無線アドホック・オーバレイネットワーク機構の提案

斉藤 匡人† 間 博人† 徳田 英幸†,‡

†慶應義塾大学大学院 政策・メディア研究科 ‡慶應義塾大学 環境情報学部
E-mail: {masato, haru, hxt}@ht.sfc.keio.ac.jp

本論文では、ユビキタスネットワーキング環境において、多様なネットワークグループを安全に独立的に共存させるためのアドホックネットワーク経路制御アーキテクチャを提案する。従来のアドホックネットワーク技術は、主にある独立した一つの無線ネットワークグループを想定してアドレッシングや経路制御サービスを提供していた。現実のユビキタスネットワーキング世界では、同一地域・場所において、複数の独立したアドホックネットワークグループが存在する可能性がありうる。これを実現するために、アドホックグループ管理を統合した経路制御機構を設計、評価する。

A Membership-Centric Routing Architecture for Ubiquitous Ad Hoc Networks

Masato Saito† Hiroto Aida† Hideyuki Tokuda†,‡

†Graduate School of Media and Governance, Keio University
‡Faculty of Environmental Information, Keio University

In this paper, we describe a group-ID oriented routing management for ubiquitous ad hoc networks, called Wireless Overlay Networks (WoN). WoN focuses on the initial phase of building ad hoc spontaneous networks, that involves addressing, naming, and multi-hop routing for the participants in the networks. Aiming at the quick and straightforward operation, we combine the three primitive functions into the group-ID based routing system. The IDs identify and separate each network group to allow multiple ad hoc networks to co-exist in the same region. WoN also realizes secure group management and plural routing protocol interoperabilities. To our knowledge, this is the first work in the ad hoc research area, that tackles plausible situations in which multiple ad hoc networks whose members are independent of each other can operate separately in the same area. We present the architectural design and the preliminary simulation results of WoN.

1 Introduction

Recent advancement in wireless communications and the spread of mobile computing devices and sensors would enable the development of ubiquitous spontaneous ad hoc networks. With the longing for ubiquitous computing and networking, spontaneous and cooperative direct communications among wireless devices are becoming attractive technology. A mobile ad hoc network is a group of mobile computing devices (or nodes), in which nodes communicate with each other using multi-hop wireless links. It does not necessarily need any stationary infrastructure such as wireless base stations or access points. Each node in the network can act as both a end-host and a router forwarding data packets to other nodes. Though applications such as disaster relief, intelligent transport systems, and complementing cellular systems are expected to realize using ad hoc networking, secure and spontaneous communication is a essential requisite for such applications.

Since node mobility in ad hoc networks causes frequent and unpredictable, changes to the network topology, it is important for communicating nodes to grasp changes of the network topology and find more efficient routes between two communicating nodes. Thus ad hoc network routing protocols are fairly challenging to design and implement. Wired network routing protocols such as OSPF [9] do not cope with well the type of rapid node mobility and network topology changes that occur in ad hoc networks and have high routing overhead due to exchanging of periodic link-state routing messages. That is why a number of research for MANET have focused on the development of their routing protocols (e.g., AODV [12], DSR [6], OLSR [3], TBRPF [11]). Lately, many security research for ad hoc networks also have been proposed in the various form. However, these research projects have studied their protocols and routing problems in a uniform and prerequisite network setting: there is only one ad hoc network in one area, particular IP address range is uniformly allocated to nodes of a network beforehand, or one common routing protocol is used in an ad hoc networks. Because most

of the previous research mainly focus on routing algorithms, group management in ad hoc networks are given assumptions and not well defined. Little research has been done in a more realistic environment in which multiple ad hoc networks whose members are independent may co-exist in the same area.

