A Secure Multiple Ad Hoc Networks Management for Ubiquitous Spontaneous Computing

Masato Saito

Graduate School of Media and Governance
Keio University
5322 Endo, Fujisawa Kanagawa 252-8520 JAPAN

Submitted in partial fulfillment of the requirements for the degree of Master of Media and Governance (Information Technology)

Thesis Supervisors:

Hideyuki Tokuda
Professor of Environmental Information, and Media and Governance, Keio University

Jun Murai
Professor of Environmental Information, Keio University

Yoshito Tobe
Professor of Information Systems and Multimedia Design, Tokyo Denki University

Abstract of Master's Thesis Academic

A Secure Multiple Ad Hoc Networks Management for Ubiquitous Spontaneous Computing

Mobile ad hoc networks (MANET) are groups of wireless mobile computers (or nodes), in which each node cooperates by forwarding packets for one another to allow nodes to communicate beyond one-hop wireless transmission range. Prior research in MANET has mainly focused on the routing functions in a uniformly and trustful environment. For instance, it is assumed that all the nodes in a specific area implement one particular routing protocol and have the accessible IP addresses uniformly.

In this thesis, we present a group separating scheme based on group identifier (MANET-ID: MID), and describe the design and performance evaluation of a secure MANET management method, called WoN. WoN realizes secure group communication by encrypting messages based on MIDs, and allows multiple MANET routing protocols to coexistent in the same area, by conducting MID-based routing separation.

Simulation studies for several scenarios of node mobility and traffic flows have revealed that adding WoN to prior proposed routing protocols (DSR and AODV) produces little overhead of routing control packets and has the good scaling behavior. In addition, we have shown that MID-based routing protocols maintains the independence behavior to other routing protocols.

Keywords:
1. Ad hoc networks, 2. Security, 3. Group Management, 4.Routing Protocol Interoperability,
5. Simulation

Masato Saito
Graduate School of Media and Governance
Keio University

修士論文要旨　　2003年度(平成15年度)

A Secure Multiple Ad Hoc Networks Management for Ubiquitous Spontaneous Computing

「セキュリティを考慮した複数アドホックネットワーク管理機構の提案と評価」

携帯通信端末の急速な普及や無線通信技術の発達に伴い、移動通信端末同士を自律的に、かつ動的に接続するモバイルアドホックネットワーク (Mobile Ad hoc NETworks: MANET) が広く注目を集めている。MANET は、インフラストラクチャ非依存、無線マルチホップ通信、端末の動的移動といった現在のインターネットでは想定外の特徴を持つ次世代無線通信ネットワークである。MANET の実現のために、経路制御プロトコルの提案・改良を中心として様々な研究が行われている。

しかし、既存の多くの MANET 研究では、ある場所に存在する端末群は全て均一の経路制御プロトコルを実装、IP アドレスはあらかじめ割当済みである、といった非現実的な前提が置かれている。実際の現実世界においては、同一地点・地域において複数主体が MANET を構築するといったことは頻繁にありうる。そこで、本研究では移動端末群をグループ識別子に基づいてグループ化し、その識別子に基づいて経路制御を行うための MANET 管理機構：WoN を提案する。WoN では、グループ識別子を使用して経路制御・通信メッセージの暗号化を行うことで悪意端末やマルチホップ転送端末に対するセキュリティ耐性を高める。さらに、複数の性質の異なる経路制御プロトコル群を同一地域で同時に稼働させることも可能となる。

移動端末数を 50 台としたアドホックネットワークを想定して、シミュレータ上における本プロトコルの評価結果を示す。本プロトコルを既存の DSR (Dynamic Source Routing) や AODV (Ad hoc On-demand Distance Vector routing) といった経路制御プロトコルに組み込み、本機構による経路制御パケット・オーバヘッドの小ささやスケーラビリティの高さを提示する。

