Self-Organization in Mobile Ad-Hoc Networks: the Approach of Terminodes

Ljubica Blažević*, Levente Buttyán, Srđan Čapkun,
Silvia Giordano, Jean-Pierre Hubaux and Jean-Yves Le Boudec

Institute for computer Communications and Applications (ICA)
Swiss Federal Institute of Technology, Lausanne, Switzerland
{ljubica.blazevic, levente.buttyan, srdan.capkun, silvia.giordano, jean-pierre.hubaux, jean-yves.leboudec}@epfl.ch

Abstract

The Terminodes project is designing a wide area, mobile ad-hoc network, which is meant to be used in a public environment; in our approach, the network is run by users themselves. We give a global description of the building blocks used by the basic operation of the network; they all rely on various concepts of self-organization. Routing uses a combination of geography-based information and local, MANET-like protocols. Terminode positioning is obtained either by GPS, or by a relative positioning method. Mobility management uses self-organized virtual regions. Terminodes employ a form of virtual money called "nuglets" as an incentive to collaborate. Lastly, we discuss directions for providing some level of security.

Keywords: self-organized network, MANET, self-organized routing, GPS-free positioning, incentive to cooperation, security

1 Introduction

The Terminodes project is a long-term research project (2000-2010) aimed at studying and prototyping large-scale self-organized mobile ad hoc networks. In this framework, the nodes are called "terminodes" (terminal+node). The project distinguishes itself from other research projects in this area in several ways: First, it encompasses all layers and explores inter-layers interactions, from the fundamentals of the physical layer up to software architecture and applications; Second, it is free from short term compatibility constraints such as the interoperation with IPv4 networks (this interoperation will be studied in the project, however); Last but not least, it tries to capture the business and societal potential generated by the paradigm shift previously described.

Self-organization is the keyword of the project [7]. Self-organized networks distinguish themselves from traditional mobile ad-hoc networks, based on the traditional Internet two level hierarchy routing architecture [10], by emphasizing their self-organization peculiarities [5]:

*contact author, tel. +41 21 693 6616, fax. +41 21 693 6610

- Self-organized networks are non-authority based networks, i.e., they can act in an independent way from any provider or common denominator, such as the Internet, even if they still require regulation (self-organization).
- Self-organized networks are potentially very large and not regularly distributed. In principle, one single network can cover the entire world. Density is supposed to be very high in small areas (e.g. towns), and low in large areas.
- Self-organized networks are highly co-operative. The tasks at any layer are distributed over the nodes and any operation is the result of the cooperation of a group of them.

Terminodes correspond to totally self-organized mobile ad hoc networks. In this kind of network, there is no operator at all: users purchase their device from a vendor, turn it on, and are automatically connected (as if they had purchased talkie-walkies). Therefore, all management functions (configuration, set up of security mechanisms, resource allocation,...) have to work without any human intervention and without any server.

Can all the mechanisms of mobile ad hoc networks be self-organized? To the best of our knowledge, this question was never been tackled in such a systematic way. Each of the following five sections illustrates the solution we envision for a specific mechanism: routing, mobility management, GPS-free positioning, incentive to cooperation, and security. More details can be found at [1].

2 Packet Forwarding

Each terminode has a permanent End-system Unique Identifier (EUI), and a temporary, location-dependent address (LDA). The LDA is simply a triplet of geographic coordinates (longitude, latitude, altitude) obtained, for example, by means of the Global Positioning System (GPS) or the GPS-free positioning method (see Section 4).

In a terminode network, two important factors affect the design of a solution for packet routing. Firstly, scalability is required, both in terms of number of nodes and geographical coverage.

Secondly, network nodes are user equipment, therefore might be available only sporadically. This second requirement imposes some incentive for users to cooperate and forward packets on behalf of others. A solution is discussed in Section 5.

As a consequence of the above requirements, our solution is designed such that a terminode relies only on itself and a small number of other terminodes for packet forwarding. In addition, we cope with uncertainty in the network by considering multipath routing as a rule, and not as an exception. We use a combination of two routing methods: Terminode Local Routing (TLR) and Terminode Remote Routing (TRR). TRR uses geographic information; it is the key element for achieving scalability and reduced dependence on intermediate systems. However, when a packet gets close to the destination, positional errors and inconsistent location information can result in routing errors and loops if locations are used for making packet forwarding decisions. Therefore, when close to destination, the packet forwarding method becomes TLR, which does not use location information. Once a packet has been forwarded with TLR, the "don't use TRR" bit is set within the packet header, thus preventing downstream terminodes from using TRR for this packet. This avoids loops due to the combination of the two routing methods.

Terminode Local Routing (TLR)

TLR allows to reach terminodes that are several wireless hops away, but is limited in distance and number of hops. TLR is inspired by the Intrazone Routing Protocol (IARP) in ZRP[11].

