The NSPR, a Brazilian Radio with Capabilities that Fully Realize Mobile Ad Hoc Network

Carlos Cristiano Nunes, Sébastien R.M.J. Rondineau, Narcelio Ramos Ribeiro
Solentech, Avenida Senador Salgado Filho 7000, Viamão, RS, cep 94440-000, Brasil

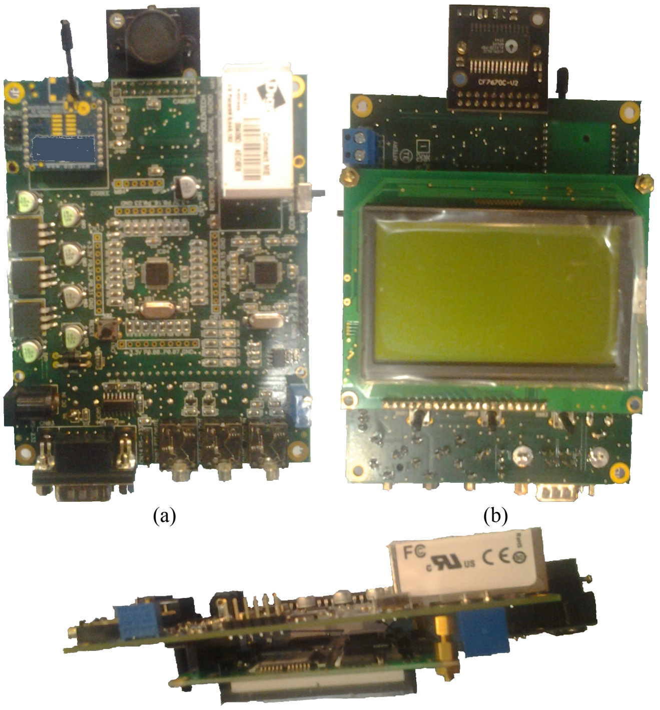
***Summary* — Mobile ad hoc networks (MANETs) represent complex distributed systems that comprise wireless mobile nodes that can freely and dynamically self-organize into arbitrary and temporary, ‘‘ad-hoc’’ network topologies, allowing people and devices to seamlessly internetwork in areas with no pre-existing communication infrastructure, e.g., disaster recovery environments or automated battlefields. Ad hoc networking concept is not a new one, having been around in various forms for over 30 years. Traditionally, tactical networks have been the only communication networking application that followed the ad hoc paradigm. The introduction of new technologies such as the Bluetooth, IEEE 802.11 and Hyperlan are helping enable eventual commercial MANET deployments outside the military domain. These recent evolutions have been generating a renewed and growing interest in the research and development of MANET. This paper attempts to provide a comprehensive overview of the Network Secure Personal Radio capabilities to fully realize mobile ad'hoc network inside the operational concept SisCOpEx, developped jointly with the Brazilian Army communication and electronic warfare center CComGEx.**

***Keywords* — Mobile Ad'Hoc Network, personal radio.**

I. INTRODUCTION

Historically, mobile ad hoc networks have primarily been used for tactical network related applications to improve battlefield communications/survivability. The dynamic nature of military operations means that military cannot rely on access to a fixed pre-placed communication infrastructure in battlefield. Pure wireless communication also has limitation in that radio signals are subject to interference and radio frequency higher than 100 MHz rarely propagate beyond line of sight (LOS) [1]. Mobile ad hoc network creates a suitable framework to address these issues by providing a multi-hop wireless network without pre-placed infrastructure and connectivity beyond LOS.

Early ad hoc networking applications can be traced back to the DARPA Packet Radio Network (PRNet) project in 1972 [1], which was primarily inspired by the efficiency of the packet switching technology, such as bandwidth sharing and store-and-forward routing, and its possible application in mobile wireless environment. PRNet features a distributed architecture consisting of network of broadcast radios with minimal central control; a combination of Aloha and CSMA channel access protocols are used to support the dynamic sharing of the broadcast radio channel. In addition, by using multi-hop store-and-forward routing techniques, the radio coverage limitation is removed, which effectively enables multi-user communication within a very large geographic area.


(a) (b)

(c)

Fig. 1. Pictures of the Network Secure Personal Radio in (a) top view, (b) buttom view, and (c) lateral view, that have capabilities to fully realize mobile ad hoc networks.