キーワード:
1. アドホックネットワーク, 2. セキュリティ, 3. グループ管理, 4.経路制御プロトコル相互接続性, 5.シミュレーション

慶應義塾大学大学院　政策・メディア研究科
斉藤 匡人

Table of Contents

List of Figures

List of Tables

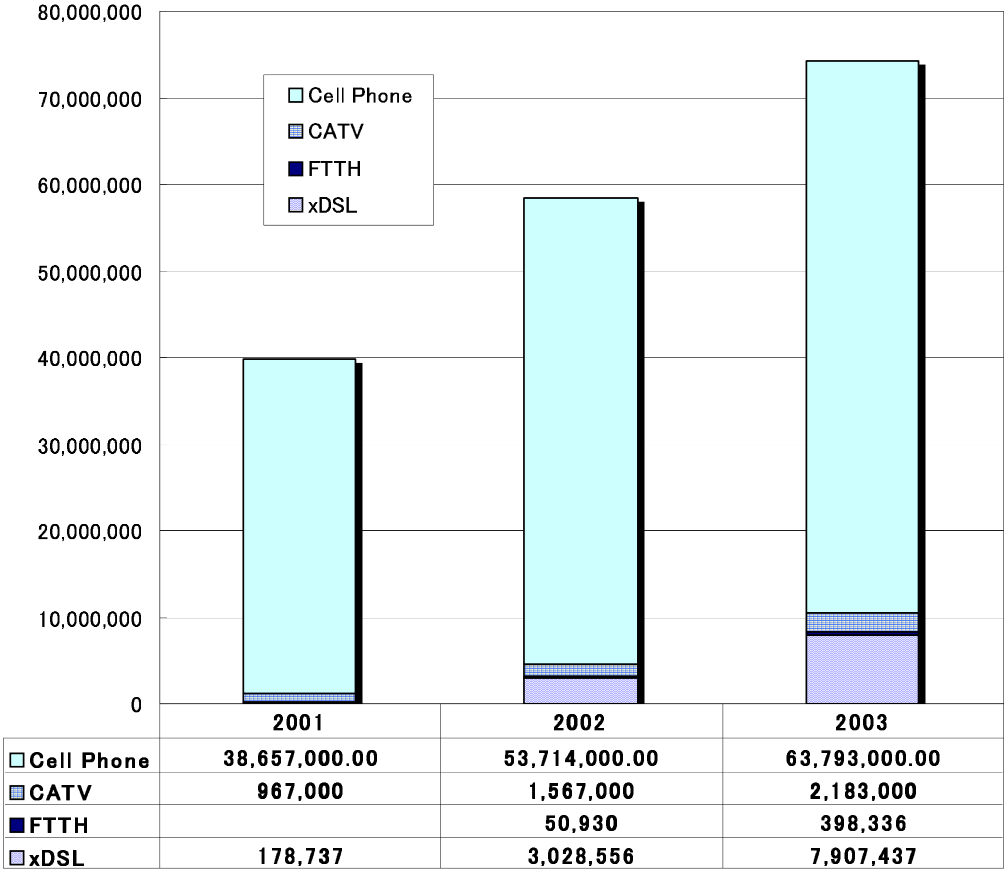
Chapter 1

Introduction

1.1 Motivation

Currently, we are remarkably benefiting from various wireless computer devices. Wireless computers range from laptops, hand-held Personal Digital Assistants (PDAs) (e.g., Palm [51]), and cell phones to sensor devices, information appliances, and palm-top game consoles. Most of them have the communication functions to access the Internet. Although the communication bandwidth of these devices are relatively narrow compared to the connections of tethered desktops or servers, these wireless devices have been tremendously deployed everywhere. Figure 1.1 shows the current transitions per the *subscribers* of major Internet access media in Japan. Since the present population of Japan is about 130 million, we can see a lot of people have been accessing the Internet. The Internet accesses via cellulars are still increasingly dominant. These accesses include three Internet services from i-mode [48] of NTT-DoCoMo, EZweb [33] of KDDI, and J-sky [67] of Vodafone. Future advances of the other PDAs or palm-top game consoles will be increased the number of wireless Internet accesses more and more.

However, one important thing is not increasing wireless devices which can access Internet, but pervading wireless communicating devices everywhere and being diverse in terms of access media and terminal forms. Figure 1.2 shows that the distribution which access



	2001	2002	2003
□Cell Phone	38,657,000.00	53,714,000.00	63,793,000.00
▦CATV	967,000	1,567,000	2,183,000
■FTTH		50,930	398,336
□xDSL	178,737	3,028,556	7,907,437

Figure 1.1: Comparison between the subscribers of main Internet access media.
Original Sources: http://www.soumu.go.jp/s-news/2003/030627_5.html, Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan, May 2003

terminals people select to connect the Internet in Japan [42]. Even the game consoles, TVs, and appliances have been providing communication features. As the dominance of cellular Internet subscribers is shown in the preceding figure, we can see that personal computers have been still dominant of the actual Internet access terminals. We think it is due to the poorness of user interfaces, the narrow bandwidth, and the lack of systematic mobile computing supports and environments of mobile computers. In the near future, most of us would be becoming to have multiple Internet access or communication devices whether wireless or

