Content Centric Networking in tactical and emergency MANETs

Conference Paper · November 2010

DOI: 10.1109/WD.2010.5657708 · Source: IEEE Xplore

3 authors, including:

Soon Y. Oh
Utopia Compression
37 PUBLICATIONS **1,114** CITATIONS

SEE PROFILE

Content Centric Networking in Tactical and Emergency MANETs

Soon Y. Oh, Davide Lau, and Mario Gerla
Computer Science Department
University of California, Los Angeles
Los Angeles, CA 90095
{soonoh, chiune, gerla}@cs.ucla.edu

***Abstract*—Reliable and secure content distribution in a disruptive environment is a critical challenge due to high mobile and lossy channels. Traditional IP networking and wireless protocols tend to perform poorly. In this paper, we propose *Content Centric Networking* (CCN) for emergency wireless ad hoc environments. CCN is a novel communication architecture capable to access and retrieve content by name. This new approach achieves scalability, security, and efficient network resource management in large scale disaster recovery and battlefield networks. Existing Internet CCN schemes cannot be directly applied to wireless mobile ad hoc networks due to different environments and specific limitations. Thus, we must extend the CCN architecture by introducing features and requirements especially designed for disruptive networks. We prove feasibility and performance of the new design via implementation and experimentation.**

I. Introduction

In recent years, Content Centric Networking (CCN) [1] has emerged where a network is viewed as dynamic storage of information and provides end-to-end communications in terms of named contents instead of traditional IP-style addressing and location. Using this new networking approach, we get the following advantages: communication overhead for binding content to site can be minimized, and in-network processing is feasible as content travels nodes through the network. CCN has been applied to the Internet, which is a huge static network. In a wireless Mobile Ad hoc NETworks (MANETs), we expect that CCN will also provide benefits, better utilizing error-prone, bandwidth constraint wireless links and reducing resource consumption.

A typical tactical or disaster recovery scenario is intrinsically hierarchical in two ways - nodes move in groups (e.g., for emergency rescue team or coalition operations) and they are connected via gateways and backbone; data has local relevance (most data is created and searched locally). There are both mobile nodes (agents, soldiers, UAVs, mobile sensors, etc.) and stationary nodes (command center, fixed sensors). Moreover, radio communications are challenging, because (1) nodes may be highly mobile especially when communications devices are installed in vehicles; (2) the node may scale to hundreds; and (3) radio signal propagation effects and operational constraints limit the effectiveness of off-the-shelf techniques such as IEEE 802.11.

While the tactical/emergency MANET is a challenging environment to content distribution, it also provides advantages, namely: group-based mobility and information locality. Internet based CCN schemes, however, cannot be directly applied for the following reasons. First, reliable data transmission and resource savings are crucial to achieve missions in the field while Internet has infinitely more resources and; the wired medium is much more reliable than the wireless medium. Second, information push, i.e., data dissemination is prevalent in order to deliver important operation messages or information to agents/soldiers in the fields; for example, information related to insurgent movements of enemy must be quickly delivered to soldiers within that sector or victims' situation must be noticed immediately to the relief team in the field. Third, security and content authentication are extremely important requirements in the tactical scenarios.

The goal of this paper is to design a CCN protocol suite that supports content addressing, repository, and distribution in a large MANET. The CCN protocol for MANETs is based on CCN in [1], in particular on the implementation of operations directly in terms of named content. We assume that a large MANET for tactical and emergency scenarios features group mobility/operation of mobile nodes and hierarchical networking structure. Therefore, first, our target CCN has efficient hierarchical storage/search architecture. Next, it employs two different type of content: topic based data and spatial/temporal contents. A publisher disseminates meta-data records via hierarchical networking structure and the records are stored in the node's registry which is also used for content searching. Finally, while the current CCN schemes proposed for the Internet operate at the application layer, in the tactical MANET, the CCN functions are spread across layers, thus the cross layer approach is critical.

The main contributions of this paper are: design and implementation of CCN on a large scale MANET where high mobility and lossy channel exist; MANET CCN saves network resource consumption, e.g., bandwidth and power, exploiting group based mobility and hierarchical network structure of the tactical filed. Finally, we show that CCN provides simple content search and delivery system in the battlefield.

