Disruption-Tolerant Content-Driven Information Dissemination in Partially Connected Military Tactical Radio Networks

Julien Haillot, Frédéric Guidec, Serge Corlay, Jacques Turbert

DISRUPTION-TOLERANT CONTENT-DRIVEN INFORMATION DISSEMINATION IN PARTIALLY CONNECTED MILITARY TACTICAL RADIO NETWORKS

Julien Haillot and Frédéric Guidec
VALORIA, Université de Bretagne Sud
Université Européenne de Bretagne
Vannes, France
{julien.haillot|frederic.guidec}@univ-ubs.fr

Serge Corlay and Jacques Turbert
CELAR (Centre d'Electronique de l'Armement)
DGA (French Armament Procurement Agency)
Rennes Armées, France
{serge.corlay|jacques.turbert}@dga.defense.gouv.fr

***Abstract*—*In this paper we address the problem of supporting communication in partially connected military tactical radio networks. In such networks traditional multi-hop forwarding techniques cannot guarantee end-to-end communication. Alternative techniques must therefore be designed to compensate for connectivity disruption. We propose a communication model that relies on opportunistic disruption-tolerant networking techniques to support information dissemination in highly fragmented military tactical radio networks. This model we designed is specifically devoted to content-driven information dissemination: pieces of information can be published on a terminal, disseminate in the network by being stored, carried, and forwarded by mobile terminals, and be received ultimately by terminals that have subscribed to receive this kind of information. This model was implemented in a middleware platform we developped, and tested on an experimental testbed composed of the French VHF battlefield radios PR4G.*

Acknowledgments: The work presented in this paper is supported by the French Agence Nationale de la Recherche under contract ANR-05-SSIA-0002-01. It is also supported by the French Armament Procurement Agency (DGA) by means of a Ph.D. grant.

INTRODUCTION

Initially produced as a voice-only combat net radio, the French VHF battlefield radio PR4G has recently acquired IP networking capabilities, multiplexing voice and data to fulfill the requirements of network centric operations. The evolution of military tactical radio networks (featuring new technologies such as IP networking, ad hoc routing protocols, increased throughput) contributes to ease the deployment of battlefield networks, and offers new perspectives for information sharing. Yet, these combined technologies do not make it possible to face all battlefield situations. Indeed, in a military tactical radio network connectivity can be disrupted because of a limited number of radio units, the mobility or lacunar deployment of these units, shadow loss, spot jamming, or even the occasional destruction of some radio units. Even if current technologies can tolerate short-time –up to a few minute– disruptions between network units, they can hardly ensure communication between units that observe long-time connectivity disruptions (between about ten minutes and several hours). Indeed, the topology of a highly disrupted tactical radio network can appear as shown in Figure 1: instead of a single connected graph, the whole network appears as a collection of smaller graphs –often referred to as "connectivity islands" in the litterature– that each represent a connected fragment of the network. Communication is possible within one island (using possibly multi-hop forwarding techniques), but no communication is possible between distinct islands. Of course, the topology of a radio-based network changes over time. As radio units move in the area covered by the network new links can appear, or be altered, thus leading to the merging or splitting of network fragments. Yet there is no guarantee that an end-to-end path can ever exist between any pair of nodes in the network.

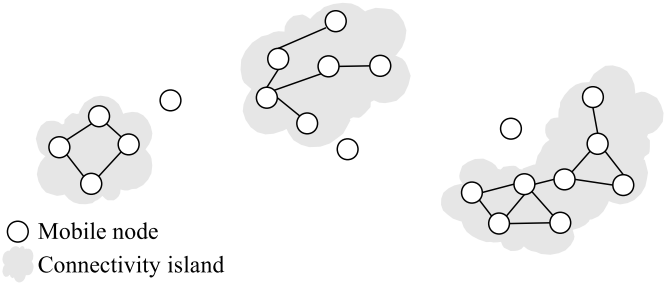

Figure 1. Example of a partially connected tactical radio network

Ensuring end-to-end communication in a disrupted radio network such as that shown in Fig. 1 is an interesting challenge. Several protocols for unicast, multicast, or broadcast forwarding in disrupted networking environments have been proposed in the litterature during the last decade. As a general rule, the approach consists in using mobile hosts as *carriers* –or data mules– for transporting messages

between non-connected parts of the network. Each mobile host is therefore expected to *store*, *carry*, and *forward* messages according to a set strategy, the main difficulty being to decide which hosts are the best carriers for each message. Good surveys of works conducted along this line can be found in [1] and [2].