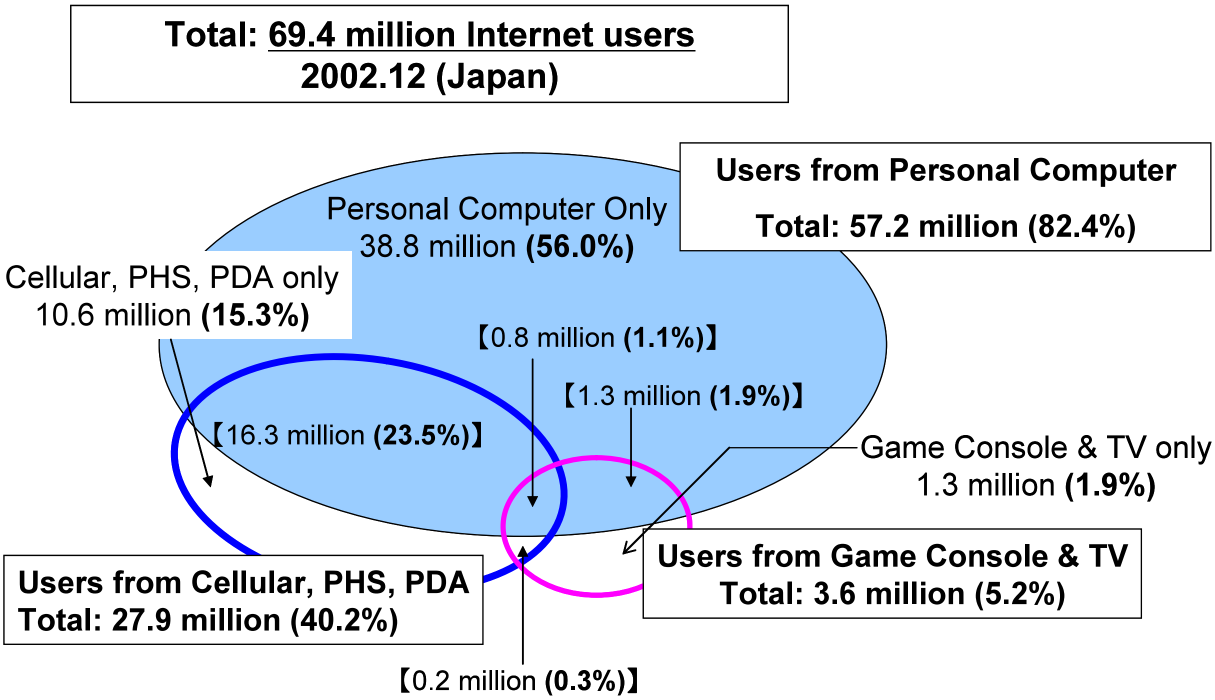


Figure 1.2: The distribution of Internet access terminals which people have chiefly used in Japan. *Original Sources: White Paper 2003 "Information and Communications in Japan," Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan, 2003*

not. There are already many challenges in the area of mobile computing.

Though the users of personal computers (including laptops and desktops), cellulars, PHS and PDA dominate the large part of all, in fact, the saturation levels of these communicating devices have nearly peaked in Japan. We can see the tendency in Figure 1.3. This figure presents the recent shipment numbers of PCs, cellulars, PDAs, and telematics in Japan. In this figure, PDAs is distinct from PCs whether having Hard-Disks or not, and telematics include car navigation terminals and its modules. Note that although PCs, cellulars and PDAs seem to have been reaching the peak, telematics field have been rapidly growing. For example, up-to-date telematics have implemented functions of HD recording, DVD playing, and the Internet accessing. Telematics and high-speed car information systems would be impose the more challenges to mobile computing.

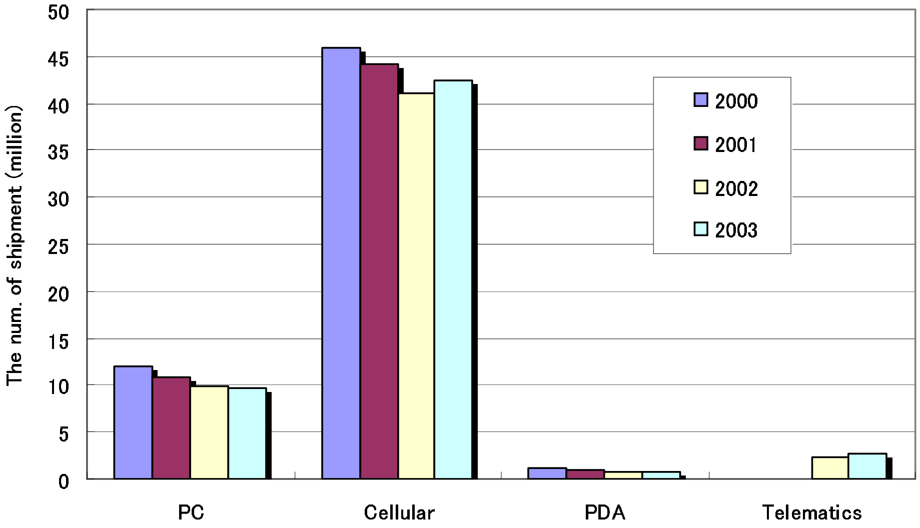


Figure 1.3: Recent shipment transitions of PC, Cellular, PDA, and Telematics.
Original Sources: http://www.nri.co.jp/news/2003/031120.html, Nomura Research Institute, Ltd., Japan, Nov 2003

Cellular terminals also have been steadily evolving. For instance, the functions of TV viewing, GPS navigation, biometrics authentications, and high quality gaming and the modules of digital cameras, integrated-circuits, and various sensors have been added to mobiles. The network bandwidth of data connection is also becoming wider up to about 2.4 Mbps such as CDMA 1X WIN of KDDI [32]. The dual-band mobile phones mounting wireless LAN interfaces (802.11b) and W-CDMA connections will be about to release within a few years by NTT DoCoMo [47]. As stated above, Japan still has the potential big market of mobile computing. Figure 1.4 shows Internet-ready cellulars "ratio" to overall per major world nations [43]. Japan has the top position in the world.