We say that terminode D is *TLR-reachable* for terminode S if S has a means to reach D with the TLR protocol. The TLR-reachable area of S includes the terminodes whose minimum distance in hops from S is at most equal to a *local radius*. The local radius is a measure, in number of hops, of the TLR-reachable area.

Every terminode proactively maintains the information (EUI, LDA) of the terminodes that are in its TLR-reachable area. TLR uses a distance vector routing protocol to send data to TLR-reachable destinations, and thus the only addressing information used for packet forwarding is the EUI of the destination.

Terminode Remote Routing (TRR)

Terminode Remote Routing (TRR) allows data to be sent to *non TLR-reachable* destinations. TRR consists of the following elements:

- *Anchored Geodesic Packet Forwarding (AGPF)* [8] is a method to send data to remote destinations. Unlike TLR, AGPF is solely based on locations.

  When S has some data for D and D is *non TLR-reachable*, S first discovers LDA_D using a mobility management method that is described in Section 3.

  Then, S sends packets by geodesic packet forwarding: the packet is sent to some neighbor X within a transmission range where the distance to D is reduced the most . At its turn, X performs the same steps: it checks whether D is TLR-reachable. If this is not the case, X sends the packet by geodesic packet forwarding. Otherwise, X uses TLR.

  In this simplest form, geodesic packet forwarding will often not work. If there is no connectivity along the shortest line, then the method fails.

  Our solution to this problem is to use *anchors*. An anchor is a point, described by geographical coordinates; it does not, in general, correspond to any terminode location. Anchors are computed by source nodes, using the path discovery methods. One such method is presented further in the paper. 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 it is close to 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, then the packet will arrive at the destination with a high probability. Figure 1 presents an example of AGPF.

- *Friend Assisted Path Discovery (FAPD)* is a path discovery method that is based on the concept of small world graphs [15]. It can be summarized as follows: 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 A can reach B by applying TLR, or because A managed to maintain one or several route vectors to B that work well. When A wants to discover a path to a destination C, then A may require assistance from a friend B. B may try to

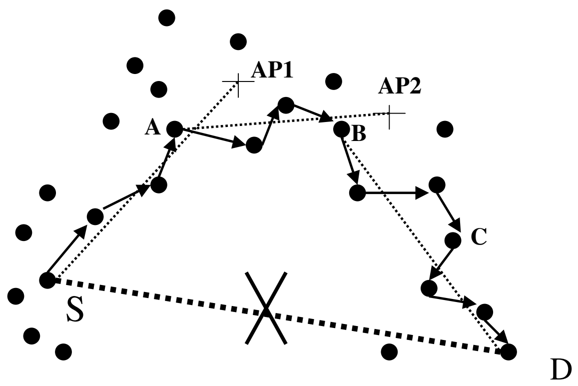


Figure 1: The figure presents how AGPF works when a terminode with EUI_S has some data to send to a terminode with EUI_D, and there is no connectivity along the shortest line from S to D. S has a path to D given by a list of geographical locations called anchored points: $\{AP1, AP2\}$. First, geodesic packet forwarding in the direction of $AP1$ is used. After some hops the packet arrives at a terminode A which finds that it is close to $AP1$. At A, the packet is forwarded by using geodesic packet forwarding in the direction of $AP2$. Second, when the packet comes to B, that is close to $AP2$, it starts sending the packet towards D. Last, when the packet comes to C it finds that D is TLR-reachable and forwards the packet to D by means of TLR.

find a path to C (perhaps with the help of its own friends). If B finds the desired path it returns it to A. A pays for the service provided by B in nuglets.

We view a terminode network as a graph, with edges representing the friends relation. We conjecture that this graph has the properties of a small world graph. Small world graphs are very large graphs that tend to be sparse, clustered and have a small diameter [15]. In a small world graph, roughly speaking, any two vertices are likely to be connected through a short sequence of intermediate vertices. This means that any two terminodes are likely to be connected with a small number of intermediate friends.

- Terminode Remote Routing is constantly modified by *Path Maintenance*.

  A terminode normally attempts to maintain several paths (described by route vectors) to any single destination of interest for it, and uses several of them in parallel. A terminode constantly monitors the cost of each path; the cost is given in terms of nuglets, packet loss and delay. Other factors like robustness, stability and security are also relevant to the cost of a path. This allows a terminode to improve paths, and delete obsolete or mal-functioning paths. In addition, information about the value of the paths is used for a terminode to decide how to split the traffic among the multiple paths that exist to the destination. A terminode sends more data along the paths that give the least congestion feedback information.