In this paper we follow the same line as the US DoD research project BBN SPINDLE [3], as we specifically consider the problem of ensuring content-driven information dissemination in partially connected radio networks. This objective differs significantly from traditional destination-based networking, for in content-based networking information must flow towards interested receivers rather than towards specifically set destinations [4]. Content-based communication therefore fits the needs of applications dedicated to information sharing and event distribution. Note that content-based networking should not be confused with multicast networking, for it is actually more powerful and more flexible than plain multicast. For one thing, content-based communication does not require that specific channels or groups be identified prior to any actual transmission. Besides, the criteria that determine whether a particular piece of information should be received by one or another receiver can be different on each receiver.

In fully-connected, stable wired networks, content-based networking is usually achieved by constructing a communication overlay that covers the whole physical point-to-point network, and that supports the forwarding of each piece of information from its sender to all interested receivers [5], [6]. This approach is hardly applicable in a partially connected network, since the absence of end-to-end connectivity precludes building an overlay that covers the whole network.

The model we propose to meet this challenge is inspired from the –somewhat abstract– Autonomous Gossiping (A/G) algorithm [7], for which ours can be perceived as an effective implementation (to the best of our knowledge, the A/G algorithm has never been implemented and used in real conditions). This model exploits transient contacts between mobile hosts to exchange pieces of information. Indeed, each host is characterized by a profile that defines the kind of information it is primarily interested in. This profile can be derived from the needs expressed by application services running locally on that host. It can also be altered –or defined altogether– by an administrator of that host. When a host meets another host, it uses this opportunity to obtain pieces of information that match its own interest profile, while providing the neighbor host with pieces of information that match its profile. Any piece of information a host manages to obtain during a radio contact is passed to local application services (if any), but it is also stored in a local cache for a while. Each mobile host therefore serves as a carrier for pieces of information it maintains in its cache. Thus, our model also relies on the *store, carry, and forward* principle, allowing information to disseminate network-wide thanks to mobile hosts that help bridge the gap between otherwise non-connected fragments of the network.

In the remainder of this paper we provide more details about our communication model, and give an overview of a middleware platform we implemented based on this model. An illustration scenario is depicted, which shows how our middleware platform could be used to help disseminate tactical information in a fragmented radio network. This scenario was actually run on an experimental testbed composed of PR4G tactical radios. We report observations made during this experiment, and provide a few figures that show how our middleware performs in realistic conditions. We conclude this paper by listing possible directions for future work.

COMMUNICATION MODEL

Our approach relies on a combination of the Publish/Subscribe paradigm with the principles of opportunistic and disruption-tolerant networking.

The model we designed is document-oriented rather than being simply message-oriented. A document is a structured piece of information a mobile host can either publish in the network, or receive from the network. Its main elements are a descriptor and a payload. The descriptor is meant to provide meta-information about the the payload, such as its origin and/or its destination, its type, a list of characteristic keywords, etc.

According to the Publish/Subscribe model, a host is only meant to receive documents for which it has subscribed for. An interesting consequence of this model is that it yields a clear decoupling between information producers and consumers. A document can be published even when no subscriber is available to receive it, and it will be received later by subscribers even after the publisher has moved away, or left the network altogether *(time decoupling)*. A document can also be published without regard to the identity of potential subscribers *(addressing space decoupling)*. Time decoupling and space decoupling between information publishers and subscribers both fit pretty well the loosely coupled nature of partially or intermittently connected networks, such as the radio-based military tactical networks we consider in this paper.

