civilian scenarios, however, availability has the greatest relevance for the user [SA99]. In the Terminode network, availability has two aspects:

- *Stimulation for co-operation.* Since *all* services (e.g., packet forwarding, mobility management) are provided by the terminodes themselves, these services are available only if the terminodes (or, more precisely, their users) are willing to provide them. On the other hand, service provision is not in the direct interest of users, because it consumes energy and, thus, reduces battery lifetime. Therefore, a stimulation mechanism is required that encourages users to leave their terminodes switched on and let them provide services to other terminodes. We discuss this issue further in Section VI, where we present an approach to solve this problem.
- *Defense against denial-of-service attacks.* Stimulation for cooperation is not enough to achieve availability, because services may be unavailable due to denial-of-service attacks, such as interception of packets and destruction or modification of control information (e.g. information required for the geodesic packet forwarding mechanism). Denial-of-service attacks are typically impossible to prevent. However, they can be made very expensive by exploiting the inherent redundancy of the ad-hoc networks [ZH99]. For instance, a packet can be sent to its destination via several disjoint routes, which makes its interception considerably more expensive for the attacker.

A fundamental tool to achieve network security objectives is cryptography. Cryptography is indispensable to confidentiality and to protection of the information integrity, and also used in mechanisms that ensure legitimate use of services (e.g. in authentication protocols). The challenge of using cryptography in the Terminode network is the management of cryptographic keys.

Since terminodes are mobile, their interactions are spontaneous and unpredictable, which makes public key cryptography more appropriate in this setting than conventional cryptography. The most widely accepted solution for the public key management problem is based on public key certificates that are issued by (off-line) certification authorities and distributed via (on-line) key distribution servers. Unfortunately, the application of certification authorities and key distribution servers contradict the self-organized[3] and self-operated features of the Terminode network.

One approach for solving the key management problem may be based on the replacement of the certification authorities with communities of users (a PGP-like solution [Zim95]) and the distribution of the key distribution server function among the terminodes (a VHR-like solution). Another approach may be to adopt a system that implicitly guarantees the authenticity of public keys, such as identity-based systems [Sha85] and those using implicitly certified keys [Gir91].

## VI. Incentive to collaborate

As we mentioned in Section V, the Terminodes network relies on the co-operative behavior of the terminodes (or, more precisely, their users). One possible approach to stimulate such behavior is to introduce the concept of money and service charges. The natural idea is that terminodes that used a service should be charged and terminodes that provided a service should be remunerated. To this end, we introduce a terminode currency that we call *nuggets*. We assume that the terminode hardware comes with an initial stock of nuggets. The terminode nuggets

[3] Note that in military networks self-organization is not required at this level. Indeed, these networks can rely on a hierarchically organized system of certification authorities, which are represented by headquarters at different levels. Self-organization of the network is required only in the battlefield, which does not effect the key management problem in such a radical way as it does in the Terminode network.

have no monetary value, and they can only be used within terminode networks.

Now, if a terminode wants to use a service (e.g., wants to send a message), then it has to *pay* for it in nuggets. This motivates each terminode to provide services to other terminodes and, in this way, increase its number of nuggets, because nuggets are indispensable for using the network.

One of the main services that the terminodes should provide to each other is the packet forwarding. We are investigating two approaches for rewarding the provision of this service.

- *Packet Purse Model.* In this approach, the originator of the packet pays for the packet forwarding service. The service charge is distributed among the forwarding terminodes in the following way: When sending the packet, the originator loads it with a number of nuggets sufficient to reach the destination. Each forwarding terminode acquires one or several nuggets from the packet and thus, increases the stock of its nuggets; the number of nuggets depends on the direct connection on which the packet is forwarded (long distance requires more nuggets). If a packet does not have enough nuggets to be forwarded, then it is discarded.
- *Packet Trade Model.* In this approach, the packet does not carry nuggets, but it is traded for nuggets by intermediate terminodes. Each intermediary "buys" it from the previous one for some nuggets[4], and "sells" it to the next one (or to the destination) for more nuggets. In this way, each intermediary that provided a service by forwarding the packet, increases its number of nuggets, and the total cost of forwarding the packet is covered by the destination of the packet.