Along with wireless access terminals, the access media are also becoming diverse and enhanced. There are a number of wireless access technologies enabling the internet access even while moving around (e.g., 802.11a and 802.11g [21], Bluetooth [62], Ultra-WideBand

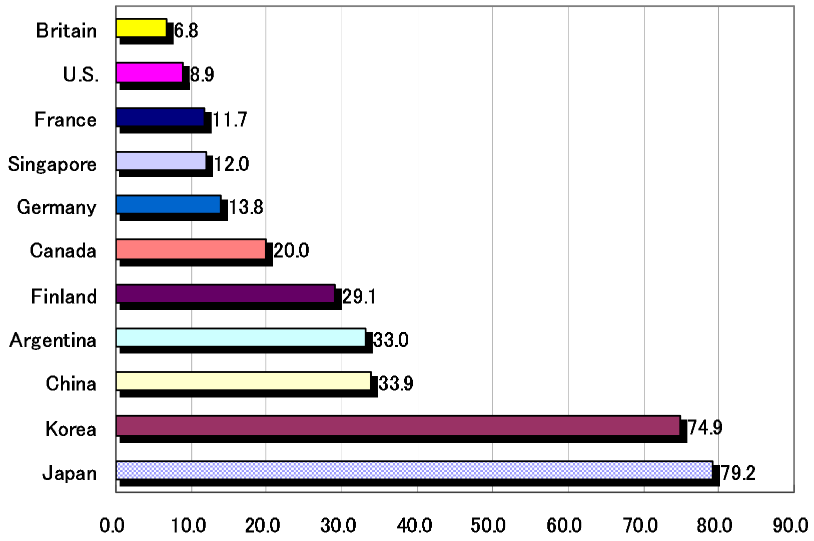


Figure 1.4: Comparison of Internet-ready cellulars "ratio" to overall cellulars per major nations. *Original Sources: White Paper 2003 "Information and Communications in Japan," Ministry of Public Management, Home Affairs, Posts and Telecommunications, Japan, 2003*

(UWB) [66], ZigBee [74], W-CDMA, or CDMA 2000 1x). We could expect that the advancement of wireless technologies realize high data throughput and high node-mobility simultaneously in the near future.

As wireless communicating devices including sensors and RFIDs are becoming ubiquitous around our environments, we believe that these wireless devices automatically connect each other directly and make the distributed novel type of mobile networks called mobile ad hoc networks (MANET), then it would lead to enrich our daily and social life furthermore. There has already been a renewed interest in MANET due to the common availability of relatively low-cost laptops and palm-tops with wireless interfaces. The interest is also caused by growing enthusiasm in running TCP/IP protocol suites in dynamic wireless environments without specific infrastructures for emergency disaster situations after earthquake or a hurricane, or the battlefield.

There are several scenarios where ubiquitous ad hoc networks are useful. One major application is a military-use communication in a battlefield where a centralized configuration is difficult (e.g., in the enemy jungle). Another application is emergency communication in disaster areas. In addition to these large-sized applications, we can use ad hoc networks when several people have meetings with computers that are equipped with wireless interfaces. Also, it can be interesting research to support intelligent transport systems and sensor networks. Above all, we are thinking ad hoc networks are good chemistry with spontaneous computing and networking which seem to be important in the future ubiquitous computing world.

Since the communicating devices (or nodes) can be mobile, the dynamic network topology of ad hoc networks would lead to be variable and serious effects on the network characteristics compared to the Internet tethered networking environment. Thus, the previous network system functions such as routing, address allocation, authentication, and authorization must be re-designed to cope with dynamic and temporary network topology changes. We should also think the mechanisms to provide the Internet connectivity for MANETs. Additionally, wireless network nodes will often be limited battery powered, which limits the capacity of CPU, memory and bandwidth. This would require network functions to be resource-efficient. Security in MANET should also be needed to take into account.

In this thesis, we identify and solve the fundamental problems of the above mentioned “ubiquitous ad hoc networks” that are **security, nodes grouping, and routing protocol interoperability**.

1.2 Challenges and Contributions

Recent advancement in wireless communications and electronics and spread of mobile computing devices have enabled 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 base stations or access points. Each node in the network can act as both a host and a router forwarding data packets to other nodes. Applications such as disaster relief, intelligent transport systems, and cellular system supporting might be expected using ad hoc networking, but secure and spontaneous communication is a required nature for such applications.