The rest of the paper is organized as follows: Section II briefly introduces previous content centric network schemes; section III describes tactical battlefield network model; Section IV presents the proposed tactical MANET Content Centric Networking in details and Section V demonstrates implemen-

tation and experiment results of CCN. The paper is concluded in Section VI.

II. Related Work

Recently, several content centric networking schemes have been proposed. They all recognize that combining identity and location into a single network address is not proper in today's Internet and try to replace host-oriented naming system with content-based networking.

TRIAD [2], [3] names content with user-friendly, structured, location-independent names. TRIAD is arguably the first to explore the name-based routing and its naming scheme has influenced later name-based routing protocols, such as DONA, CCN, etc. It routes on URLs by mapping URLs to next-hops. TRIAD forwards the request to the next hop, continuing until a copy of the data is found and its location is returned to the client.

Data-Oriented (and beyond) Network Architecture (DONA) [4] uses flat, self-certifying names instead of IP DNS system. Generated content is published and registered with a tree of trusted Resolution Handlers (RHs) so that RHs provide a forwarding table that is next hop information of content. If the location of content is changed, the new information must be registered in order to retrieve it; otherwise, no user can find the new location.

Routing on Flat Labels (ROFL) [5] uses semantic-free flat labels and creates a circular namespace (e.g., DHT [6]) for correct routing like Chord [7]. Receivers put in a trigger, data identifier, and their address into the DHT. The trigger is routed to the sender who has the requested identifier and files.

Content Centric Network (CCN) [1] provides a network wide content caching and user-friendly, hierarchical names for routing. The content publisher names content and adds digital signature to guarantee security; intermediate routers can validate an incoming packet using digital signature. A publisher announces content availability and a node sends request. CCN employs a longest-match look-up on its name to forwarding decision. If there are multiple servers announcing content, unlike IP forwarding, the request is forwarded toward all these content sources. Furthermore, CCN routers provide caching within the network and thus any CCN routers on paths that have the requested data can respond and send the data.

The above name-based routing protocols, however, are Internet protocols and thus they do not support routing in high mobile and lossy channel environments. MANET CCN employs the key features of the existing schemes such as user-friendly names and intermediate node caching, but it adds new functionalities to adapt to the unpredictable wireless medium and to disruptive mobile environments.

III. Network Model

Due to its infrastructureless nature, a MANET is ideally suited for tactical and emergency operations since it can be quickly deployed anywhere. The most important feature of such networks is group-based mobility. Soldiers, military vehicles, and emergency personnel move in groups to achieve a mission. In a tactical network, groups are interconnected to form a hierarchical topology as shown in Figure 1 [1]. The lowest level of the network consists of soldier handheld devices or mobile/static sensors that provide critical tactical edge connectivity. Communication devices provide a mobile ad hoc networking capability for ground combat operations and the support of voice/data communication services. However, their waveform supports low bandwidth ($<$ 600Kbps) and devices have limited storage with low power. Thus, the lowest level domain of the structure consists of the small unit operations (e.g., squad or platoon) that cover a small area while gateways provide seamless communications among multiple local domains. In an emergency network, rescue people also bring low performance, mobile ad hoc networking capability devices that provides voice and data communication services.

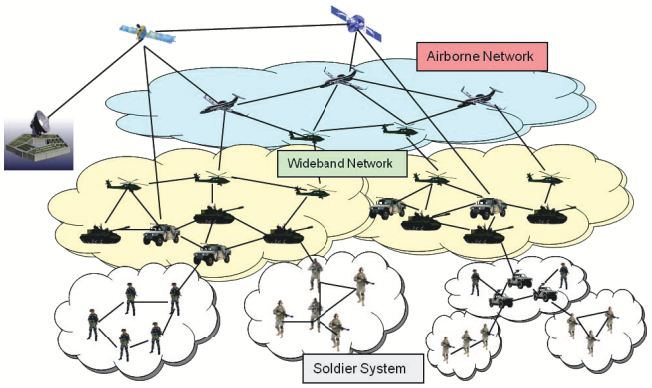

Fig. 1. Hierarchical network structure in the battlefield.

The local domain gateways interface with an upper level, wideband domain that provides interconnection between stub networks and the large scale, highly mobile wide area backbone. The backbone consists of both static and mobile nodes deployed in a large area and supporting high bandwidth (e.g., 2Mbps), large storage and high transmit power. The highest level of the architecture provides global satellite communications narrowband (64Kbps) connectivity.