Clearly, the models described above must be enforced somehow, otherwise terminodes may depart from them. The basic problems to be solved are related to nugget forgery, protection of the packet purse integrity (in the Packet Purse Model), and the fair exchange of packets for nuggets (in the Packet Trade Model). Enforcement of the models may be based on the application of a tamper resistant hardware module in each terminode, which can be used for the management of nuggets, and cryptographic protection of messages [BH00]. The challenge is to find a trade-off between the robustness of the solution and its efficiency; forwarding a single packet should not require complex cryptographic protocols and heavy computational effort, because the cost of these may well exceed the value of the service.

## VII. Application Scenarios and Discussion

Increasingly often, replacing a technology can be more cost-effective than enhancing it. The newer the technology, the richer are the potentials for new services.

Infrastructure-less mobile networks can be an appropriate solution in a number of situations. A first example is a natural disaster. An earthquake, a hurricane, or a flood can severely damage the wired and wireless infrastructure of a region. At the same time, the need to communicate increases dramatically in order to organize relief and assistance. Terminodes can be a way to keep communications operational: even if some of them are lost or destroyed in the disaster, the remaining ones will spontaneously organize themselves to support the traffic.

A second example is related to political instability. Too often, because of a high level of corruption or because of guerilla activities, the communication network of a given region or country does not have the appropriate level of dependability. Such a situation can significantly hamper development and progress toward democracy. By empowering citizens with the networking functions, the terminodes can be an efficient solution to this kind of problem. A more general example is related to the cases where the economic madel of a cellular network does not make sense (e.g., very poor countries and/or remote areas).

Terminodes can also be used for a wide range of applications in situations less critical than the ones described earlier. As mentioned in section 2, they can serve to support a kind of "citizen band", by which people could avoid having to go through the infrastructure of a given operator – due to cost or privacy concerns.

[4] Except for the first intermediary that receives the packet for free from the originator.

## VIII. Conclusion

In this paper, we have stated the main objectives of our work and we have sketched the solutions we are exploring. Currently we are working in the following directions. First, we are refining the requirements, notably in terms of scalability, with prominent humanitarian organizations. Second, we are checking the robustness of our solutions, notably by means of simulations. Third, we are building analytical models for the most involved parts of the design, such as the radio architecture and the packet forwarding principle.

The long-term goal is to design a device that will empower citizens with direct communication facilities.

## Acknowledgements

We would like to thank Christian Bonnet, Thomas Gross, Martin Vetterli, and all the team of the Terminodes project for interesting and useful discussions.

## References

[80299] ISO/IEC 8802-11:1999(E) ANSI/IEEE Std 802.11. *Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications*. 1 edition, 1999.

[BCS99] S. Basagni, I. Chlamtac, and V.R. Syrotiuk. Geographic Messaging in Wireless Ad Hoc Networks. *VTC99 Huston*, 1999.

[BCSW99] S. Basagni, I. Chlamtac, V.R. Syrotiuk, and B.A. Woodward. A Distance Routing Effect Algorithm for Mobility (DREAM). *MOBICOM'99 Seattle*, 1999.

[BH00] Levente Buttyán and Jean-Pierre Hubaux. Enforcing service availability in mobile ad-hoc WANs. In *Proceedings of the First IEEE/ACM Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC)*, August 2000.

[Blu99] Bluetooth. *Specification of the Bluetooth System, v.1.0 A Core*. 1 edition, 1999. available from http://www.bluetooth.com.

[For94] W. Ford. *Computer Communications Security – Principles, Standard Protocols and Techniques*. Prentice Hall, Inc., 1994.

[Gir91] M. Girault. Self-certified public keys. In *Advances in Cryptology - EUROCRYPT'91*, pages 490–497. Springer-Verlag, 1991.

[GLAF99] J. J. Garcia-Luna-Aceves and Chane L. Fullmer. Floor acquisition multiple access (fama) in single-channel wireless networks. In *Mobile Networks and Applications*, volume 4, pages 157–174, 1999.

[HBGH99] JP. Hubaux, JY. Le Boudec, S. Giordano, and M. Hamdi. The terminode project: Toward mobile ad-hoc wans. In *Proceedings of Workshop on Mobile, Multimedia Conference*, San Diego, USA, November 1999.