Survivable Radio Networks (SURAN) were developed by DARPA in 1983 to address main issues in PRNet, in the areas of network scalability, security, processing capability and energy management. The main objectives were to develop network algorithms to support a network that can scale to tens of thousands of nodes and withstand security attacks, as well as use small, low-cost, low-power radios that could support sophisticated packet radio protocols [1]. This effort results in the design of Low-cost Packet Radio (LPR) technology in 1987 [2], which features a digitally controlled DS spread-spectrum radio with an integrated Intel 8086 microprocessor-based packet switch. In addition, a family of advanced network management protocols was developed, and hierarchical network topology based on dynamic clustering is used to support network scalability. Other improvements in radio adaptability, security, and increased capacity are achieved through management of spreading keys [3].

Towards late 1980s and early 1990s, the growth of the Internet infrastructure and the microcomputer revolution made the initial packet radio network ideas more applicable and feasible [1]. To leverage the global information infrastructure into the mobile wireless environment, DoD initiated DARPA Global Mobile (GloMo) Information Systems program in 1994 [4], which aimed to support Ethernet-type multimedia connectivity any time, anywhere among wireless devices. Several networking designs were explored; for example Wireless Internet Gateways (WINGs) at UCSC deploys a flat peer-to-peer network architecture, while Multimedia Mobile Wireless Network (MMWN) project from GTE Internetworking uses a hierarchical network architecture that is based on clustering techniques.

Tactical Internet (TI) implemented by US Army at 1997 is by far the largest-scale implementation of mobile wireless multi-hop packet radio network [1]. Direct-sequence spread-spectrum, time division multiple access radio is used with data rates in the tens of kilobits per second ranges, while modified commercial Internet protocols are used for networking among nodes. It reinforces the perception that commercial wireline protocols were not good at coping with topology changes, as well as low data rate, and high bit error rate wireless links [5].

In 1999, Extending the Littoral Battle-space Advanced Concept Technology Demonstration (ELB ACTD) was another MANET deployment exploration to demonstrate the feasibility of Marine Corps war fighting concepts that require overthe-horizon (OTH) communications from ships at sea to Marines on land via an aerial relay. Approximately 20 nodes were configured for the network, Lucent 's WaveLAN and VRC-99A were used to build the access and backbone network connections. The ELB ACTD was successful in demonstrating the use of aerial relays for connecting users beyond LOS. In the middle of 1990, with the definition of standards (e.g., IEEE 802.11 [6]), commercial radio technologies have begun to appear on the market, and the wireless research community became aware of the great commercial potential and advantages of mobile ad hoc networking outside the military domain. Most of the existing ad hoc networks outside the military arena have been developed in the academic environment, but recently commercially oriented solutions started to appear (see, e.g., MeshNetworks and SPANworks).

Ad hoc networking issues

In general, mobile ad hoc networks are formed dynamically by an autonomous system of mobile nodes that are connected via wireless links without using the existing network infrastructure or centralized administration. The nodes are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. Such a network may operate in a standalone fashion, or may be connected to the larger Internet. Mobile ad hoc networks are infrastructure-less networks since they do not require any fixed infrastructure, such as a base station, for their operation. In general, routes between nodes in an ad hoc network may include multiple hops, and hence it is appropriate to call such networks as ‘‘multi-hop wireless ad hoc networks’’. Each node will be able to communicate directly with any other node that resides within its transmission range. For communicating with nodes that reside beyond this range, the node needs to use intermediate nodes to relay the messages hop by hop.

The ad hoc networks flexibility and convenience do come at a price. Ad hoc wireless networks inherit the traditional problems of wireless communications and wireless networking [7]:

- the wireless medium has neither absolute, nor readily observable boundaries outside of which stations are known to be unable to receive network frames;
- the channel is unprotected from outside signals;
- the wireless medium is significantly less reliable than wired media;
- the channel has time-varying and asymmetric propagation properties;
- hidden-terminal and exposed-terminal phenomena may occur.

To these problems and complexities, the multihop nature, and the lack of fixed infrastructure add a number of characteristics, complexities, and design constraints that are specific to ad hoc networking [8,9]:

Autonomous and infrastructure-less. MANET does not depend on any established infrastructure or centralized administration. Each node operates in distributed peer-to-peer mode, acts as an independent router and generates independent data. Network management has to be distributed across different nodes, which brings added difficulty in fault detection and management.