In this paper, we propose a secure group management system for MANET, called WoN, that is based on group identifiers (MANET ID: MID). It is a remedy for some of above problems in realistic MANET environments. In WoN, members having the same MID can build the independent MANET spontaneously even if other MANETs co-exist in the same location. Since MIDs are just logical identifiers, MIDs are chosen using consistent hash functions and are allocated to each MANET group. In spontaneous and ubiquitous MANETs, the network age seems to be not long but rather short, so distributed network addressing schemes including duplicate address detections may be an expensive approach. We take an approach such as a MID-based group separating. To do the MID-based ad hoc network routing, we can separate multiple MANETs in the same real environments. Additionally, our MID-based group management can achieve the security, spontaneous networking, and independence of each multiple MANETs while keeping the overhead relatively low. WoN also allows multiple ad hoc network routing protocols to coexist and function in the same area at the same time.

To realize ubiquitous ad hoc networking in real environments, we make three contributions in this paper. First, we show several research issues of **ad hoc network bootstrapping in realistic environment**. Second, we present the design and evaluation of **a group separating scheme based on ad hoc group-ID (MID), called WoN**, to build secure, spontaneous, and separated ad hoc networks. Finally, we give the first method to **coexist various ad hoc network routing protocols in the same area.**

2 Background

Secure Group Management

To build and deploy MANETs realistically, we need to consider group membership management as the initialization phase. Robust group management is closely related to security for MANET. The group management issue becomes more complicated when the communications need to be secure.

A basic principle in MANET is a *group* of users or computing nodes. A group is a set of entities that may want to communicate with each other and cooperate for some purposes. The size of MANET groups may vary from several communicating nodes to hundreds or thousands of nodes. The purpose for forming a group could be shared applications and data, physical location, or tactical tasks. Forming a group can also be the initialization step for sharing a secret such as group keys, which will be used to separate the insiders from the outsiders. Generally, group membership management involves adding and removing nodes in the group, and authenticating the group members.

The group management and security of most traditional wired networks have relied on the existence of a fixed specialized infrastructure. In MANET, all the procedures and services should be done in a truly ad hoc and distributed manner.

Related Work

We describe related work on group management and security in MANET. Few research on group membership management have so far been done, we think it is because designing ad hoc networking protocols has been really challenging and tough work. We introduce a few previous work in MANETs and some work in powerful and wired distributed systems.

While traditional secure communications have been based on point-to-point communication with trusted servers, the basis for the security of MANET is the use of multicast inside a group. For instance, the ad-hoc network management protocol by Chen et al. [2] is based on secure multicast that should be received only by a given group of nodes. As this work is mainly focusing on the network management, group membership management have not been taking into account well.

Maki et al. [7] have presented a fully distributed, certificate-based protocol for group membership management in MANETs. The scheme is based on public key cryptography and the use of signed certificates. The members are represented by their public signature keys, and each group has a public signature key to represent the group. Certificates signed by the group key are used to indicate the membership of the nodes. The method seems to be robust against most physical failures in MANETs because of taking the characteristics of MANET into account well. However, the relation between the group membership management and network routing function is not clear and considered well in the paper. In short, since the certificate-based protocol is an application-level solution, in ad hoc networking environments it is a costly approach in regards to power consumption and computation overhead. We also think node addressing issue should be attacked.

3 WoN Base Architecture

We describe the basic design of WoN. First, we arrange the design choices and requirements on the first step of MANET formation. Second, we introduce the group identifiers to separate MANET groups, called MANET-ID (MID). We then describe a MID-based group membership management scheme, called WoN.

3.1 MANET Building Process

In the face of deployment of ad hoc networking, it is necessary to consider such a situation where there are multiple ad hoc group networks close in an area; each of them may have the sharing purposes, applications, tasks, or location-dependent services. These situations could happen in the various contexts of office and home life, emergency operations, or military work. One important thing is how to find or define the boundary of an ad hoc group network. Defining who is a member of the group is also the first step to establish such networking.