In fully-connected wired networks, information dissemination based on the Publish/Subscribe model is usually obtained by installing servers dedicated to storing all published messages (or documents) until they can be re-

trieved by subscribers. Alternatively, content-driven routing structures can be established in order to forward messages directly from publishers to subscribers.

In a partially connected network, though, such solutions can hardly be applied. Indeed there is no guarantee that temporaneous end-to-end forwarding paths can ever exist between publishers and subscribers. Besides, no host is stable and accessible enough to play the role of a server for all other hosts. Our approach therefore consists in implementing a peer-to-peer model (rather than a client-server one), whereby all mobile hosts cooperate to disseminate documents network-wide.

As mentioned before our model takes inspiration from the Autonomous Gossiping (A/G) algorithm [7]. The interest profile of a host is actually defined as a combination of predicates characterizing the different kinds of documents (if any) it has subscribed for. Whenever a mobile host manages to obtain a new document that matches its own interest profile, this document is stored in a cache for a while, so it can later be proposed to other mobile hosts and forwarded to these hosts if they are interested by this document. By storing, carrying, and forwarding a document while moving in the network, each host therefore helps disseminate this document far beyond the radio range of its publisher.

An overview of the protocol we designed in order to support the dissemination of documents in a disconnected network is sketched below. Details of how this protocol is actually implemented in a middleware platform we developed are given in the next section.

In our system, each host periodically broadcasts an announcement in order to inform its neighbors (if any) about its identity and interest profile. This announcement can optionally include a catalog of document descriptors, as explained below. By sending such an announcement periodically, a node informs its neighbors about its presence and about the kinds of documents it is interested in. Conversely, by receiving similar announcements a host discovers its neighbors, and learns about their own interest profiles. By matching its neighbor's profiles against the descriptors of the documents it maintains in its cache, a host can select descriptors of documents that might be of interest to at least one of its current neighbors. It can thus build a catalog containing these descriptors, and incorporate this catalog in its next announcement.

Upon receiving such a catalog, each host matches the descriptors it contains against its own interest profile in order to identify documents that match this profile –that is, documents it is interested in– and that are not already present in its local cache. If such documents are identified, then a request for these documents is sent to the announcer, which complies by sending the missing documents on the radio channel.

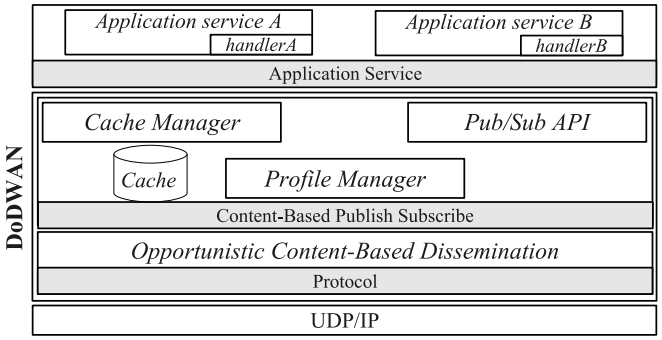

Figure 2. Architecture of the DoDWAN middleware

Finally, when a host receives a document it has requested, this document is put in the local cache so it can later be proposed to other hosts met while moving in the network. Of course, this communication model that relies on mobile carriers to transport information can yield significant latency that applications have to take into account while sharing information.

THE DODWAN MIDDLEWARE PLATFORM

Figure 2 provides an overview of a middleware platform we developed according to the model described in the former section. This platform is called DoDWAN (for Document Dissemination in disconnected mobile Wireless Ad Hoc Networks). It has been fully implemented in Java, and is now distributed under the GNU Lesser General Public Licence[1].