Multi-hop routing. No default router available, every node acts as a router and forwards each others packets to enable information sharing between mobile hosts.

Dynamically changing network topologies. In mobile ad hoc networks, because nodes can move arbitrarily, the network topology, which is typically multi-hop, can change frequently and unpredictably, resulting in route changes, frequent network partitions, and possibly packet losses.

Variation in link and node capabilities. Each node may be equipped with one or more radio interfaces that have varying transmission/receiving capabilities and operate across different frequency bands [10,11]. This heterogeneity in node radio capabilities can result in possibly asymmetric links. In addition, each mobile node might have a different software/hardware configuration, resulting in variability in processing capabilities. Designing network protocols and algorithms for this heterogeneous network can be complex, requiring dynamic adaptation to the changing conditions (power and channel conditions, traffic load/distribution variations, congestion, etc.).

Energy constrained operation. Because batteries carried by each mobile node have limited power supply, processing power is limited, which in turn limits services and applications that can be supported by each node. This becomes a bigger issue in mobile ad hoc networks because, as each node is acting as both an end system and a router at the same time, additional energy is required to forward packets from other nodes.

Network scalability. Currently, popular network management algorithms were mostly designed to work on fixed or relatively small wireless networks. Many mobile ad hoc network applications involve large networks with tens of thousands of nodes, as found for example, in sensor networks and tactical networks [1]. Scalability is critical to the successful deployment of these networks. The steps toward a large network consisting of nodes with limited resources are not straightforward, and present many challenges that are still to be solved in areas such as: addressing, routing, location management, configuration management, interoperability, security, highcapacity wireless technologies, etc.

As shown, the USA Army, as a national investment, has been developping, for the last 40 years, a completely integrated MANET. Brasil, with its own reality is starting the same process, which is the object of the next part.

II. THE SISCOPEX

The SisCOpEx is a Systems Operational Concept (CONOPS) that has been written jointly with the Brazilian Army (EB) communication and electronic warfare center (CComGEx). It is based on the constatations that, from brigade to platoon, C2 systems use radios to enable communication in broadcast or point to point, that these devices were incorporated into the EB, without having a formal CONOPS, generating the following facts:

- there are over 18,000 radio stations in the EB, purchased from different companies, without interoperability between them,
- when the Army operates in conjunction with the public security forces, civil defense and emergency services, there are difficulties to have secured communications, which complicates the coordination of actions,
- radios purchased abroad, because until then, there was no national solution,
- purchases done on resources opportunities,
- spending do not match the level of operation that could have been reached,
- there is low satisfaction with the material in use,
- sometimes purchased equipments were not consolidated at all (not even at home),
- suppliers without vision of the future,
- selling only equipment, not solution,
- tough logistics,
- inadequate training of mechanics,
- high unavailability of the equipments,
- suppliers treat Brasil like 3rd world country.

The SisCOpEx aims to solve these problems, investing, here in Brazil, in national technology, as The USA heavely did to create their first MANET in a long term program as shown in the introduction.

The SisCOpEx uses the concept of network-centric warfare (NCW) in a limited geographic area, composed of doctrine (capacity building, training, procedures, methods, concepts and tactics), technologies, tool for decision support, logistics and personnel, whose main purpose is to reduce the uncertainty of the decision of the operating environment and expedite the cycle of C2, with consequent increased likelihood of success and achievement of asymmetry in the activities of C2-level Brigade to Platoon.

Moreover, the SisCOpEx will enable interoperability within and between military services, Public Safety and Civil Defense.

The concept of NCW has marked the NATO C2 systems, and especially the armies of developed countries. It would be very difficult for Brazil to adopt this concept earlier because it required an expensive mobile and fixed structure. In SisCOpEx this cost is much lower, it will be incorporated into the concept of networks "On the Fly" or MANET, thus eliminating the need for costly infrastructure for deployment (back bone), and this bone is back susceptible to location, interference or physical destruction.

The concept of networks "on the fly" means each radio is at the same time, router and host system, allowing instant formation of networks, for a certain period of time and space delimited, for example, in any battlefield occupied by friendly forces or a smaller area, where operating a GC or a brigade. These networks are formed instataneaously as soon as two or more radios are turned on.