Let us think the construction process of an ad hoc network from the initial condition: there are some nodes who may know each other or not, in a place, and they try to build an ad hoc network for certain purposes. These nodes have communicating devices and implement one ad hoc routing protocol which is compatible TCP/IP protocol suites, but not configure the IP addresses and know none of the other nodes' information. So, they use broadcasting only at the initial phase. These assumptions seem to be reasonable and general since they do not depend on specific routing protocols, pre-built network setting, fixed infrastructure, and so on. In such a situation, the following functions are needed to cooperate: addressing, naming, and ad hoc routing. In traditional fixed networks, IP addressing is done statically or dynamically by a centralized administration. Figure 1 presents the difference of the end-node behavior when joining networks between infrastructure-based networks and ad hoc networks.

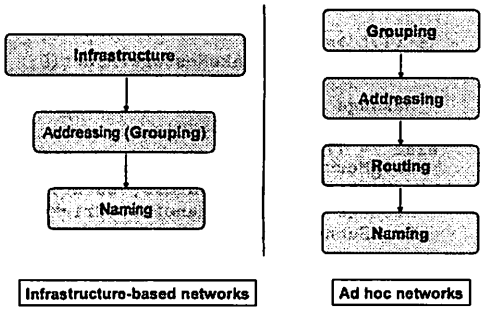


Figure 1: Required functions of the end-node when joining networks initially in infrastructure-based and ad hoc networks.

Although grouping functions are generally implementing at the application layers in wired networks, we should consider on which layers those should be realized taking into account the nature of ad hoc networking. If addressing and naming are done at the initialization phase of MANET, we must consider the security issues and it is inefficient due to the unnecessary resource consumption, for example, forwarding the packets which do not belong a group is unlikely act for resource-limited group nodes. To consider the fully distributed nature of ad hoc networking, we believe that the first step to build ad hoc networking is membership grouping.

There are two actions in the initial phase of ad hoc networking, which are to:

- Create a MANET from the scratch.
- Join a MANET which is already created.

When one node decides to create a MANET, it generates a group name or pre-defined consensus name. Here, we assume that this group names are distributed or shared through secure and local channels such as personal contacts or pre-distribution by e-mails. The details of MID allocation is described in the next subsection. Its name is inserted to WoN routing module on each node. Then, each member having the name do the broadcasting to discover the members. In the routing modules of nodes who is not in "group A," the discovery packets are silently discard.

Then, only the members of "group A" are discovered for each other. At the same time, WoN allocates the temporal IP addresses uniquely using consistent hashing of the group name. Also, consistent hash function assigns each node an m-bit identifiers (i.e., MIDs). Standard SHA-1 is currently adopted as a basic hash function. Note that as already generating the shared MID on each member of "group A" by themselves, it is not needed to consider the issue of convergence and partition of networks. However, MIDs and temporal IP addresses could possibly be duplicated with other group (or MANET) due to the nature of consistent hashing though a marginal probability.

Although we can do the encryption of messages for secure communicating, MID based encryption may be resource consuming operation because encryption processes are running every receiving packets.

3.2 MANET ID (MID)

In MANETs, the network lifetime may be so short that the fully-featured addressing (as that of Internet) is excessive function. Lightweight addressing would be appropriate for MANET. So, we take an approach using group-ID (MID). The MID approach is appropriate for user oriented computing. Basically, the decision makers to group multiple nodes and devices may be users who own these nodes (e.g., devices or computers). This is the natural boundary of a MANET.

MID structure

MID is the identifiers which are just m bits long. The MID-space is flat.

MID allocation and sharing

We show the MID allocation and sharing process in the following Figures 2 and 3. The ManetID in these figures indicates MID. MIDs are assigned by consistent hash function based on a shared group name. MIDs are logical m-bit identifiers having flat structure. By using appropriate consistent hashing, we can assume that MID identifiers are randomly distributed. This allocation scheme is similar to the approach in $i3$ research [13] which bases on Chord protocol [14]. Our MIDs generated from arbitrary group names are semantic-less names because the semantics of identifiers are generally application-specific. It is not desirable to define a uniform semantic categories of identifiers. Thus, as the initial phase sharing a group name which is based on MID, we assume the various sharing methods of any group names: secure and local channels such as personal contacts or pre-distribution by e-mails, pre-defined group lists, location-dependent allocation, off-line talks, or on-demand group name search.