Since node mobility in ad hoc networks causes frequent, unpredictable and drastic changes to the network topology, it is especially important for communicating nodes to grasp changes of the network topology and find efficient routes between two communicating nodes. Ad hoc network routing protocols are fairly challenging to design and implement. Wired network routing protocols such as BGP [60] or OSPF [45] 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. Thus, a number of research for MANET have focused on the development of their routing protocols (e.g., AODV [54], DSR [29], LAR [34], OLSR [13], TBRPF [49], ZRP [72]). 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 beforehand, or one routing protocol is used in an ad hoc networks. 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 thesis, we propose a secure group management scheme 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 randomly and are allocated to each MANET group. In spontaneous and ubiquitous MANETs, the network age seems to be not long but rather short that distributed network addressing scheme including duplicate address detections is an expensive approach. Thus, 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 thesis. First, **we show several research issues of ad hoc network initialization in realistic environment**. Second, **we present the design and evaluation of a group separating scheme based on ad hoc group ID (MANET-ID: MID), called WoN, to build secure, spontaneous, and separated ad hoc networks**. Third, **we give the first method to co-exist various ad hoc network routing protocols in one same area**.

1.3 Structure of Thesis

The rest of this thesis is organized as follows.

Chapter 2 describes background materials in the area of wireless networks and MANETs, the future directions on where ubiquitous computing and MANET (Bubble Networks) are converging everywhere, and its applications. In Chapter 3, we present the problem definitions of this thesis about the security and protocol interoperability for MANET. Then, we discuss the design and the detailed description of our WoN which employs secure MANET managements in Chapter 4, and Chapter 5 gives the implementation of OR2 in the packet-level simulator. In Chapter 6, we present the evaluation results and analyses of several simulation studies, and how multiple MANET routing protocols (such as DSR and AODV) interoperate in the same area simultaneously. Finally, in Chapter 7, we present conclusions and discuss several future work.

Chapter 2

Research Background

This chapter describes the research background of this thesis. We first present an overview of wireless networks. Next, we focus and explain various wireless LAN technologies which are assumed environments of our research. Then, we describe an overview of mobile ad hoc networks and the four main proposed routing protocols for MANET. Finally we introduce the future ubiquitous computing and bubble networking as our research background.

2.1 Overview of Wireless Networks

For a start, let us review a summary of wireless networks. The wide range of wireless networks includes in-room infrared and bluetooth networks, building-wide wireless LANs, campus-area packet radio and hot spot wireless networks, metropolitan-area cellular wireless networks, regional-area fixed wireless cable networks, and broadcast satellite networks. Figure 2.1 shows the entire picture of current wireless overlay network architecture [2]. These wireless networks are different from each other in terms of maximum raw bandwidth, channel access mechanisms, link protocols, frequency, power, and covering mobility. Among them, we regard the conventional campus-area and hot spot wireless LAN networks as the basis of our research target. These wireless LAN networks are surely promising because of recent advancement of wireless networking technologies and prevalence of wireless communicating devices

2.2 Wireless LAN Technologies

This section explains wireless LAN technologies throughly. We describe the popular and promising wireless technologies related to this thesis.

Wireless LANs are mainly in-room, in-building, or small-area (e.g., up to about 300 meter) networks that provide maximum bandwidth between 1 and 54 Mbps over a relatively small range. Practical used examples of them include IBM's infrared, Lucent's WaveLAN [50], IEEE 802.11b [23], 802.11a [22], 802.11g [24], and Bluetooth. Most of them operate in the unlicensed Industrial, Scientific and Medical (ISM) bands at 915 MHz, 2.4 GHz and 5 GHz that have been set aside by the national regulations for experimental purposes. Almost these technologies include medium access control (MAC) and physical layer (PHY) specifications. Not yet made public, future wireless LAN specifications such as UWB and IEEE 802.11n