This type of network makes it very difficult to interrupt communications by friends stock electronic attack (blocking and deception) or physical destruction by the enemy, because if a node is destroyed or locked does not break the links, since all radios are system node.

Furthermore, it is also used the term "mesh sensors". This means using all sensors (electronic / electrical, mechanical, and especially humans) existing on the battlefield, in a network, to collect information and reduce the uncertainty of the decision. The following figure illustrates the advantages of working with meshes of sensors.

The effect can be achieved with the use of concepts such as mesh sensor networks, on the fly, data fusion and transformation of the doctrine enables accomplish several goals with the operational and logistical SisCOpEx.

Purpose

All processes, methods, tactics, tools, procedures, training, logistics and technology will be deployed by SisCOpEx in order to achieve the following objectives:

- increasing the decision success probability,
- increasing the situacional conciousness,
- increasing the synchronization capability,

- increasing the action velocity,
- reducing the cost,
- increasing the lethality,
- increasing the survivingness,
- increasing the interoperability.

Composition

The SISCOPEX is a complex system depends basically on four main components:

- *Sensors*. Its function is to collect data on operation environment and make them available on the networks. The sensors can be electrical / electronic, mechanical or human that is in the operational scenario. The combatant or system user, besides being an active agent, able to change the scenario, it is a potential sensor as it can see the enemy movements, sense the variations of weather in the area of operations, realizing the depth of a river etc. Use these skills to compose a sensor network in a systematic way is one of the advantages of SISCOPEX because the fighter, seen as a sensor, is spread on the ground for almost the entire area of operations.
- *Devices that create the networks, called Inter-combatant Networks (ICN) and Interface and Communications Gateway (ICG)*. The ICN aims to put people who need to share a common network operating environment. The ICN is established for single use radios (each combatant can have one). The ICG are devices that can do transceiver, gateway, router, and data fusion, or transmit data between different ICN or vertically. An ICG can have all the above functions or just a few. One of the functions of the ICG is the gateway and can receive data from a network in a given protocol or IEEE standards and transmission to another network with another protocol or standard. The information will transmit horizontally in the ICN (between fighters or other user) and migrate through the ICG vertically, enabling the information arrives at Brigade almost immediately. Likewise, it is possible that a "task order" issued by a fraction or the Brigade arrives on the desired network almost immediately.
- *Platforms* are meant to increase mobility and range of networks. The following types of platforms may exist: Human beings, Surface Mobile Units, Mobile Units Air, Space Unit.
- *The combatants or users*. It is the process active agent that is able to change settings and take advantage of what SisCOpEx can provide.

The SisCOpEx is not an isolated system, it is complementary to the EB C2 system, because it meets the needs of C2 from the brigade level to a GC and creates interfaces with other systems in which the EB is involved.

III. THE NSPR

The purpose of ICN radios is to create networks and subnetworks that enable the objectives of the SisCOpEx. The National Secure Personnal Radio (NSPR), as shown on Fig.1, created by the Brazilian company Solentech, is the first achievement toward the implantation of all the CONOPS objectives.

The NSPR can be described through the OSI model as follows.

Physical layer

The *physical layer* (PHY) ultimately provides the data transmission service, as well as the interface to the physical layer management entity, which offers access to every layer management function and maintains a database of information on related personal area networks. Thus, the PHY manages the physical *Radio Frequency* (RF) transceiver providing 18 dBm of RF output power and -102 dBm of RF input sensitivity and performs channel selection and energy and signal management functions. It operates on the unlicensed 2400-2500 MHz ISM frequency band divided in 14 channels with a rate of 115.2 kbit/s, based on *direct sequence spread spectrum* (DSSS) technique in the *Offset quadrature phase-shift keying* (*OQPSK*) modulation, to garantee:

- Resistance to intended or unintended jamming,
- Sharing of a single channel among multiple users,
- Reduced signal/background-noise level hampers interception,
- Determination of relative timing between transmitter and receiver.

Medium Acess Control layer

The medium access control (MAC) enables the transmission of MAC frames through the use of the physical channel. Besides the data service, it offers a management interface and itself manages access to the physical channel and network beaconing. It also controls frame validation, guarantees time slots and handles node associations. Finally, it offers hook points for secure services.