DoDWAN provides high-level application services with a publish/subscribe API. Through this API an application service can *publish* a document, and *subscribe* to receive specific kinds of documents. As a general rule, a mobile host that subscribes to receive a particular kind of document is expected to serve as a mobile carrier for this kind of document. Yet a host can also be configured so as to serve as an altruistic carrier for documents that present no interest to the application services it runs locally. This behavior is optional, though, and it must be enabled explicitly by an administrator of the DoDWAN platform.

Cache Manager: Each instance of the DoDWAN platform maintains a cache, in which documents can be stored for a while. This cache is under the responsibility of a *Cache Manager* (see Figure 2) that decides which documents to put in the cache and which to remove when needed. Obviously all mobile hosts involved in a radio network do not necessarily have the same characteristics. Most notably small hand-held devices are usually resource-limited and cannot allocate much storage space for DoDWAN's cache. Conversely, larger devices such as laptops or

[1]http://www-valoria.univ-ubs.fr/CASA/DODWAN

even workstations can maintain a large cache and therefore store many documents in transit. In any case, both the capacity of the cache and the policy enforced by the *Cache Manager* can be different on different mobile hosts running DoDWAN.

Documents and document descriptors: As mentioned in the former section a document in the model we designed is composed of two main parts: a descriptor, and a payload. In DoDWAN the payload is simply perceived as a sequence of raw bytes. The descriptor is a collection of attributes that each combine a name and a value. These attributes are meant to be freely defined by the developers of application services built on top on DoDWAN. The only exceptions to this rule are a Unique Document Identifier (UDI) and a Document DeadLine (DDL), that must appear in any document's descriptor. The UDI allows DoDWAN to differentiate documents, while detecting duplicate copies of the same document. Its value is automatically calculated by DoDWAN based on a combination of the publisher's MAC address and of the document payload's MD5 hash key. The Document DeadLine (DDL) can be specified by the application service that publishes a document. It is meant to indicate how long this document should disseminate in the network, and therefore how long copies of this document should be kept by mobile hosts in their local cache.

In the current implementation of DoDWAN, descriptors are formatted in XML. This approach was chosen because of the flexibility of the XML syntax, and because of the many tools available for parsing and processing XML structures. A compression algorithm (detailed below) is however used in order to compensate for the verbosity of the XML syntax.

Predicates and interest profile: Whenever an application service subscribes to receive a particular kind of document, it provides a predicate that characterizes this kind of document. Predicates are expressed using the XPATH syntax. For example, if an application service is interested in documents containing JPEG images and published by *User56* after February 28th, the selection predicate for such documents could be `[publisher='User56' AND productionDate<='28 February 2009' AND type='image/jpg'].`

The *Profile Manager* (see Fig. 2) collects all subscription predicates specified by local application services, and defines the host's interest profile accordingly. Basically, this profile is simply a combination of all subscription predicates. It defines the whole set of document types the local host is interested in, and should thus strive to obtain from other hosts.

Resilience to connectivity disruptions: DoDWAN peers interact with each other by exchanging control and data messages encapsulated in UDP datagrams. No session –and especially no TCP session– is ever established between neighbor hosts because of the high level of connectivity disruptions expected between these hosts. As a general rule, interactions between neighbor peers rely on an opportunistic scheme rather than on a strict transactional scheme. Each peer only maintains soft-state information about its neighbors. Thus, whenever a node broadcasts an announcement, for example, some of its neighbors may fail to receive this announcement, without ever compromising either the sender or any potential receiver. Likewise, whenever a node requests a message and fails to obtain this message, it simply waits until it can get another chance to grab this message (either from the same neighbor, or from a different one).