In this hierarchical structure, soldier handheld devices become information consumers while upper level nodes and gateways act as information publishers and storages. Data generated by lowest level nodes or sensors is transmitted to an upper level node through a gateway and is disseminated to interested consumers throughout the network.

IV. Content Centric Networking

In this section, we present details of the MANET CCN protocol.

A. Data and Temporal/Spatial Content

Content can be generated and named by any nodes in the network. It is stored at the publisher which is the content originator itself or a backbone node near the content originator. Unlike Internet, content in the tactical/emergency MANET can be classified as topic based content (e.g., data files, video and audio files, etc) and spatial/temporal content (e.g.,

[1]Readers can find a more realistic and detailed description in [8]

situation awareness data from sensors, an operation message from the command center). In this classification, situation content has higher priority than topic based content, its value depending on location and time. Thus, situation content must be quickly disseminated toward the intended locations even though there is no request. Furthermore, the spatial/temporal content must include exact time and location information in the content name, e.g., EnemyUAVs-Moday3pm-(X,Y)-from-South-to-North.mov. The publisher transmits it to a gateway towards the upper level of the network where the command center is located. If the publisher and content location is not matched (e.g., UAV records a wide area of the enemy camp), the content can also be delivered by location based geographic routing. For example, a sender broadcasts the content stamping its own location. Nodes receiving it compare own, sender, and content locations. If receiver's location is closer to the intended destination than the transmitter's location, the node caches it and re-broadcasts; otherwise, it ignores the content.

Data files have no spatial/temporal dependency and they can be requested from anywhere in the network. A publisher only retrieves them once it receives an indication of interest from others since disseminating data files may waste network resources. The publisher generates and distributes meta-data with content details to neighbors to domain gateways. Other nodes search data files using these meta-data records. As data files and spatial/temporal content are transmitted, intermediate nodes cache them in their local repository for future transmission.

B. Content, Meta-data, and Interest Storage

Local storage is a key function of the CCN and the MANET CCN also supports it. Even though local storage has its cost, it can save network bandwidth preventing duplicated data transmission. Due to low power and lossy channels in wireless networks, power and bandwidth savings are very important. Moreover, storage is becoming progressively cheaper and of smaller footprint, making the CCN solution very effective.

The MANET CCN nodes cache arriving content in own Content Repository to maximize the probability of sharing. As we mentioned before, however, since handheld devices do not have enough repository space and power, only upper level nodes and gateways store content. The handheld devices shortly save received content in the buffer and transmit it if neighbors are interested in. Data files are stored when possible (using LRU or LFU replacement), but spatial/temporal content remains in the Content Repository as long as its location and time information are viable. As time passes and the node moves to other locations, the spatial/temporal content becomes obsolete and is removed.

Received meta-data generated by a publisher is maintained in the Meta-Data Registry which is a structured storage system. The meta-data includes various attributes, e.g., file type, creation time, originator, size, description, etc. The data name is derived by combining those attributes. Thus, Meta-Data Registry can be a hash table for efficient look up. For instance, Mercury DHT [9] uses each attribute for content addressing; i.e., it maintains a Distributed Hash Table (DHT) for each attribute, and multi-dimensional content can be searched by sequentially accessing each attribute. However, the Meta-Data Registry does not map to storage space like peer-to-peer system. It is used to forward an Interest packet toward a node having content or being a potential content generator. Thus it records one hop destination and outgoing interface for content. Users search data from the Meta-Data Registry. All CCN nodes, even solider handheld devices, maintain it.

Interest Registry stores Interest that is relayed by a node. If a node does not have a data file, it relays received Interest to neighbors or a gateway. After relaying, a node records Interest with incoming and outgoing interface in the registry. This information is used later to find duplicated Interest and to forward data content to a node that generated Interest.

C. Routing

Tactical MANET CCN employs two kinds of routing schemes: content pushing and pulling. In contrast, Internet CCN uses content pulling and content announcement pushing [1]. As we mentioned before, content pushing is achieved by geographical routing with which spatial/temporal content travels toward a command center and to proper locations via backbone network.