[HP99] Z.J. Haas and M.R. Pearlman. Determining the Optimal Configuration for the Zone Routing Protocol. *IEEE JSAC*, August 1999.

[Hu93] Limin Hu. Distributed code asignments for cdma packet radio networks. *IEEE/ACM Transactions on Networking*, 1(6):668–677, 1993.

[Hub99] J-.P. Hubaux. Terminodes : Toward Self-organized Mobile Networks. Technical Report "SSC/1999/022", EPFL-ICA, June 1999.

[ICP+99] A. Iwata, C.-C. Chiang, G. Pei, M. Gerla, and T.-W. Chen. Scalable Routing Strategies for Ad-hoc Wireless Networks. *IEEE JSAC*, 1999.

[JT87] J. Jubin and J.D. Tornow. The DARPA Packet Radio project. *Proceedings of the IEEE.*, 1987.

[KV98] Youngbae Ko and N. H. Vaidya. Location-Aided Routing (LAR) Mobile Ad Hoc Networks. *MOBICOM'98 Dallas*, 1998.

[LB00] J.-Y. Le Boudec L. Blazevic, S. Giordano. Self-organizing wide-area routing. In *in ISAS 2000 - Orlando, USA, July 2000*, 2000.

[LH00] B. Liang and Z. J. Haas. Virtual backbone generation and maintenance in ad hoc network mobility management. In *IEEE Infocom 2000*, 2000.

[LJC+00] J. Li, J. Jannotti, D.S.J. De Couto, D. R. Karger, and R. Morris. A scalable location service for geographic ad hoc routing. In *ACM Mobicom'2000*, 2000.

[MBJJ99] David A. Maltz, Josh Broch, Jorjeta Jetcheva, and David B. Johnson. The Effects of On-Demand Behavior in Routing Protocols for Multi-Hop Wireless Ad Hoc Networks. *IEEE JSAC*, August 1999.

[Mob99] Mobile Ad-hoc Networks (manet) WG. Mobile Ad-hoc Networks (manet) Charter. Wg charter, IETF, 1999. http://www.ietf.org/html.charters/manet-charter.html.

[MZ99] A.B. MCDonald and T.F. Znati. A Mobility-Based Framework for Adaptive Clustering in Wireless Ad Hoc Networks. *IEEE JSAC*, August 1999.

[OP98] Tero Ojanpera and Ramjee Prasad. An overview of air interface multiple access for imt-2000/umts. *IEEE Communications Magazine*, 36(9):82–95, 1998.

[SA99] F. Stajano and R. Anderson. The resurrecting duckling: Security issues for ad-hoc wireless networks. In *Proceedings of the 7th International Workshop on Security Protocols*, Cambridge, UK, April 1999.

[Sha85] A. Shamir. Identity-based cryptosystems and signature schemes. In *Advances in Cryptology - CRYPTO'84*, pages 47–53. Springer-Verlag, 1985.

[She96] Timothy J. Shepard. A channel access scheme for large dense packet radio networks. In *Proc. of SIGCOMM'96*, pages 219–230, CA, USA, August 1996.

[ter]

[TK75] F. Tobagi and L. Kleinrock. Packet switching in radio channels: Part ii – the hidden terminal problem and the busy-tone solution. *IEEE Transactions on Communications*, 23(12):1417–1433, 1975.

[umt97] Universal mobile telecommunications system (umts). Technical Report TR 101 146, ETSI – Eureopean Telecommunications Standards Institute, F-06921 Sophia Antipolis Cedex - FRANCE, December 1997. available from http://www.etsi.org.

[Ver98] S. Verdu. *Multiuser Detection*. Cambridge university, 1998.

[WESW98] Hagen Woesner, Jean-Pierre Ebert, Morten Schlager, and Adam Wolisz. Power-saving mechanisms in emerging standards for wireless lans: The mac level perspecitve. *IEEE Personal Communications*, pages 40–48, June 1998.

[ZH99] L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24–30, November/December 1999.

[Zim95] P. Zimmermann. *The Official PGP User's Guide*. MIT Press, 1995.