If any new groups will be needed to build or group names need to change, we can cope with it to make the new MIDs dynamically. In WoN architecture, changing MIDs dynamically is not allowed now.

3.3 MID-based Routing

To manage MIDs in ad hoc networks, WoN layer takes the task and interacts with IP routing protocols. Since WoN is the separated layer from rout-

```
/* Obtain ManetID from Addressing Plane */
Loop {
  ReceiveIDfromApplication(ManetID,
                           SubnetSize);
  if (ManetID is not in ''ManetIDList'') {
    /* Extract unique private subnetID
                    IP address prefix */
    SubnetIDofIPAddress = Hash(ManetID);
    HostIDofIPAddress = Random();
    MyIPAddress = SetLocalIPAddress(
      SubnetIDofIPAddress, HostIDofIPAddress,
                                  SubnetSize);
    OrigMessage = MakeMessage(ManetID,
      MyIPAddress, DefaultTtl, Seq);
    Message = Encrypt(ManetID, OrigMessage);
    WaitRandomTime();
    if ( ReceivePacket(ManetID) == false )
      SendBroadcast(Message);
    else
      Discard(Message);
  }
}
```

Figure 2: **WoN Sending Algorithm**

ing functions, WoN simplifies the design of ad hoc routing systems and applications based on it by addressing these difficult problems below:

- **Decentralization**: WoN is fully distributed: no node is more important than any other. This improves robustness and makes WoN appropriate for loosely-organized ubiquitous ad hoc network applications.
- **Scalability**: The cost of a WoN grouping grows as linearly as the number of nodes, so even very large systems are feasible. No parameter tuning is required to achieve this scaling. We assume that the number of nodes in an ad hoc network is about one hundred.
- **Availability**: WoN automatically adjusts its internal tables to reflect newly joined nodes as well as node failures. This is true even if the system is in a continuous state of change.
- **Flexible naming**: WoN places no constraints on the structure of the MID it looks up: the MID-space is flat. This gives applications a large amount of flexibility in how they map their own names to MID keys.

3.4 WoN System Architecture

Figure 4 shows the system architecture of WoN in a Unix-like modern operating system. For securing each ad hoc networks independently after building the group membership, we may need to add some new entries to the kernel routing tables. It also may involve implementing queuing for every deferred route to kernel internals, but we think to avoid changing the kernel source code if possible. Thus, we will exploit Linux Netfilter [10], which provides a set of hooks in the kernel networking stack, where kernel modules can register callback functions, and allows them to mangle each packet traversing the corresponding hooks. Moreover, since it is likely that one node belongs to multiple WoNs and each application uses the different

```
/* Already share ManetID through (personal
                contact, direct access, etc). */
Loop {
  ReceiveBroadcastPackets(Message);
  foreach ( ManetID in ManetIDList) {
    if ( Decrypt(Message, ManetID) == true )
      if ( AlreadyReceivedSeq(Message, ManetID)
                                          == true)
        Discard(Message);
      Ttl = ExtractTtl(Message, ManetID);
      MacAddres = ExtractMac(Message, ManetID);
      SrcIPAddress = ExtractSrc(Message, ManetID);
      MemberList = ExtractList(Message, ManetID);
      if (SrcIPAddress == MyIPAddress) {
        MyIPaddress = ChangeMyIPAddress(
                                    MyIPAddress);
        /* Arrage differences of members */
        AddMemberList(ManetID, MacAddress,
                                  MemberList);
        OrigMessage = MakeMessage(ManetID,
                        MyIPAddress, DefaultTtl);
        Message = Encrypt(ManetID, OrigMessage);
        SendBroadcast(Message);
      } else {
        AddMemberList(ManetID, MacAddress,
                                  SrcIPAddress);
        if (TTL >= 1)
          OrigMessage = MakeMessage(ManetID,
                    MemberList+MyIPAddress, Ttl-1);
          Message = Encrypt(ManetID, OrigMessage);
          SendBroadcast(Message)
        else /* TTL == 0 */
          OrigMessage = MakeMessage(ManetID,
            MemberList+MyIPAddress, DefaultTtl);
          Message = Encrypt(ManetID, OrigMessage);
          SendSubnetBroadcast(Message,
                              SubnetIDofIPAddress);
      }
    else Discard(Message);
  }
}
```