To get data, a node sends Interest, i.e., the name of the content, to neighbors and to the gateway of the domain. Upon receiving Interest through its interface, a node looks up Content Repository and transmits content packets through the interface where the Interest arrived if it has. Then the Interest is discarded. If there is no matched data, the node next looks up Interest Table, which records track of Interests that were relayed. If the table has the matched entry, the node adds an arrived interface index in the entry and discards Interest. Otherwise, it searches Meta-Data Registry. If the matched entry is found in the registry, the node re-broadcasts Interest; otherwise, forwards it toward the domain gateway. Relayed Interest information, including arrived and transmitted interface, is written in the Interest Table.

Data packet simply follows the Interest Table entry back to the node requested data. While delivering data packets, intermediate nodes replicate/cache packets in the own Content Repository. Due to wireless shared medium, the MANET CCN has more features than Internet CCN. First, it employs Interest aggregation. For example, a node defers Interest transmission upon overhearing the same Interest transmitted by a neighbor since it may get the data overhearing the transmission toward the neighbor node. Next, the MANET CCN has packet collision avoidance mechanism employing control packets, Reply and Request. It may possible that more than one neighbor start transmitting data content. To avoid collision in this situation, a node having content sends Reply to Interest before transmitting data. The destination node sends back a Request packet and the node sends packets upon receiving Request.

D. Content Security and Authentication

CCN supports content-based security as required in tactical and emergency communications. Using PKI, all transmitted packets are authenticated with digital signatures or encrypted by a public key. A gateway in the domain has a private key and member nodes in the domain have a public key. A gateway add digital signature using a private key to packets transmitted to members; members encrypt packets by gateway's public key when they transmit packets, e.g., Interest or sensor data, to the gateway. For transmission between domain members, a sender transmits packets to the destination adding digital signature and passes own public key to the gateway encrypting it by gateway's public key. The destination acquires sender's public key from the gateway.

In [1], public key location is recorded in the data packet in order for the receiver to obtain it. However, in the battle-field/emergency rescue scenarios, to get the key from a specific site, say, it is impractical and impossible. Thus, public and private key must be pre-assigned before nodes disperse in the field. In the tactical/emergency MANET, a network planner and a management tool [8] exist. They can pre-assign keys and signature algorithms[2].

V. Implementation and Evaluation

In this section, we evaluate and validate the performance of our MANET CCN design and implementation. We implement MANET CCN on laptops with Linux OS following the specifications in the previous sections. CCN nodes have Content Repository, Meta-Data Registry, and Interest Table. Gateway nodes publish and deliver content data to member nodes within a domain. Gateway nodes flood their meta-data list and update their meta-data upon receiving neighbors' lists. A node sends Interest to the gateway. It sends back a Reply packet to the Interest packet originator if the gateway has requested data. Upon receiving a Request packet, the gateway starts transmitting data packets. For content verification, we implement private and public key security using RSA algorithm. The gateway has a private key to generate its digital signature. Group members have the public key to verify content from the gateway. CCN has no underlying routing protocol; nodes simply pass packet hop-by-hop via UDP connections.

We study a simple four nodes (all gateway nodes) topology in Figure 4 and compare CCN performance with peer-to-peer routing protocol performance in terms of advertise/publish overhead and content distribution delay. We choose Pastry file sharing with OLSR routing protocol as term of comparison. We download and compile FreePastry 2.1 [10], [11] and OLSRD 0.5.6-r8 [12], [13] on laptops. Pastry is an Internet based, decentralized, self-organizing, and fault-tolerant overlay network, with a ring-structure. It stores key-value pairs using a distributed hash table; it supports efficient query routing, deterministic object location, and load balancing in an application-independent manner [10]. The Optimized Link State Routing Protocol (OLSR) is a proactive ad hoc routing protocol based on the link state model. To reduce broadcast overhead, OLSR uses the Multi-Point Relay (MPR) scheme where only designated neighbors relay broadcast packets [12].

We use two metrics: *Control Packet Overhead* the amount of traffic required for link maintenance and for meta-data and key-value pairs updating; and *Content Distribution Delay* the time to complete data delivery. We evaluate and compare the two above protocols in representative wireless environments using four laptops.

First we measure the control packet overhead of both protocols during 600 second experiments. We inject new data every 3 seconds in order that both protocols periodically advertise/publish information of new content in the network. In Figure 2, FreePastry reports 378B/s average traffic while CCN shows only 72B/s traffic in Figure 3. Moreover, FreePastry exhibits periodic traffic bursts caused by the P2P ring-structure maintenance. In addition, OLSR traffic is added in Figure 2. Note that FreePastry has significant high traffic without any data transmission. In contrast CCN does not generate any extra traffic besides publishing Meta-Data, since it does not require any underlying routing protocol and overlay structure,

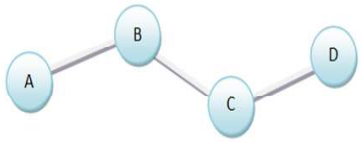

Fig. 4. Four gateway topology for the MANET CCN test.