Document compression and fragmentation: While designing our middleware platform, we strived to make it as frugal as possible regarding the resources it consumes, and especially regarding its consumption of wireless bandwidth: both the number and the size of the messages required for disseminating documents are kept at a minimum. Moreover, all kinds of messages (i.e. periodic announcements, requests, and the actual documents published by application services) are systematically transmitted in a compressed form. In its current implementation DoDWAN relies on the LZ77 lossless data compression algorithm, as defined by Lempel and Ziv in 1977. It additionally supports the segmentation and reassembly of large documents that cannot fit in a single IP packet, even in compressed form. Each fragment resulting from this segmentation takes the form of a full-featured document, which shares the same descriptor as the original document. Fragment documents can therefore propagate independently of each other in the whole network, and be reassembled only when they reach a host whose interest profile matches the descriptor of the original document. This possibility for document fragments to propagate separately in the network brings in robustness to the whole dissemination process, as a mobile host can help in the dissemination of a document even if it only owns copies of some of the fragments that compose this document.

Compatibility with wireless transmission technologies: To date DoDWAN can drive either Wi-Fi interfaces (running in ad hoc mode) or PR4G tactical radios. Several application services involving DoDWAN and Wi-Fi interfaces have already been developed, such as a peer-to-peer system for component-based software deployment, or peer-to-peer versions of the legacy email and newsgroup services. In the next section we address the problem of using DoDWAN in a military tactical network involving PR4G radios.

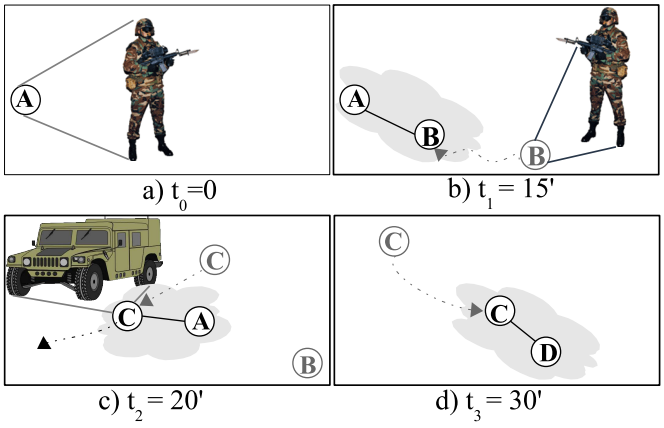

Figure 3. Scenario of radio contacts between mobile units

ILLUSTRATION SCENARIO

In this section we present a scenario that depicts how DoDWAN-enabled terminals could be used to ensure information dissemination in a battlefield environment. For the sake of clarity this scenario only involves a couple of mobile terminals. In real conditions dozens of terminals could rely on our middleware to publish and receive documents. Figure 3 shows the mobility scenario of terminals, and Figure 4 exposes the timeline of communication between these terminals according to this scenario.

Warfighter A is conducting an observation mission on the frontline and is currently out of radio contact with his group leader D. Other warfighters roam the area in order to help in the communication between A and D. Tactical observations made by A must be transferred to D as fast as possible, without interrupting A's mission.

At time t_0 (see Fig. 3-a) A starts up his terminal T_A in order to publish a document pertaining to battlefield conditions (typically a short text message describing something he has observed recently, an annotated map, or even a picture he has taken with a digital camera). As soon as T_A is enabled, the DoDWAN middleware it runs starts broadcasting a periodic announcement. The document D1 published by warfighter A is not sent immediately on the radio channel, though. It is first simply put in T_A's local cache, which possibly already contains many other documents. Since no other terminal has been detected in the neighborhood yet –which means no other terminal is currently within radio range–, the announcement broadcast by terminal T_A simply contains its ID, and a description of its interest profile.

At time t_1 (see Fig. 3-b) another warfighter B comes within radio range of A's terminal. Warfighter B also carries a communication terminal that periodically broadcasts an announcement indicating its own identity and interest profile. B is not involved in A's mission, though, and his terminal is therefore not configured so as to relay A's observations. Upon receiving one of T_B's announcements terminal T_A discovers that it has acquired a new neighbor, but by matching T_B's profile against the descriptors of the documents stored in its local cache T_A also discovers that T_B is not interested in any of the documents stored in its cache. Terminal T_A therefore refrains from proposing any document to T_B, and continues announcing its presence (ID and interest profile) with no catalog in its announcements.