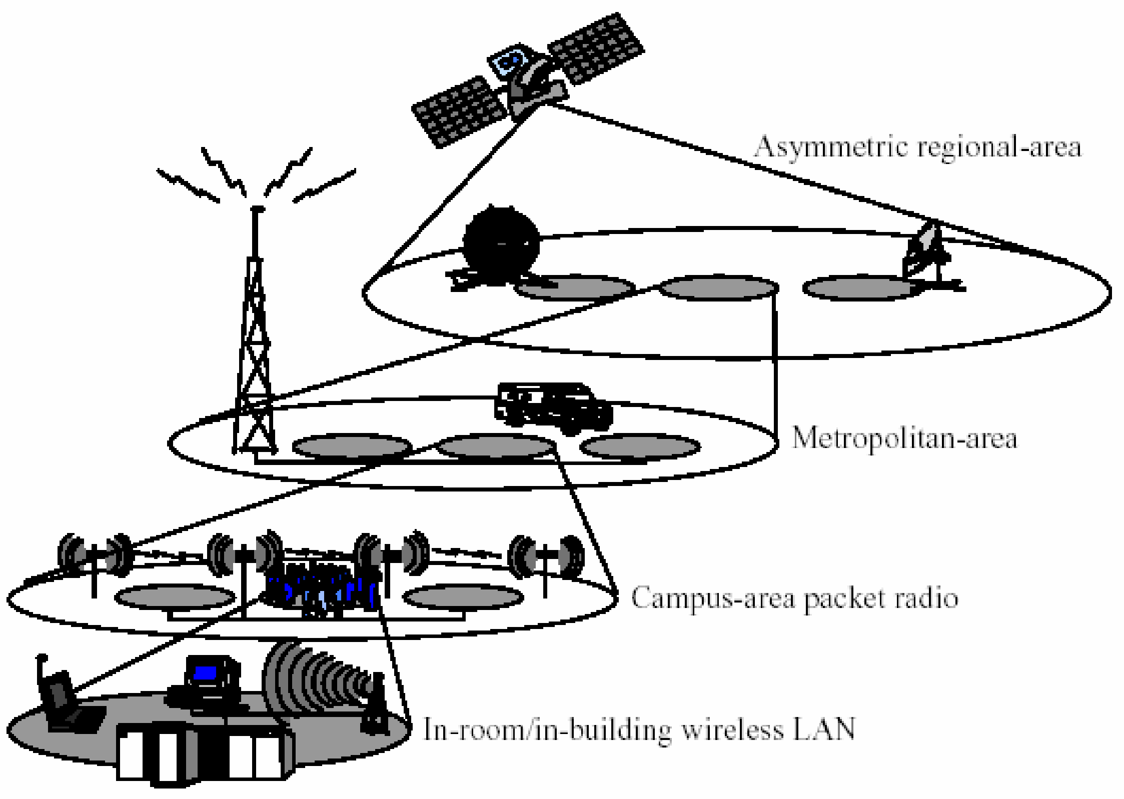


Figure 2.1: Wireless overlay network architecture.
Sources: Challenges to Reliable Data Transport over Heterogeneous Wireless Networks, Hari Balakrishnan, Ph.D. Thesis, 1998

would be expected to achieve data rate over 100 Mbps.

In what follows, we outline several related wireless technologies and standards briefly.

2.2.1 CSMA/CA

The Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) is a channel access scheme used by most *wireless LANs* in the ISM bands. For example, IEEE 802.11 [21] and WaveLAN [65] specifications adopt this mechanism. Channel access methods is one part of a protocol that defines how one node uses the access medium.

The basic principle of CSMA/CA is listen before talk and contention. This is an asynchronous message passing mechanism (connection-less), realizing the best effort service, but no bandwidth and latency guarantee. The main advantages are that it is suited for network communicating protocols such as TCP/IP, adapts quite well with variable conditions of data traffic and surrounding environments, and is fairly robust against wireless interferences.

CSMA/CA is derived from CSMA/CD (Collision Detection), which is the base of wired Ethernet. The main difference is in the collision avoidance methods: on a wire environment, transceivers have the ability to listen access medium while transmitting, so they could detect collisions However, even if a radio node could listen on the channel while transmitting, the strength of its own transmissions would mask all other signals on the air. It is because the difference of electric power between transmission and reception is substantially large. So, the protocol cannot directly detect collisions like with Ethernet and only tries to avoid them.

2.2.2 WaveLAN and IEEE 802.11

WaveLAN operates in either the 902-928 MHz or the 2.4-2.8 GHz ISM license-free bands. WaveLAN employs a Ethernet-like CSMA/CD MAC protocol. WaveLAN network interfaces equips with standard Intel 82593 single-chip CSMA/CD LAN controllers, custom logic for signal processing and modem control, and a custom radio transceiver. The transmitter applies DQPSK modulation to a 2 megabit/s data stream, yielding a 1 megabaud signal. This signal is further modulated by an 11 chip per bit sequence to produce an 11 MHz wide signal which is transmitted with a power antennas and multiple incoming signal paths to combat multi-path interference.

Generally, 802.11 refers to a family of specifications developed by the IEEE for wireless LAN technology. 802.11 specifies an over-the-air interface between a wireless client and a base station (i.e, infrastructure mode) or between two wireless clients (i.e, ad hoc mode). The IEEE accepted the specification in 1997. As one of the 802.11 standards, 802.11 is applied to wireless LANs and provides 1 or 2 Mbps transmission in the 2.4 GHz band using either frequency hopping spread spectrum (FHSS) or direct sequence spread spectrum (DSSS). Most 802.11-family commercial products adopt DSSS. This standard defines the medium access control (MAC) and physical layers (PHY) for a LAN with wireless connectivity. It addresses local area networking where the connected devices communicate over the air to other devices that are within close proximity to each other. As an optional feature, the 802.11 standard includes the RTS/CTS (Request to Send/Clear to Send) function to control station access to the medium, in particular to handle the problem of hidden terminals.

From early stages of MANET research, WaveLAN and 802.11 technologies have often been assumed and used as an underlying layer of MANET routing protocols.