Protocol

The protocols build on recent algorithmic research (Ad-hoc On-demand Distance Vector - AODV, neuRFon) to automatically construct a low-speed ad-hoc network of nodes. In most large network instances, the network will be a cluster of clusters. It can also form a mesh or a single cluster. The current protocols support beacon and non-beacon enabled networks.

In non-beacon-enabled networks, an unslotted *carrier sense, multiple access/collision avoidance* (CSMA/CA) channel access mechanism is used. In this type of network, the Routers typically have their receivers continuously active, requiring a more robust power supply. However, this allows for heterogeneous networks in which some devices receive continuously, while others only transmit when an external stimulus is detected.

In beacon-enabled networks, the special network nodes called Routers transmit periodic beacons to confirm their presence to other network nodes. Nodes may sleep between beacons, thus lowering their duty cycle and extending their battery life. Beacon intervals depend on data rate; they may range from 15.36 milliseconds to 251.65824 seconds at 250 kbit/s, from 24 milliseconds to 393.216 seconds at 40 kbit/s and from 48 milliseconds to 786.432 seconds at 20 kbit/s. However, low duty cycle operation with long beacon intervals requires precise timing, which can conflict with the need for low product cost.

In general, the protocols minimize the time the radio is on, so as to reduce power use. In beaconing networks, nodes only need to be active while a beacon is being transmitted. In non-beacon-enabled networks, power consumption is decidedly asymmetrical: some devices are always active, while others spend most of their time sleeping. The basic channel access mode is CSMA. That is, the nodes talk in the same way that people converse; they briefly check to see that no one is talking before they start, with three notable exceptions. Beacons are sent on a fixed timing schedule, and do not use CSMA. Message acknowledgments also do not use CSMA. Finally, devices in Beacon Oriented networks that have low latency real-time requirements may also use Guaranteed Time Slots (GTS), which by definition do not use CSMA.

Network layer

The main functions of the network layer are to enable the correct use of the MAC sublayer and provide a suitable interface for use by the next upper layer, namely the application layer. Its capabilities and structure are those typically associated to such network layers, including routing.

On the one hand, the *data entity* creates and manages network layer data units from the payload of the application layer and performs routing according to the current topology. On the other hand, there is the layer *control*, which is used to handle configuration of new devices and establish new networks: it can determine whether a neighboring device belongs to the network and discovers new neighbors and routers. The control can also detect the presence of a receiver, which allows direct communication and MAC synchronization. The routing protocol used by the Network layer is, as aid earlier, AODV. In order to find the destination device, it broadcasts out a route request to all of its neighbors. The neighbors then broadcast the request to their neighbors, etc. until the destination is reached. Once the destination is reached, it sends its route reply via unicast transmission following the lowest cost path back to the source. Once the source receives the reply, it will update its routing table for the destination address with the next hop in the path and the path cost.

Nodes types

Nodes/devices are of three types:

- the *coordinator device* (CD): The most capable device, the coordinator forms the root of the network tree and might bridge to other networks. There is exactly one coordinator in each network since it is the device that started the network originally. It stores information about the network, including acting as the Trust Center & repository for security keys.
- the *Router device (RD)*: As well as running an application function, a router can act as an intermediate router, passing on data from other devices.
- the *End Device (ED)*: Contains just enough functionality to talk to the parent node (either the coordinator or a router); it cannot relay data from other devices. This relationship allows the node to be asleep a significant amount of the time thereby giving long battery life. An ED requires the least amount of memory, and therefore can be less expensive to manufacture than a RD or CD.

Topologies

Networks can be built as either peer-to-peer or star networks. However, every network needs at least one CD to work as the coordinator of the network. Networks are thus formed by groups of devices separated by suitable distances. Each device has a unique 64-bit identifier, and if some conditions are met short 16-bit identifiers can be used within a restricted environment. Namely, within each PAN domain, communications will probably use short identifiers.