At time t_2 (see Fig. 3-c) a vehicle C also enters the radio range of T_A. Upon receiving an announcement broadcast by the terminal T_C transported in this vehicle, T_A discovers that this terminal should be interested by document D1 (which means C is meant to participate in A's mission). It therefore incorporates a catalog in its periodic announcement. This catalog contains the descriptor of document D1, and possibly other descriptors of documents available in T_A's cache and that match T_C's interest profile. After receiving such an announcement from T_A, T_C processes the catalog it contains in order to identify documents that are not already in its local cache. Since descriptor D1 belongs to this category, T_C sends a request to T_A, asking that the corresponding document be broadcast on the radio channel.

A short while after document D1 has been transmitted to terminal T_C, warfighter A suspends his terminal and moves away. Note that it is not necessary for this warfighter to be aware that the document he published at time t_0 has indeed been transferred to one or several other terminals. The actual dissemination of this document is ensured automatically in the background by the DoDWAN middleware, which seizes any possible opportunity to pass the document from terminal to interested terminal.

Let us now consider the terminal T_C transported in vehicle C. After a –possibly long– trip T_C gets at time t_3 (see Fig. 3-d) within radio range of the group leader's terminal T_D, whose interest profile of course matches the descriptor of document D1. Upon receiving an announcement broadcast by T_D, T_C discovers that T_D might indeed be interested in document D1 (note that T_D may have already received a copy of D1 from another mobile terminal). T_C therefore includes D1's descriptor in a catalog embedded in its periodic announcement, and lets T_D decide if it wishes to get a copy of D1. If that is the case, then T_D sends a request to T_C accordingly, and T_C complies by broadcasting D1 as requested.

Note that with this approach a document published by terminal T_A has eventually reached terminals T_C and T_D, although T_A and T_D have never been within mutual transmission range, and although no temporaneous end-to-end path has never existed between them in the scenario considered. Terminal T_C has actually served as a mobile carrier for a piece of information published on T_A, and

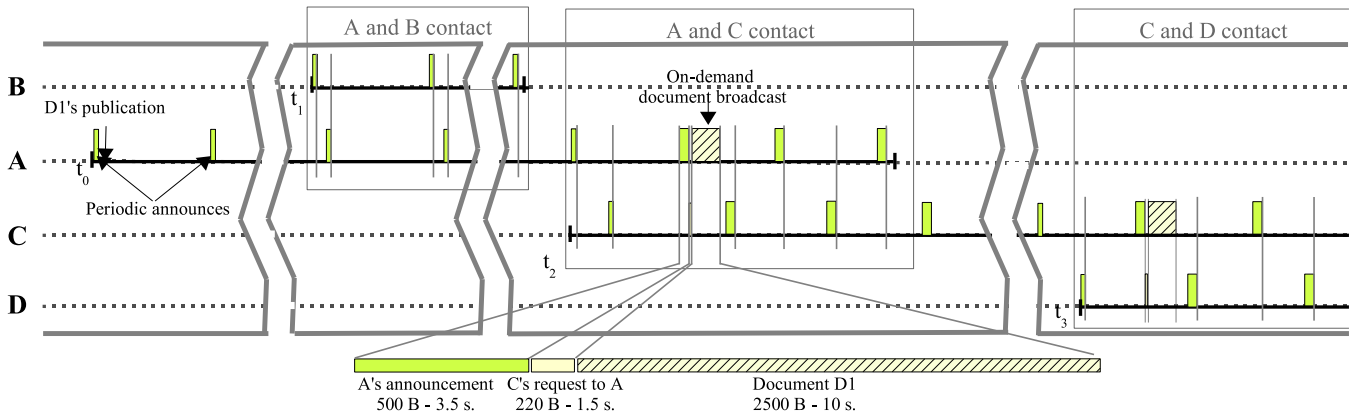

Figure 4. Timeline of the communication scenario

that was of interest to terminal T_D. This scenario illustrates how disruption-tolerant, opportunistic networking can be used to ensure information dissemination in a partially connected military tactical radio network. It also shows how content-based differentiation can be used to drive the dissemination of information in the network, by making each terminal selective to one or another kind of document.