Figure 3: **WoN Receiving Algorithm**

MID, we need the mechanism of *Addressing Plane* which controls the relation between multiple MIDs and the applications. In this mechanism, we need to modify each application to use multiple MIDs in one node. To allow that without the modification of applications is our ongoing and future work. We also may need to incorporate security functions such as encrypting messages. We are currently implementing this architecture.

4 Performance Evaluation

We show several preliminary simulation results of WoN. We simulate WoN on several large mobile topologies to qualify and quantify the scaling behavior and the overhead of WoN in Network Simulator (ns2) [15]. In our simulation, the distributed coordination function (DCF) of the IEEE standard 802.11 for wireless LANs is used as the MAC layer. All the simulation parameters are same as the previous salient research work ([1] and [4]) for reasonable comparison.

4.1 Traffic and mobility models

Traffic and mobility models use similar to previous published results using *ns-2* ([1] and [4]) for appropriate performance comparisons. Traffic sources are

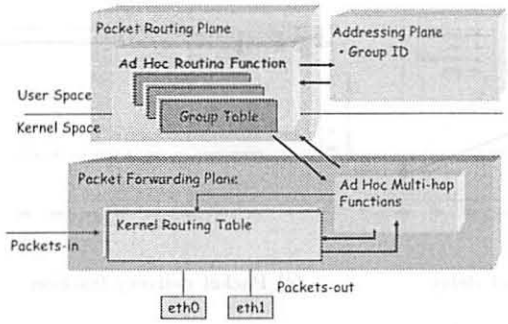


Figure 4: WoN system architecture

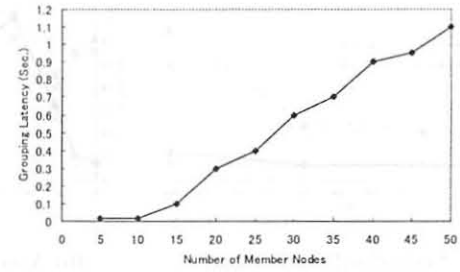


Figure 5: The group construction latency as a function of the num. of group members.

Constant Bit Rate (CBR). The source and destination pairs are spread randomly over the network. Only 512 byte data packets are used. The number of source-destination pairs and the packet sending rate in each pair is varied to change the offered load in the network.

To investigate how WoN system performs in the *realistic* node mobility pattern, we have used the novel two node mobility models: the "random orientation model" and "random escape model" [8]. These mobility models generate some network congestion points and network partitioning areas, respectively. The generated group nodes may be some group having certain purposes. The two models are based on the the *random way-point model* [5] used in most of the previous simulation research. We use these three mobility model in a rectangular area. $1500m \times 300m$ field configuration with 50 nodes is used. We vary the pause time, which affects the relative speeds of the mobile nodes; in this thesis, we used the following pause times (0, 30, 60, 120, 300, 500 [sec]). Simulation are run for 500 simulated seconds for 50 nodes.

4.2 Evaluation Results

Scaling Behavior

First, we have measured the scaling behavior of WoN on the initialization latency in case increasing the number of member nodes (from 5 to 50). The initialization latency is the elapsed time to complete exchanging the group membership information among the group members. This is from the member discovering phase to the finishing phase, after sharing the Manet ID. Figure 5 shows the result. We see that this shows the reasonable linear scaling behavior. Of course, the processing times for handling duplicate IP addresses is included in this result.