Performance of Terminode Routing

We carried out simulations of the TLR and TRR protocols. We briefly explain here the mobility model that was used in our simulations and some simulation results. For further details on the simulations, the interested reader is referred to [8].

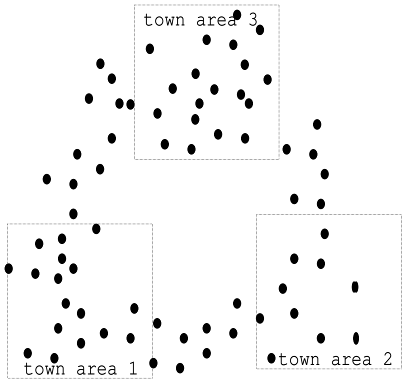


Figure 2: An example of the simulation area that consists of three towns. Terminodes stay within a scope of the same town for a certain number of movements, and then they choose at random another town area to which they move.

The simulation area is composed of a number of regions called "towns". Inside town areas, terminodes move according to the "random waypoint" mobility model. After a certain number of movements within the scope of the same town, a terminode moves to another town area. Terminodes that move between the town areas simulate highways between towns. We believe that this mobility model is closer to a real-life situation for a wide-area mobile ad-hoc network than the "random waypoint", since it better represents the fact that most people move for a certain period within one area, and then they move away to another distant area.

An example of the model of a simulated area that consists of three towns is presented in Figure 2. If source and destination are in two different towns, e.g., in towns area 1 and 2 respectively, the source may send data to the destination using two paths. One is the direct geodesic path that connects town 1 and town 2. Another path is via town 3 and this path consists of an anchor point in the area of town 3.

In [8], are presented in details simulation results with 600 terminodes moving according to the mobility model described above. These results show that the terminode routing is able to deliver over 80% of user data in a large and highly mobile simulation environment, where traditional MANET routing protocols, given that they are not designed for such environment, achieve less than 10%.

3 Mobility Management: the Virtual Home Region

Mobility management is performed by three components. Firstly, Terminode Local Routing (TLR) is able to track a destination terminode in the vicinity of a relaying terminode. Secondly, LDA management is performed by the method described below. It is required for Terminode Remote Routing (TRR). Thirdly, hosts that are engaged in a conversation keep track of each other using a tracking protocol, not described in this paper.

The main objective of LDA management is to distribute the location information inside the network in a dynamic, scalable, secure, and fair way, i.e., without privileging any node or region. At the same time, we are not concerned with maintaining the exact location information. All we require is that the LDA of the destination, learnt at the source, is accurate enough such that the packet eventually arrives at some terminode that finds the destination inside its TLR-reachable area.

Any mobility management system where the management is assigned in a fixed or static way to one or to a group of nodes is in conflict with the security and the peer-to-peer characteristics of a terminode network, because the node(s) that plays the manager role could profit from its position of superiority. Moreover, these systems are not applicable on a large scale, because they require a large amount of communication among nodes.

Therefore we introduce a new architecture where the information is dynamically distributed inside the network, and where the communication involved is only due to the upgrade or the retrieval of the location information. The main functions of this architecture are: (1) maintaining the location information, and (2) distributing the location information inside the network. These functions are performed in a reliable and robust way.

In this architecture, each node advertises its current position (LDA) to a geographical region called Virtual Home Region (*VHR*). The VHR has a fixed centre C_{VHR} and a variable radius that adapts to the density of the area containing the VHR, in order to maintain an approximately constant number of nodes inside the VHR.

The fixed centre is computed using some predefined, publicly known hash function H. H is a static mapping between the space of EUIs $\{EUI_i\}$ and the geographical space of a terminode network such that: $H(EUI_A) = C_{VHR}$ for each $A \in \{EUI_i\}$.

A terminode A does location update by sending position advertisements towards its VHR. All terminodes in A's VHR store the mapping between A's EUI and its LDA. They act as management system for A for the time they belong to A's VHR; once they leave it, they loose this role.

The radius of the VHR is increased or decreased if the number of nodes in the VHR is not adequate. This can happen either because there are too many nodes in the VHR, and the management and the retrieval of the location information requires too many communications, or because there are not enough nodes, and the system is not robust.

When a terminode B wants to retrieve the location of A (it must know A's EUI), it sends a query towards A's VHR (which can be computed by B since the hash function is publicly known). Once this request is received, the location information of A is sent back by the nodes of the VHR of A. This information is used to start a communication with A. During the communication, A and B rely on a direct system of mobility tracking. Figure 3 illustrates the distribution and the retrieval of the location information in a terminode network.

There are several possible location update schemes that can be applied in a terminode network.