Figure 5. Architecture of a typical mobile unit running DoDWAN

EXPERIMENTAL RESULTS

The scenario presented in the former section was actually run on a testbed dedicated to tactical radio simulation. This testbed is maintained by the Electronic Warfare Department of the French Armament Procurement Agency. The tactical radio network testbed installed in CELAR, is composed of 20 PR4G radio transceivers from THALES Communications. These transceivers are connected to a radio switch, which makes it possible to simulate different deployment topologies or radio propagation conditions. The main advantage of this testbed over a real outdoor environment is that all the radio units are co-localized and the radio propagation conditions are under control, which makes it easier to conduct repetitive experiments in controlled conditions. Current versions of the PR4G radio support up to 64 kbps data transfer waveform in a 25 kHz channel, retaining the system's frequency hopping and anti jamming modes. The system also supports a proprietary frequency hopping multiplex mode (called SIVD) offering simultaneous and independent secure Voice and Data communications. The radio also features a standard IP/Ethernet interface and a built-in IP router.

Our prime motivation for using this testbed was to assess whether the DoDWAN middleware –and most especially the protocol it implements– can perform satisfactorily with the narrowband transmission rates permitted by PR4G radios.

In accordance with the scenario described above, the experiment we run on the testbed involved 4 communication units. Each unit was composed of a PR4G radio associated with a data terminal (see Fig. 5) connected to the Ethernet interface of the PR4G. We actually used netbooks as terminals, but any kind of hand-held device featuring a standard IP stack and a Java 1.6 runtime environment could be used as well. The PR4G radios were set to run the so-called IP-Multiplex communication profile, which features simultaneous secured voice and data capabilities with a data rate of a few kbps. Although this profile does not support multi-hop transmissions (since no dynamic ad hoc routing protocol is used), it provides one-hop multicast IP based on broadcast transmissions. It therefore perfectly fits the needs of our communication middleware, which relies on periodic and sporadic broadcasts of UDP datagrams.

It is worth mentioning that PR4G radios can use the TOS (Type Of Service) field in IP packets to ensure reliable transmissions at data-link level, as well as packet prioritization. These facilities were used during our experiment to increase the reliability of radio transmissions, and to give control traffic priority over data traffic.

The mobility of terminals during the course of the scenario was simulated by adjusting the attenuation matrix of the testbed. The announcement period was set to 60 seconds on all terminals. The document published on terminal A at time t_0 was actually a 2.5 kB JPEG image, with an associated descriptor of 500 Bytes. The interest profiles defined on each terminal weighed about 300 Bytes (after LZ77 compression). The timeline of the scenario was defined as follows: $t_0 = 0, t_1 = 15\,min., t_2 = 20\,min, t_3 =$

30 *min*.

The whole scenario progressed as expected on the experimentation testbed. The systematic compression of all control and data messages (i.e. periodic announcements, requests, and documents) using the LZ77 algorithm proved quite effective, considering the low bit rate allowed by PR4G modems. Indeed, most control messages (encapsulating XML structures) were compressed with an average compression ratio of 12:1, which for example yielded transmission times varying between 2.5 and 3.5 seconds for each periodic announcement (depending on whether an announcement included a catalog or not). The longest transmission time observed during the simulation was of course that of document D1, which was broadcast shortly after time t_2 by terminal A in response to C's request, and once again after time t_3 by terminal C in response to D's request. In both cases the actual broadcast of D1 occupied the radio channel during about 12 seconds.

To complement these figures it is worth mentioning that compression and decompression times with the LZ77 algorithm never exceeded 10 ms on the 1.6 GHz netbooks we used as experimentation terminals.