Peer-to-peer (or point-to-point) networks can form arbitrary patterns of connections, and their extension is only limited by the distance between each pair of nodes. They are meant to serve as the basis for ad hoc networks capable of performing self-management and organization. Since the standard does not define a network layer, routing is not directly supported, but such an additional layer can add support for multihop communications. Further topological restrictions may be added; the standard mentions the cluster tree as a structure which exploits the fact that an ED may only be associated with one CD ou RD at a time to form a network where ED's are exclusively leaves of a tree, and most of the nodes are RD's and the CD. The structure can be extended as a generic mesh network whose nodes are cluster tree networks with a local coordinator for each cluster, in addition to the global coordinator.

A more structured star pattern is also supported, where the coordinator of the network will necessarily be the central node. Such a network can originate when an RD or CD decides to create its own PAN and declare itself its coordinator, after choosing a unique PAN identifier. After that, other devices can join the network, which is fully independent from all other star networks.

Data transport architecture

Frames are the basic unit of data transport, of which there are four fundamental types (data, acknowledgment, beacon and MAC command frames), which provide a reasonable tradeoff between simplicity and robustness. Additionally, a superframe structure, defined by the coordinator, may be used, in which case two beacons act as its limits and provide synchronization to other devices as well as configuration information. A superframe consists of sixteen equal-length slots, which can be further divided into an active part and an inactive part, during which the coordinator may enter power saving mode, not needing to control its network.

Within superframes contention occurs between their limits, and is resolved by CSMA/CA. Every transmission must end before the arrival of the second beacon. As mentioned before, applications with well-defined bandwidth needs can use up to seven domains of one or more contentionless guaranteed time slots, trailing at the end of the superframe. The first part of the superframe must be sufficient to give service to the network structure and its devices. Superframes are typically utilized within the context of low-latency devices, whose associations must be kept even if inactive for long periods of time.

Data transfers to the coordinator require a beacon synchronization phase, if applicable, followed by CSMA/CA transmission (by means of slots if superframes are in use); acknowledgment is optional. Data transfers from the coordinator usually follow device requests: if beacons are in use, these are used to signal requests; the coordinator acknowledges the request and then sends the data in packets which are acknowledged by the device. The same is done when superframes are not in use, only in this case there are no beacons to keep track of pending messages.

Point-to-point networks may either use unslotted CSMA/CA or synchronization mechanisms; in this case, communication between any two devices is possible, whereas in "structured" modes one of the devices must be the network coordinator.

In general, all implemented procedures follow a typical request-confirm/indication-response classification.

Reliability and security

The physical medium is accessed through a CSMA/CA protocol. Networks which are not using beaconing mechanisms utilize an unslotted variation which is based on the listening of the medium, leveraged by a random exponential backoff algorithm; acknowledgments do not adhere to this discipline. Common data transmission utilizes unallocated slots when beaconing is in use; again, confirmations do not follow the same process.

Confirmation messages may be optional under certain circumstances, in which case a success assumption is made. Whatever the case, if a device is unable to process a frame at a given time, it simply does not confirm its reception: timeout-based retransmission can be performed a number of times, following after that a decision of whether to abort or keep trying.

Because the predicted environment of these devices demands maximization of battery life, the protocols tend to favor the methods which lead to it, implementing periodic checks for pending messages, the frequency of which depends on application needs.

Regarding secure communications, the MAC sublayer offers facilities which can be harnessed by upper layers to achieve the desired level of security. Higher-layer processes may specify keys to perform symmetric 128-bit AES cryptography to protect the payload and restrict it to a group of devices or just a point-to-point link; these groups of devices can be specified in acess control lists. Furthermore, MAC computes *freshness checks* between successive receptions to ensure that presumably old frames, or data which is no longer considered valid, does not transcend to higher layers.

In addition to this secure mode, there is another, insecure MAC mode, which allows access control lists merely as a means to decide on the acceptance of frames according to their (presumed) source.

Application layer

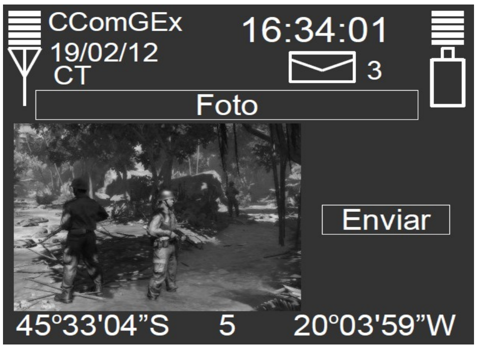
The application layer of the radio is a complex coordination, through an ARM7 microprocessor, of several perifercs to fit into small frames circulating at a low data rate of 115.200 kbit/s:

- an OLED display,
- a GPS receiver using NMEA protocol to be fully integrated in the C2 Cmb,
- serial 232 / Ethernet communication ports,
- a low resolution color camera,
- a vocoder, with speakers and microphone,
- rechargeable battery.