Overhead

We evaluated WoN that uses MID as shared keys between communicating and forwarding nodes. We modeled this WoN by modifying the *ns-2* DSR and models in several ways: we increased the packet sizes to reflect the additional fields necessary for authenticating the packets, and modified the handling of Route Discovery and Maintenance phase for the additional encryption and authentication processing in WoN; we adjusted the processing delay. We compare this WoN+DSR versus DSR, and WoN+AODV versus AODV. All protocols were run on identical movement and communication scenarios, in the below each node mobility models. We computed three metrics for each simulation run:

- *Packet Delivery Ratio (PDR)*: The fraction of application level data packets sent that are actually received at the respective destination node.
- *Average Delay*: The average time elapsed from when a data packet is first sent to when it is first received at its destination.
- *Normalized Routing Load*: Compares the number of transmissions of overhead non-data bytes to the number of transmissions of data bytes.

Group Orientation Mobility

This model tends to make several group networks and node congestion points. Thus, we can assume the effectiveness of the active shortening in such a area. In Figure 6(a), 6(b) and 6(c), we can see that the overhead of WoN is negligible in the three metrics. To generate heavy mobility loads, we have set the ratio of oriented nodes to core nodes to *0.8* (i.e., in 50 mobile nodes case, the number of oriented nodes is *40*) .

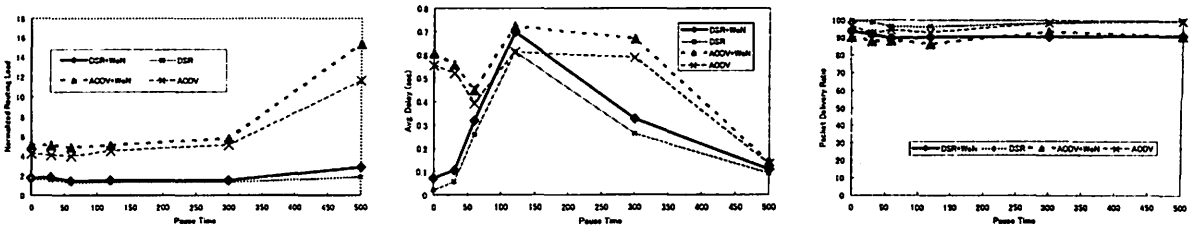
Group Escape Mobility

On the other hand, this model makes some network partition areas intentionally. Thus, mobile ad hoc nodes suffer from frequent link failure and relatively high-speed node mobility. As Figure 7(a), 7(b) and 7(c) show, both WoN protocols degrade its performance marginally as well as the above results. In this case, we used the ratio of escape nodes to core nodes to *0.8*.

5 Future Work

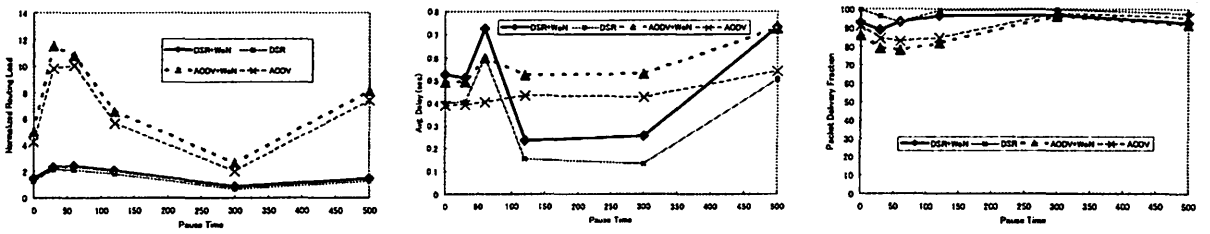
We plan to enhance the security feature of WoN by using asymmetric encryption (or public key encryption) scheme. To evaluate the robustness of WoN, we will construct a model for the types of attacks possible in ubiquitous ad hoc networks and spontaneous computing. In such a environment, WoN needs to exploit encrypted control and data messages always while taking into efficiency and generality consideration.