Next, we compare content distribution delay for both protocols. In the experiment, various file sizes e.g., 1, 5, 10, 15, 20, 25 and 100MB , are transmitted from node A to other nodes as shown in Figure 4. The Figure 4 topology is linear and packets cannot reach two hops away nodes, i.e., C cannot receive A's transmission. In peer-to-peer transmission in Figure 5, delays are almost same in both protocols. Actually, CCN exhibits a little bit longer delay than FreePastry during experiments because of hop-by-hop content delivery. However, as we expected, CCN presents significantly lower delay once content is distributed to all nodes in the network. After Node B receiving content, Node C requests data from Node A and then Node D follows. To do this, FreePastry must make four connections to node A one after another since intermediate nodes discard packets after successfully relaying. In contrast, CCN nodes store relayed data in own repository; thus it is not necessary to make connection to an original content publisher. In this case, CCN destination can receive data from any one hop neighbor and thus delay is significant reduced. In Figure 6, CCN delay increases slowly in the function of content size and finally, CCN spends only a half of time compare to FreePastry to complete 100MB data. Furthermore, this content replication and store can save channel bandwidth in the network.

VI. Conclusion

Today's Internet applications are dominated by content distribution, but the Internet still follows the traditional host-to-

[2]Furthermore, domain splitting, merging, and gateway re-selecting may be possible in high mobile tactical area; they are not mentioned here for space limitations.

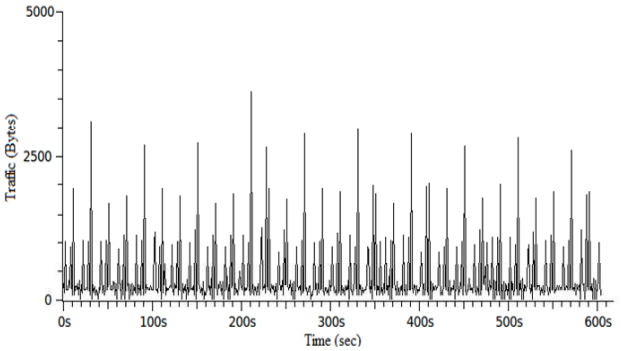

Fig. 2. Control overhead of FreePastry with OLSR.

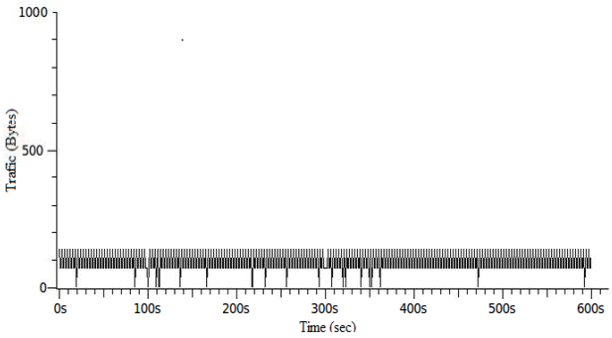

Fig. 3. Control overhead of MANET CCN protocol.

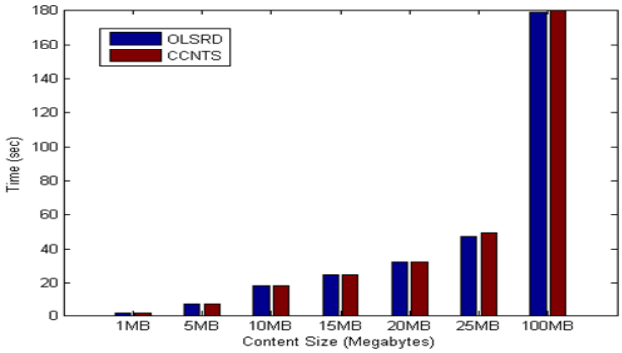

Fig. 5. End-to-end delay to transmit content from Node A to Node D.