As a whole, this experimentation trial conducted with the PR4G testbed confirmed that the DoDWAN middleware platform can indeed perform satisfactorily on terminals associated with PR4G tactical radios. It also confirmed that the communication model implemented by the DoDWAN middleware allows the effective dissemination of tactical information in a disrupted military tactical radio network. Most notably, it showed that the load induced by this dissemination is compatible with the low data rates supported in such a network.

Now the question of scalability should also be considered. Although no large-scale experiment with PR4G radios has been conducted so far, we have already obtained promising results while running the DoDWAN middleware platform on dozens of hand-held devices featuring Wi-Fi interfaces. These results were obtained either in real conditions, or using a simulator. For example, [8] presents some the results we obtained while simulating the behavior of 120 Wi-Fi enabled mobile terminals running DoDWAN, these terminals being carried by pedestrians such as students moving in a campus-like environment.

CONCLUSION

In this paper we have presented a new system for content-based information dissemination in partially connected military tactical radio networks. This system is meant to complement traditional networking solutions, as it can support communication in challenged battlefield environments where the dynamicity of the radio network and the absence of end-to-end connectivity sometimes preclude building ad hoc routing structures.

The middleware we designed provides a Publish/Subscribe API, whereby information published on one radio unit can flow in the network and ultimately reach any interested receiver. Opportunistic disruption-tolerant networking techniques are used to support information dissemination in the network. Mobile units that roam the network are used as mobile carriers for information, and therefore help bridge the gap between non-connected parts of the network.

Experiments conducted on a testbed composed of PR4G military tactical radios confirm that the model we defined is effective at disseminating selective information in a partially connected ad hoc network. Most notably the middleware we developed based on this model can efficiently drive tactical radios in a battlefield environment.

Directions for future work include continuing these experiments in real conditions, possibly with a larger set of radio units. This work should be conducted in the framework of the future European project MIDNET (MIlitary Disruption-tolerant NETworks).

REFERENCES

[1] L. Pelusi, A. Passarella, and M. Conti, "Opportunistic Networking: Data Forwarding in Disconnected Mobile Ad Hoc Networks," *IEEE Communications Magazine*, Nov. 2006.

[2] Z. Zhang, "Routing in Intermittently Connected Mobile Ad Hoc Networks and Delay Tolerant Networks: Overview and Challenges," *IEEE Communications Surveys and Tutorials*, vol. 8, pp. 24–37, Jan. 2006.

[3] R. Krishnan et al., "The SPINDLE Disruption-Tolerant Networking System," in *Proceedings of IEEE Military Communications Conference*, pp. 1–7, Oct. 2007.

[4] A. Carzaniga and A. L. Wolf, "Content-based Networking: A New Communication Infrastructure," in *NSF Workshop on an Infrastructure for Mobile and Wireless Systems*, no. 2538 in LNCS, (Scottsdale, Arizona), pp. 59–68, Oct. 2001.

[5] P. Costa and G. P. Picco, "Semi-Probabilistic Content-Based Publish-Subscribe," in *25th International Conference on Distributed Computing Systems*, (Columbus, Ohio, USA), pp. 575–585, June 2005.

[6] R. Meier and V. Cahill, "STEAM: Event-Based Middleware for Wireless Ad Hoc Network," in *International Conference on Distributed Computing Systems, Workshops*, pp. 639–644, July 2002.

[7] A. Datta, S. Quarteroni, and K. Aberer, "Autonomous Gossiping: a Self-Organizing Epidemic Algorithm for Selective Information Dissemination in Mobile Ad-Hoc Networks," in *International Conference on Semantics of a Networked World*, no. 3226 in LNCS, (Paris), pp. 126–143, June 2004.

[8] J. Haillot and F. Guidec, "A Protocol for Content-Based Communication in Disconnected Mobile Ad Hoc Networks," in *IEEE 22nd International Conference on Advanced Information Networking and Applications (AINA'08)*, (Okinawa, Japan), pp. 188–195, IEEE CS, March 2008.