The following schemes are proposed for personal communications networks(PCN)[14] and can be used in a terminode network. In the *timer-based* location update scheme, each terminode periodically sends a location update to its VHR. In the *distance-based* update scheme, each terminode tracks the distance it has moved since its last update and sends its location update whenever the distance exceeds a certain threshold. In the *predictive distance-based* scheme, the terminode reports to its VHR both its location and velocity. Based on this information, and a mobility pattern, the location of the terminode can be predicted. The terminode checks its location periodically and sends a location update to its VHR whenever the distance between the predicted location and its exact location exceeds the given threshold. When a terminode B needs location of a terminode A, it does the prediction of A's LDA from the information in the A's VHR. In our current design we use the *distance-based* location update scheme.

In order to have a robust and self-operating management, terminodes must cooperate

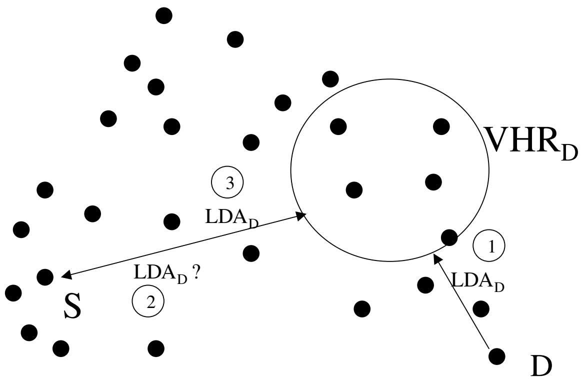


Figure 3: The figure presents one example of the distribution and retrieval of the location information. (1) The terminode D periodically sends its position (LDA_D) to its VHR. When a terminode S wants to communicate with D, it firstly computes the center of the VHR of D as $H(EUI_D)$ and then (2) sends a request toward the region around this point. When this request is received by the terminodes in the VHR of D, (3) LDA_D is sent back to S.

for storing location information, and serving as temporary distributed memory for other terminodes. This may be stimulated by paying nuglets to the terminodes in the VHR. The advantage of this approach is that it has reasonable amount of communications to distribute and retrieve location information, and no central or statically defined servers are necessary.

In the proposed solution for mobility management, a terminode B that needs a location of a close terminode A, may contact a potentially distant VHR of A. One possible solution to this problem is to organize the VHR-based mobility management in a hierarchical way in order to scale better in a large network. In this solution, every terminode would have several geographically distributed VHR that contain its location. For retrieving location information of another terminode, a terminode would contact the corresponding VHR that is closest to it. [9] presents how to geographically distribute location servers in a large network.

4 GPS-free positioning

Terminode positioning is used by every terminode to obtain its position. The position of a terminode can be obtained by means of the GPS positioning method. However, there are situations where GPS is not available. This happens, notably when the GPS signal is too weak (e.g., indoor), when it is jammed, or when a GPS receiver has to be avoided for cost or integration reasons.

In this section, we briefly describe the Self Positioning Algorithm (SPA) for positioning of terminodes in a terminode network that is GPS-free. SPA provides a position information to terminodes in the scenarios where an infrastructure does not exist and GPS cannot be used. Complete description of SPA is given in [4].

SPA uses distance measurements between terminodes to build the Network Coordinate System (NCS)(Figure 4). The Time of Arrival (TOA)[13] method is used to obtain the distance between two terminodes. Despite the distance measurement errors and the motion of terminodes, SPA provides sufficient location information and accuracy to sustain basic

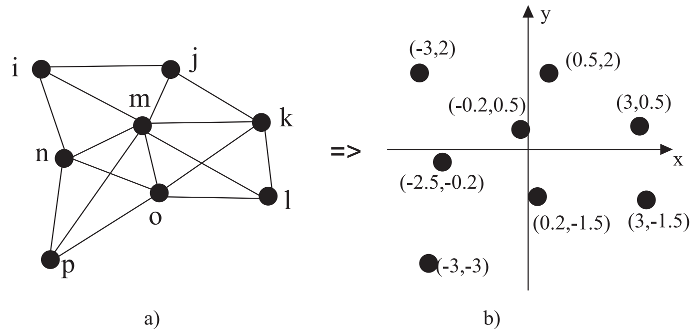


Figure 4: The Self Positioning Algorithm (SPA) uses the distances between the terminodes and builds the Network Coordinate System (NCS). Lines in Figure 3(a) represent the distances that terminodes can obtain by applying the TOA method. This is done by measuring signal propagation time between the two neighboring terminodes. Figure 3(b) shows the NCS. The value next to each terminode represent its position within the NCS.

network functions. For the sake of simplicity, we present SPA in two dimensions, but it can be easily extended to provide position information in three dimensions.