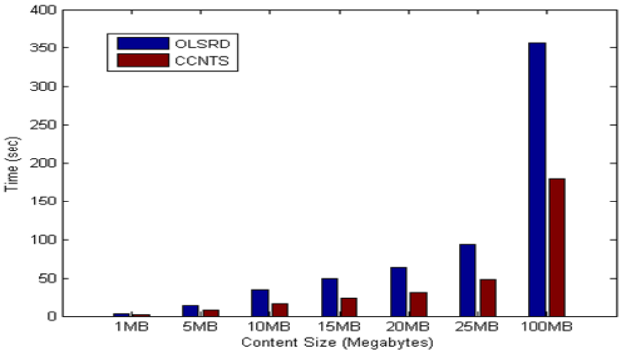

Fig. 6. End-to-end delay to distribute content from Node A to all other nodes.

host connections model. Recently, a content centric networking concept has been proposed for the Internet where content name rather than host identifiers, e.g., IP address, is used for routing. However, the Internet content centric networking scheme is based on a static environment. In this paper we propose a MANET CCN scheme that inherits existing methods such as user-friendly name and data caching, but also adds functionalities designed to make it robust to wireless, lossy channels and mobile situations. The MANET CCN replicates the simplicity and scalability of MANET networking by exploiting the inherent hierarchical naming and networking structure. In addition, it saves network resources such as channel bandwidth and power by taking advantage of efficient caching. It increases security by using digital signature and PKI data encryption. We have implemented MANET CCN in a simple testbed and have demonstrated its performance benefits and superiority over existing address schemes through a set of representative experiments.

For the future work, we plan to extend the hierarchical MANET CCN concept beyond the tactical and emergency scenarios, to general wireless mobile networks. To do this, first we will design faster and more reliable routing and data delivery scheme; next, we will develop efficient meta-data look up algorithms; finally, we will develop new security methods that are suitable for general wireless networks.

REFERENCES

[1] V. Jacobson, D. Smetters, J. Thornton, M. Plass, N. Briggs, and R. Braynard, "Networking named content," in *the 5th ACM International Conference on Emerging Networking Experiments and Technologies (CoNEXT 2009)*, Rome, Italy, December 2009.

[2] D. Cheriton and M. Gritter, "Triad: A new next-generation internet architecture," 2000.

[3] M. Gritter and D. R. Cheriton, "An architecture for content routing support in the internet," in *USITS'01: Proceedings of the 3rd conference on USENIX Symposium on Internet Technologies and Systems*. Berkeley, CA, USA: USENIX Association, 2001, pp. 4–4.

[4] T. Koponen, M. Chawla, B.-G. Chun, A. Ermolinskiy, K. H. Kim, S. Shenker, and I. Stoica, "A data-oriented (and beyond) network architecture," in *ACM SIGCOMM*, Kyoto, Japan, October 2007, pp. 181–192.

[5] M. Caesar, T. Condie, J. Kannan, K. Lakshminarayanan, and I. Stoica, "Rofl: routing on flat labels," in *SIGCOMM*, Pisa, Italy, Septempber 2006, pp. 363–374.

[6] H. Balakrishnan, M. F. Kaashoek, D. Karger, R. Morris, and I. Stoica, "Looking up data in p2p systems," *Communications of the ACM*, vol. 46, no. 2, pp. 43–48, 2003.

[7] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," in *SIGCOMM '01: Proceedings of the 2001 conference on Applications, technologies, architectures, and protocols for computer communications*. New York, NY, USA: ACM, 2001, pp. 149–160.

[8] "Delivering mobile ad hoc networking to the joint warfighter," May 2009. [Online]. Available: http://jpeojtrs.mil/files/domains/09_NED_AFCEA_Brief_v6.pdf

[9] A. R. Bharambe, M. Agrawal, and S. Seshan, "Mercury: Supporting scalable multi-attribute range queries," in *In SIGCOMM*, 2004, pp. 353–366.

[10] A. Rowstron and P. Druschel, "Pastry: Scalable, distributed object location and routing for large-scale peer-to-peer systems," in *IFIP/ACM International Conference on Distributed Systems Platforms (Middleware)*, November 2001.

[11] "Freepastry web site." [Online]. Available: http://www.freepastry.org/FreePastry

[12] T. Clausen and P. Jacquet, "Rfc 3626: Optimized link state routing protocol (olsr)," 2003.

[13] "Olsrd web site." [Online]. Available: http://www.olsr.org