2.2.3 IEEE 802.11b, a, g, e, h, and i

IEEE 802.11 has so far derived many supplemental and exnteded specifications of wireless LAN technologies. They are individually having wide variety of sophisticated features relative to the original 802.11: 802.11b, a, and g provide higher-speed data transmissions up to 54 Mbps, 802.11e supports Quality of Service (QoS) in wireless LANs for multimedia applications such as VoIP, streaming video and provides the means of prioritizing the radio channel access by different stations and data streams, 802.11h tries to avoid wireless interference by changing the frequency dynamically and enhance channel energy measurement and reporting mechanisms to improve spectrum and transmit power management of 802.11a, and 802.11i improves and enhances security and authentication mechanisms of 802.11 MAC. Figure 2.2 presents the current and future flows of various 802.11-derived standard establishments.

We are concerned here with 802.11b, a, and g, since they would seem to be most appropriate wireless technologies for MANET. 802.11b (also referred to as 802.11 High Rate or Wi-Fi) is an extension to 802.11 and provides 11 Mbps transmission (with a fallback to 5.5, 2 and 1 Mbps) in the 2.4 GHz band. 802.11b uses only DSSS. 802.11b was a 1999 ratification to the original 802.11 standard, allowing wireless functionality comparable to Ethernet. 802.11b-compatible commercial wireless LAN products are most dominant, and most laptop computers install 802.11b wireless LAN interfaces by default. 802.11a is an extension to 802.11 that applies to wireless LANs and provides up to 54 Mbps in the 5GHz band. 802.11a uses an orthogonal frequency division multiplexing (OFDM) encoding scheme rather than FHSS or DSSS. 802.11g applies to wireless LANs and provides 20+ Mbps in the 2.4 GHz band. 802.11a and g compatible products have currently appeared to public, several advanced notebooks implement these wireless interfaces in the default. In Japan, 802.11b, a, and g supported wireless access points and other products have already been sold.

Some of current MANET research have targeted or focused on 802.11b [38, 18], 802.11a [56, 55], or 802.11e [17].

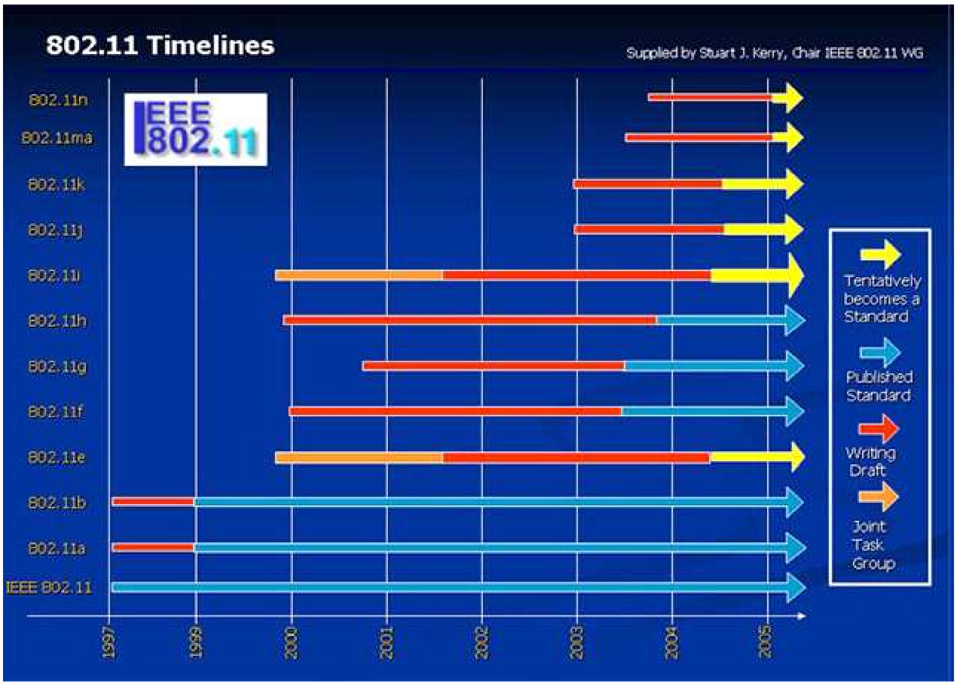


Figure 2.2: Current flows of 802.11 standards establishment.
Sources: Wi-Fi Planet Conference & Expo,
http://pcweb.mycom.co.jp/news/2003/12/09/32.html, 2003

2.2.4 Bluetooth and UWB

Bluetooth is a short-range radio technology aimed at simplifying communications among Internet devices and between devices and the Internet. It also aims to simplify data synchronization between Internet devices and other computers. Products with Bluetooth technology must be qualified and passed interoperability testing by the Bluetooth Special Interest Group prior to release. Many Bluetooth-enabled products are already released in the various forms such as computer mice, keyboards, handsets, telematics, laptop computers, cellulars, PDAs, and printers. Bluetooth is intended to create short-term local network connections among nearby devices in such environments as personal area networks and home area networks. Some Bluetooth-based MANET research have been proposed [35, 73, 9]. However, the Bluetooth protocol stack is not really designed for TCP/IP, and the initialization procedure for setting up networking seems to be time-consumed and a bit complex, so it is not well appropriate for MANET aiming at ubiquitous spontaneous computing.