SPA is performed at each terminode and consists of the following steps:

- a terminode measures distances to its neighbors and sends this information to all its neighbors
- a terminode builds its Local Coordinate System (LCS) and computes the positions of its neighbors in LCS
- a terminode computes the density factor of its n-hop neighborhood (i.e. the number of terminodes in the n-hop neighborhood)
- a terminode with the highest density factor forms a Location Reference Group (i.e., the terminodes in its m-hop neighborhood) and computes the center and the direction of the Network Coordinate System
- all terminodes compute their position in the Network Coordinate System

Below, we define the operation of SPA in more details.

Local Coordinate System (LCS)

Every terminode i defines its Local Coordinate System (LCS_i) by choosing two neighbor terminodes p and q such that the distance d_{pq} between p and q is known, larger than zero and such that the terminodes i, p and q do not lay on the same line. Terminode i becomes the center of the LCS_i with the coordinates $(0, 0)$. The direction of LCS_i is defined such that terminode p lays on the positive x axis of the coordinate system and terminode q has a positive y component.

Every terminode i computes positions of its neighbors in its LCS_i. If the terminode j is the neighbor of i, p and q (this means that the distances d_{ij}, d_{qj}, d_{pj} are known to i) its position is then computed by triangulisation [13] (an intersection of three circles). This is

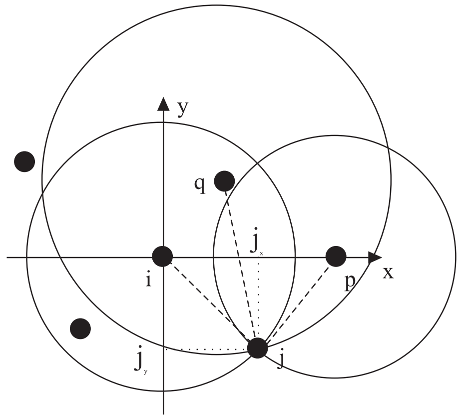


Figure 5: The terminode i defines its local coordinate system (LCS_i) by choosing two neighbors, e.g, p and q. The position of its neighbor j in LCS_i can be obtained by triangulisation. j is positioned at the intersection of the three circles with centers in i, p and q, and with radii equal to distances from these terminodes to j respectively.

illustrated in Figure 5. If k is not a neighbor of p and q, i obtains k's position in LCS_i by choosing two neighbors of k whose positions in LCS_i are already obtained.

The choice of p and q can be optimized with respect to the desired coverage and accuracy of the algorithm.

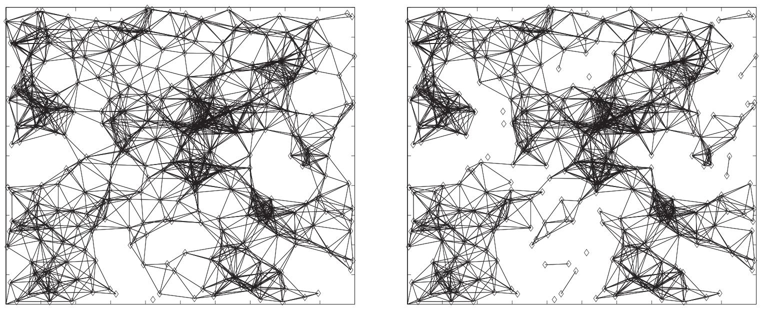
Network Coordinate System (NCS)

After building their local coordinate systems, terminodes compute their density factors. The terminode with the highest density factor will "slave" the other terminodes and its m-hop neighborhood becomes a *Location Reference Group (LRG)* of the network. The center and the direction of NCS are then computed as the geometric center of the terminodes in LRG and as the average of the directions of their coordinate systems, respectively. This information is then propagated to the terminodes in the network and they compute their position in NCS.

Performance of the Self Positioning Algorithm (SPA) and limitations

We have evaluated SPA and detailed performance results can be found in [4]. A network of terminodes is represented by a graph G_N, where vertices correspond to terminodes and an edge exists between a pair of terminodes if they are in each others power range. We construct another graph G_{GPS}, where vertices correspond to terminodes and an edge exists between a pair of terminodes if they can propagate the information about the NCS to each other. We observe the edge connectivity of these graphs, being the minimum number of edges whose removal from a graph make a graph disconnected. The edge connectivity of G_N is here referred to as the connectivity of the terminode network and the edge connectivity of G_{GPS} is referred to as the connectivity of SPA.

Clearly, the connectivity of SPA will always be smaller or equal to the connectivity of the terminode network. In the ideal case, the information about the NCS would be propagated between each pair of nodes that are in each others power range and thus the node connectivity



(a) (b)

Figure 6: An example of (a) network connectivity and (b) SPA connectivity for a network of 400 terminodes with a power range of 110 m and a node density of 400 terminodes/km^2

and SPA connectivity would be equal. The connectivity of SPA therefore shows the sensitivity of SPA to the given connectivity of the network.