The firmware running on the ARM-based processor uses *Finite-State Machine (FSM)* techniques to channel all traffic data through different connected peripheric hardware, routing and prossessing sub-frames onto a final application frame, converted to the RF packet that hops on the network. A tremendous effort has been put into the software design, using advanced aproaches, in order to turn possible the mission-critical achievement under a non-complex hardware platform. Individual priority levels are given to each peripheral (e.g. GPS, Keypad, Display, Audio and Video). An "Application Sense" algorithm, providing a friendly *Graphic User Interface (GUI)*, redistributes all these levels at every iteraction.

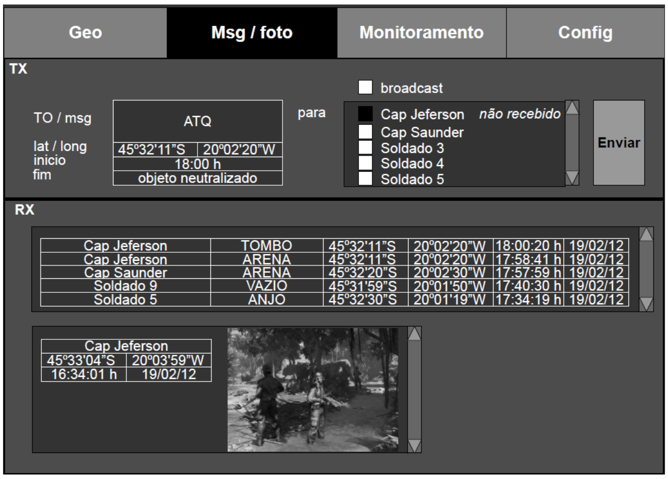
All the three devices kinds (CD, RD, ED) are using the exactly same hardware configuration. The differences are in the parametrization of the firmware.

Another part of the application layer is included in a computer linked to the CD. This application creates a log any event such as message and picture transfert as shown on fig.3, or the real-time geolocalization of each radio as shown on fig.4.



CComGEx 16:34:01
19/02/12
CT
✉ 3
Foto
Enviar
45°33'04"S 5 20°03'59"W

Fig. 2. One screen shot of the NSPR display when ready to send a picture.



Geo | Msg / foto | Monitoramento | Config

TX

TO / msg: ATQ
lat / long: 45°32'11"S 20°02'20"W
inicio: 18:00 h
fim: objeto neutralizado

para
□ broadcast
■ Cap Jeferson *não recebido*
□ Cap Saunder
□ Soldado 3
□ Soldado 4
□ Soldado 5

Enviar

RX

Cap Jeferson	TOMBO	45°32'11"S	20°02'20"W	18:00:20 h	19/02/12
Cap Jeferson	ARENA	45°32'11"S	20°02'20"W	17:58:41 h	19/02/12
Cap Saunder	ARENA	45°32'20"S	20°02'30"W	17:57:59 h	19/02/12
Soldado 9	VAZIO	45°31'59"S	20°01'50"W	17:40:30 h	19/02/12
Soldado 5	ANJO	45°32'30"S	20°01'19"W	17:34:19 h	19/02/12

Cap Jeferson
45°33'04"S 20°03'59"W
16:34:01 h 19/02/12

Fig. 3. Screen shot of the computer display linked to the CD when checking data transfered such as pre-existing messages and low resolution pictures.