We will also add WoN to OLSR [3] and TBRPF [11] and evaluate its effectiveness. In



(a) Normalized routing load (b) Average data packet delay (c) Packet delivery fraction

Figure 6: **Group orientation mobility model.**



(a) Normalized routing load (b) Average data packet delay (c) Packet delivery fraction

Figure 7: **Group escape mobility model.**

comparison to DSR and AODV, these two protocols assume larger scale ad hoc networks by using multi-point relays (OLSR) or pro-active link-state source tree computing (TBRPF). By doing so, we can investigate the interoperability issue between on-demand routing and pro-active routing protocols. It is much important thing since AODV, DSR, OLSR, and TBRPF are currently reviewed and well-studied by most of MANET research and IETF working groups.

Of course, we need to complete experimental implementation and evaluations of WoN as rapidly as possible. That is our long term goal of our research. Implementing WoN in real life seems to be significantly relate to Zero-Configuration architecture [16] and ad hoc routing protocols. Also, the application of WoN to group management of ad hoc sensor networks should be interesting research.

References

[1] Josh Broch, David A. Maltz, David B. Johnson, Yih-Chun Hu, and Jorjeta Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *Proceedings of ACM/IEEE MobiCom'98*, October 1998.

[2] Wenli Chen, Nitin Jain, and Suresh Singh. ANMP: Ad Hoc Network Management Protocol. *IEEE Journal on Selected Areas in Communications*, 17(8):1506–1531, Aug 1999.

[3] T. Clausen and Philippe Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626, October 2003.

[4] Samir R. Das, Charles E. Perkins, and Elizabeth M. Royer. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. In *Proceedings of IEEE INFOCOM'00*, pages 3–12, March 2000.

[5] David B. Johnson and David A. Maltz. *Dynamic Source Routing in Ad Hoc Wireless Networks.* In Mobile Computing, edited by Tomasz Imeilinski and Hank Korth, chapter 5, pages 153-181, Kluwer Academic Publishers, 1996.

[6] David B. Johnson, David A. Maltz, and Yin-Chun Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. IETF Internet-Draft [Work in Progress], July 2004.

[7] Silja Maki, Tuomas Aura, and Maarit Hietalahti. Robust Membership Management for Ad-hoc Groups. In *Proceedings of the 5th Nordic Workshop on Secure IT Systems (NORDSEC 2000)*, October 2000.

[8] Masato Saito, Hiroto Aida, Yoshito Tobe, and Hideyuki Tokuda. A Proximity-based Dynamic Path Shortening Scheme for Ubiquitous Ad Hoc Networks. In *Proceedings of IEEE International Conference on Distributed Computing Systems (ICDCS'04)*, March 2004.

[9] J. Moy. Open Shortest Path First (OSPF) Version 2, July 1997.

[10] The netfilter/iptables project. netfilter. http://www.netfilter.org/.

[11] R. Ogier, F. Templin, and M. Lewis. Topology Dissemination Based on Reverse Path Forwarding (TBRPF). RFC 3684, February 2004.

[12] Charles E. Perkins, Elizabeth M. Royer, and Samir R. Das. Ad Hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[13] Ion Stoica, Daniel Adkins, Shelley Zhuang, Scott Shenker, and Sonesh Surana. Internet Indirection Infrastructure. In *Proceedings of ACM SIGCOMM'02*, pages 73–86, August 2002.

[14] Ion Stoica, Robert Morris, David Karger, Frans Kaashoek, and Hari Balakrishnan. Chord: A Scalable Peer-To-Peer Lookup Service for Internet Applications. In *Proceedings of ACM SIGCOMM'01*, pages 149–160, August 2001.

[15] The VINT Project. Network simulator - ns2. http://www.isi.edu/nsnam/ns, 2001.

[16] The Zeroconf Working Group. Zero Configuration Networking (Zeroconf) [Work in Progress]. http://www.zeroconf.org/, 1999-9.