Figure 6 illustrates the network connectivity and the connectivity of SPA for a randomly generated network of terminodes. In this example, for the chosen power range, the network connectivity is clearly higher than the SPA connectivity. The example also indicates and our results in [4] further show that not very high network connectivity ensures that the SPA connectivity remains larger than zero.

The accuracy of the positions obtained by SPA strongly depends on the distance measurements and on the speed of movement of terminodes. Higher speeds of the terminodes introduce additional errors and the positions of terminodes need to be frequently recomputed. Inaccurate positions of terminodes have negative impact on the performance of the packet forwarding algorithm in a terminode network.

5 Incentive to cooperation

In a terminode network, *all* networking services are provided by the terminodes themselves. However, service provision is not in the interest of terminodes (or more precisely, their users), because it consumes energy (reduces battery lifetime) without any direct advantages. Therefore, terminodes (their users) may tend to be selfish: they use services provided by the others, but they do not want to provide services to the community[1]. Clearly, selfish terminodes may hinder the functioning of the network completely. Therefore, a stimulation mechanism is required that encourages users to provide services to each other.

So far, wireless mobile ad-hoc networks have been envisioned mainly for military applications and crisis situations (e.g., in rescue operations). In both cases, the users of the network are assumed to belong to the same administration authority (e.g., to the same platoon, or to the same rescue team), and thus, they are naturally motivated to cooperate. In terminode networks, this assumption does not hold, because each user can be considered to be a distinct administration authority with selfish objectives.

[1]We assume that users have full control over their terminodes: they can tamper with its hardware and software, and modify its behavior. We understand that regular users usually do not have the required level of knowledge and skills to do this. Criminal organizations, however, can have enough interest and resources to reverse engineer a terminode and sell tampered terminodes with modified behavior on a large scale.

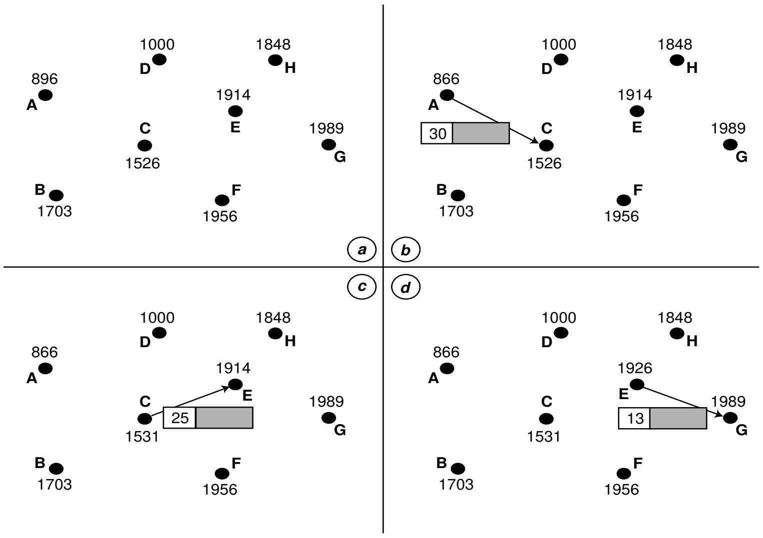


Figure 7: In the Packet Purse Model, the packet is loaded with nuglets by the originator. Forwarding terminodes take some nuglets out of the packet as a reward for the packet forwarding service they provide. In the figure, the numbers beside the terminodes represent their current stock of nuglets (a). When sending a packet to G, A loads 30 nuglets in it (b). Forwarding terminodes C and E then take 5 (c) and 12 (d) nuglets out of the packet, respectively.

Our approach to solve this problem and stimulate terminodes for cooperation is based on the introduction of a virtual currency, which we call *nuglets*, and mechanisms for charging/rewarding service usage/provision. We assume that the terminode hardware comes with an initial stock of nuglets, which have no monetary value and can only be used within terminode networks. The natural idea is that terminodes must pay for a service to those terminodes that provided the service. This makes nuglets indispensable for using the network, and thus, each (rational) user is interested in increasing her stock of nuglets. The exclusive way to achieve this is to provide services to the community. In the sequel, we illustrate this idea on a specific example: charging/rewarding the packet forwarding service.

Packet forwarding can be paid by either the originator or the destination of the packet. We call the approach in which the originator pays *Packet Purse Model*. In this model, 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 nuglets sufficient to reach the destination. Each forwarding terminode acquires some nuglets from the packet and thus, increases the stock of its nuglets. The exact number of nuglets taken out from the packet may depend on many things, including the cost of forwarding (in terms of battery power), the current battery status of the forwarding terminode, and its current number of nuglets. If a packet does not have enough nuglets to be forwarded, then it is discarded. Figure 7 illustrates the Packet Purse Model.