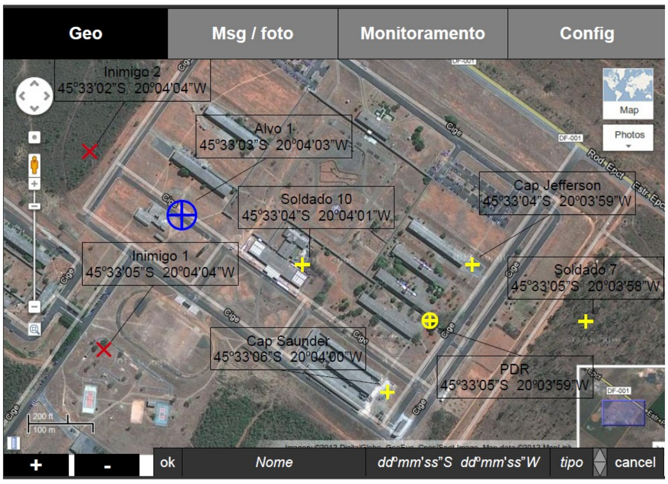


Fig. 4. Screen shot of the computer display linked to the CD when geolocalized data such as position of each NSPR in real-time.

The CD can also be plugged into a computer to have access to the real-time position of each radio, and keep an historical logfile of each event.

This digital radio transmits data, pre-existing messages, voice and static images as shown on fig.2. The routing function has also been tested and approved by the CComGEx in June 2012. During these tests, it has been noticed that the use of the 128-bit AES cryptography, which drastically reduces the real data payload, slightly degrades the link performances between two radios in a hop.

IV. Final Observations

As the USA are doing for a very long time, Brazil is starting to invest in MANET through its national capabilities. Indeed, the Brazilian Army communication and electronic warfare center CComGEx wrote jointly with Solentech, a Brazilian company, a CONOPS called SisCOpEx to achieve the following objectives:

- increasing the decision success probability,
- increasing the situacional conciousness,
- increasing the synchronization capability,
- increasing the action velocity,
- reducing the cost,
- increasing the lethality,
- increasing the survivingness,
- increasing the interoperability.

Based on that CONOPS, the Brazilian company Solentech developped and designed the National Secure Personnal Radio (NSPR), which is a radio which capabilities fully realize mobile ad hoc network. The NSPR is first of a family that fits the ICN concept and later on the IGN concept.

Acknowledgements

The authors wish to acknowledge the General A. Santos Guerra for giving the opportunity to work on this huge challenge through the access to the CComGEx facilities. Special thanks to both Cap Saunders and Cap. Jefferson for their collaboration in writing the SisCOpEx, another special thanks to Cap. Farno for testing of the NSPR capabilities, and to Maj. Knevitz for the overall coordination. Many thanks to Dr Hugo Saporetti from INATEL for providing the application part implemented in the computer that connects to the CD.

REFERENCES

[1] James A. Freebersyser, Barry Leiner, A DoD perspective on mobile ad hoc networks, in: Charles E. Perkins (Ed.), Ad Hoc Networking, Addison Wesley, Reading, MA, 2001, pp. 29–51.

[2] W. Fifer, F. Bruno, The low-cost packet radio, Proceedings of the IEEE 75 (1) (1987) 33–42.

[3] N. Shacham, J. Westcott, Future directions in packet radio architectures and protocols, Proceedings of the IEEE 75 (1) (1987) 83–99.

[4] B. Leiner, R. Ruth, A.R. Sastry, Goals and challenges of the DARPA GloMo program, IEEE Personal Communications 3 (6) (1996) 34–43.

[5] J. Strater, B. Wollman, OSPF Modeling and Test Results and Recommendations, Mitre Technical Report 96W0000017, Xerox Office Products Division, March 1996.

[6] IEEE standard for Wireless LAN- Medium Access Control and Physical Layer Specification, P802.11, November 1997. See also.

[7] IEEE P802.11/D10, January 14, 1999.

[8] M.S. Corson, J.P. Maker, J.H. Cernicione, Internet-based mobile ad hoc networking, IEEE Internet Computing 3 (4) (1999) 63–70.

[9] C.-F. Chiasserini, R.R. Rao, Pulsed battery discharge in communication devices, in: Proceedings of The Fifth Annual ACM/IEEE International Conference on Mobile Computing and Networking (MOBICOM 99), August 15–19, 1999, Seattle, WA, pp. 88–95.

[10] I. Chlamtac, A. Lerner, Link allocation in mobile radio networks with noisy channel, in: IEEE INFOCOM, Bar Harbour, FL, April 1986.

[11] I. Chlamtac, A. Lerner, Fair algorithms for maximal link activiation in multi-hop radio networks, IEEE Transactions on Communications COM-35 (7) (1987).