The main advantage of this model is that, besides stimulating cooperation among the terminodes, it may also deter users from sending useless data and overloading the network. The main disadvantage is that it might be difficult to estimate the number of nuglets that are required to reach a given destination.

This latter problem is overcome in the *Packet Trade Model* where the destination pays for the packet forwarding. In this model, the packet does not carry nuglets, but it is traded for nuglets by forwarding terminodes. Each forwarding terminode "buys" it from the previous one for some nuglets[2], and "sells" it to the next one (or to the destination) for more nuglets than it paid for. In this way, each forwarding node increases its number of nuglets, and the total cost of forwarding a packet is covered by the destination of the packet.

Besides relieving the originator of estimating the number of nuglets that would be required to deliver a packet, another advantage of this model is that it is better suited for multicast communications. A disadvantage is that this approach does not deter users from flooding the network.

Clearly, the models described above must be secured and protected against various attacks. The basic problems to be solved are related to nuglet forgery, protection of the integrity of the packet purse (in the Packet Purse Model), and the fair exchange of packets for nuglets (in the Packet Trade Model). Protection may be based on the application of a tamper resistant hardware module in each terminode, which can be used for the management of nuglets, and cryptographic coding of messages [2]. 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.

In order to see the effects of the introduction of the charging models on the performance of the network, we conducted appropriate simulations. We compared the throughput of the geodesic packet forwarding algorithm described in Section 2 to the throughput that the network achieves when this algorithm is extended with the Packet Purse Model. We simulated two versions of the Packet Purse Model: one in which each forwarding terminode acquires a constant number of nuglets, fixed by the originator, from the packet purse (PPM with Fixed Per Hop Charges); and another in which the number of nuglets charged by the forwarding terminodes is determined hop-by-hop using auctioning principles (PPM with Auctions). Figure 8 shows the results that we obtained for various initial battery levels. As expected, the throughput decreases when the Packet Purse Models are used, since, in this case, packets can be dropped by forwarding terminodes due to the low value of the packet purse or the fixed per hop charge. However, except for very low battery levels, the difference among the performances of the three algorithms is not significant (less than 5%). For further details on the simulations, the interested reader is referred to [3].

6 Security

Security in networks (including wireless mobile ad-hoc networks) is concerned with confidentiality and integrity of information, as well as legitimate use and availability of services. Although the security concerns remain the same, there are certain limitations in wireless mobile networks that typically are not found in fixed networks, and that make security problems more complex:

- Mobile ad-hoc networks do not have centralized monitoring and/or management points.
- Because of node mobility, the topology of the network changes dynamically; the nodes are often sporadically connected.
- The nodes communicate via wireless links, which can be eavesdropped easily.

[2] Except for the first forwarding terminode that receives the packet for free from the originator.

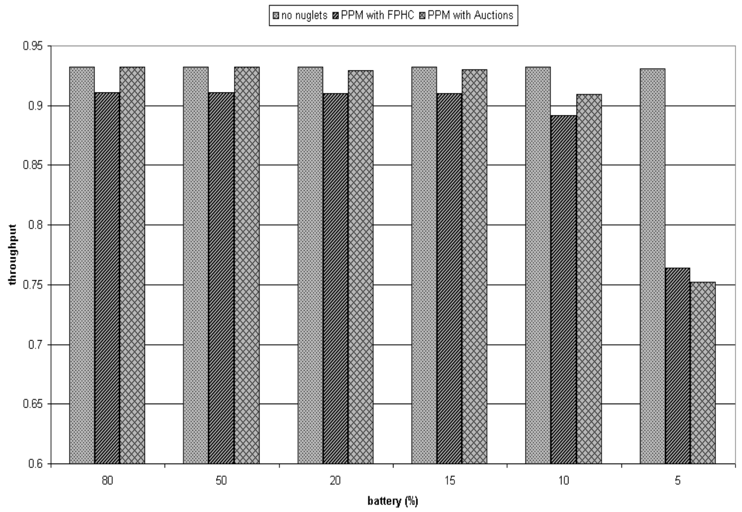


Figure 8: The figure shows the throughput of the network when the pure geodesic packet forwarding algorithm is used as well as when this algorithm is extended with the Packet Purse Models (PPM with Fixed Per Hop Charges and PPM with Auctions). The results show that, except for very low battery levels, the throughput does not decrease significantly with the introduction of the Packet Purse Models.

- The nodes are often battery powered, therefore communication and computing costs should be reduced.
- Because of their physical characteristics, the nodes have limited computing power (certainly smaller than non-mobile devices have).
- The nodes can be physically captured and compromised, unlike in fixed networks, where critical devices (e.g., routers) can be locked in "safe rooms".

A fundamental tool to achieve the network security objectives is cryptography. Cryptography is indispensable to confidentiality and integrity protection of information, and also used in mechanisms that ensure legitimate use of services (e.g., in authentication protocols). The challenge of using cryptography in a 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) certificate directories. Unfortunately, the application of certification authorities and certificate directories contradicts with the self-organized[3] and self-operated features of a terminode network.

[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 on the battlefield, which does not effect the key management problem in such a radical way as it does in a terminode network.

One possible approach to solve the key management problem may be based on the replacement of the certification authorities with communities of users (a PGP-like solution [16]) and the distribution of the certificate directory 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 [12] and those using implicitly certified keys [6]; however, this kind of solution still requires a trusted authority, at least at system initialization. We are investigating the way to provide public key cryptography in a totally self-organized manner.

7 Conclusion

We have presented a global description of some aspects of the project called Terminodes. More specifically, it can be described at three levels of abstraction.

- At the most concrete level, terminodes are a technical challenge, in the general domain of mobile ad-hoc networks. We have presented a global design of a terminode network. Self-organized routing, location management, GPS-less positioning, and nuglets are our main ingredients. The combination of a public environment with the absence of operator poses a number of challenges; we have shown how our global design addresses them by focusing on self-organization. A remarkable feature of terminodes is the presence of nuglets; it is used as the basis for inciting users to cooperate, and as a congestion control mechanism for discovery and routing mechanisms.

  We have focused in this paper on the most basic elements of a terminode infrastructure, mainly those related to the network layer, roughly speaking. There are many other important topics in the terminode project that we did not address in this paper. A first topic is the organization of software and components. Self-organization can be viewed as a form of competition, and a terminode component may become obsolete simply because more efficient ones exist, which are more able to get the best utility out of the network. Thus all of our components are modules that can be upgraded or completely modified as they become obsolete. Secondly, terminode applications are a way to continue the path opened up by internet peer-to-peer computing applications such as Gnutella: network crawling, search for information resources and highway traffic jam alerts are just a few examples. A key feature of all our design is self-organization. While this tends to make the design considerably more complex, we believe that the benefits in term of robustness and ease of use have the potential to change the way in which we think of networks and information systems.

- At the intermediate level, terminodes are an **intellectual stimulus**; in other words, they are a way to fuel creativity in order to identify new research challenges. An example of a question already generated is "How do we define a formal model for fair exchange".

- At the highest level of abstraction, terminodes are a **societal/political vision**, in which the ultimate aim of self-organized communication is considered. Indeed, we believe that long term research should contain a dimension that goes beyond purely technical questions.

References

[1] www.terminodes.org.

[2] 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)*, pages 87–96, August 2000.

[3] Levente Buttyán and Jean-Pierre Hubaux. Nuglets: a virtual currency to stimulate cooperation in self-organized mobile ad hoc networks. Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne, January 2001.

[4] Srdjan Capkun, Maher Hamdi, and Jean-Pierre Hubaux. GPS-free positioning in mobile Ad-Hoc networks. *Proceedings of the 34th HICSS*, January 2001.

[5] S. Giordano. Mobile ad-hoc networks. In *Handbook of Wireless Network and Mobile Computing, ed. I. Stojmenovic*. John Wiley & Sons, 2001, to appear.

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

[7] J.-P. Hubaux, T. Gross, J.-Y. Le Boudec, and M. Vetterli. Towards self-organized mobile ad-hoc networks: the terminodes project. *IEEE Communications Magazine*, January 2001.

[8] L. Blazevic, S. Giordano, J. Y. Le Boudec. Self Organized Terminode Routing. Technical Report DSC/2000/040, Swiss Federal Institute of Technology – Lausanne, December 2000.

[9] J. Li, J. Jannotti, D. De Couto, D. Karger, and R. Morris. A Scalable Location Service for Geographic Ad Hoc Routing. *Mobicom'00, Boston*, 2000.

[10] J.P. Macker, V.D. Park, and M.S. Corson. Mobile and wireless internet services: putting the pieces together. *IEEE Communications Magazine*, June 2001.

[11] Marc R. Perlman and Zygmunt J. Haas. Determining the Optimal Configuration for the Zone Routing Protocol. *IEEE JSAC*, 17(8), August 1999.

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

[13] M.I. Silventoinen and T. Rantalainen. Mobile station emergency locating in GSM. In *IEEE International Conference on Personal Wireless Communications*, 1996.

[14] V. W.-S. Wong, V. C.M. Leung. Location Management for Next-Generation Personal Communications Networks. *IEEE Network*, September/October 2000.

[15] D. J. Watts. *Small Worlds, The dynamics of networks between order and randomness.* Princeton University Press, 1999.

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