Ultra Wide Band (UWB) is a wireless communications technology that can currently transmit data at speeds between 40 to 60 megabits per second and eventually up to 1 gigabit per second. UWB transmits ultra-low power radio signals with very short electrical pulses, often in the picosecond (1/1000th of a nanosecond) range, across all frequencies at once. UWB receivers must translate these short bursts of noise into data by listening for a familiar pulse sequence sent by the transmitter. Because of its low power requirements, UWB is very difficult to detect and therefore difficult to regulate. Because it spans the entire frequency spectrum (licensed and unlicensed), it can be used indoors and underground, unlike GPS. UWB has three basic areas of applications, which are communication, positioning and imaging. The main commercial application will be for communication, but it can also be used for both indoor and outdoor 3-D positioning. Another important application is high resolution imaging like microwave remote sensing. An UWB sensor can pass through doors and walls and hence detect the objects inside the room or under the ground. UWB products is still under research and development, but it would be extremely interesting research of MANET using the UWB communication and radar.

2.3 Mobile Ad Hoc Networks

This section describes an overview of mobile ad hoc networks and previously proposed major routing protocols. Then, we discuss the current directions of MANET research.

2.3.1 Overview

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 require any stationary infrastructure such as base stations. Each node in the network can act as both a host and a router forwarding data packets to other nodes.

Since node mobility in an ad hoc network causes frequent, unpredictable and drastic changes to the network topology, it is especially important for communicating nodes to grasp changes of the network topology and find efficient routes between two communicating nodes. A number of research for mobile ad hoc networks have focused on the development of their routing protocols (e.g., AODV [54], DSDV [53], DSR [29], LAR [34], OLSR [13], TBRPF [49], TORA [52], ZRP [72]). These routing protocols can be classified into three types: *pro-active*(DSDV, OLSR, and TBRPF), *reactive*(AODV, DSR, LAR, and TORA) and *hybrid*(ZRP). Pro-active protocols attempt to continuously evaluate the routes within the network, so that when a packet needs to be forwarded, the route is already known and can be immediately used. On the other hand, reactive protocols invoke a route determination procedure on an *on-demand* basis. Lastly, hybrid protocols are mixture of reactive/pro-active scheme. The Location-Aided Routing (LAR) protocol utilizes location information (for instance, obtained using the global positioning system) to improve performance of routing protocols. By using location information, LAR protocol limits the search for a new route to a smaller request zone of the ad hoc network.

Some comparisons between these different protocols have been published [6], [27]. Both reported results based on simulations show that the reactive protocols perform significantly better than traditional pro-active protocols (e.g., DSDV, ZRP) in most situations. The key advantage behind on-demand protocols is the reduction of routing overheads. On-demand routing protocols maintain only active paths to destinations to which data must be sent. Minimizing the routing overhead is required in such a dynamic environment of ad hoc networks due to limited available bandwidth, unpredictable nodes mobility, battery outages, interference and high bit error rates.

2.3.2 Routing Protocols

We present descriptions of the remarkable four proposed routing protocols for mobile ad hoc networks. These routing protocols have been submitted to the Mobile Ad-hoc Networks (MANET) working group [44] in the Internet Engineering Task Force (IETF) [25]. AODV and OLSR have recently been available as Request for Comments (RFC). DSR and AODV are on-demand protocols, OLSR and TBRPF are pro-active protocols.

- **The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR)**

  The Dynamic Source Routing protocol (DSR [29]) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of “Route Discovery” and “Route

Maintenance," which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use. The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only "soft state" in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes, and is designed to work well with even very high rates of mobility. This document specifies the operation of the DSR protocol for routing unicast IPv4 packets.

- **Ad hoc On-Demand Distance Vector (AODV) Routing**

  The Ad hoc On-Demand Distance Vector (AODV [54]) routing protocol is intended for use by mobile nodes in an ad hoc network. It offers quick adaptation to dynamic link conditions, low processing and memory overhead, low network utilization, and determines unicast routes to destinations within the ad hoc network. It uses destination sequence numbers to ensure loop freedom at all times (even in the face of anomalous delivery of routing control messages), avoiding problems (such as "counting to infinity") associated with classical distance vector protocols.

- **Optimized Link State Routing Protocol (OLSR)**

  The Optimized Link State Routing (OLSR [13]) protocol for mobile ad hoc networks is an optimization of the classical link state algorithm tailored to the requirements of a mobile wireless LAN. The key concept used in the protocol is that of multipoint relays

(MPRs). MPRs are selected nodes which forward broadcast messages during the flooding process. This technique substantially reduces the message overhead as compared to a classical flooding mechanism, where every node retransmits each message when it receives the first copy of the message. In OLSR, link state information is generated only by nodes elected as MPRs. Thus, a second optimization is achieved by minimizing the number of control messages flooded in the network. As a third optimization, an MPR node may chose to report only links between itself and its MPR selectors. Hence, as contrary to the classic link state algorithm, partial link state information is distributed in the network. This information is then used for route calculation. OLSR provides optimal routes (in terms of number of hops). The protocol is particularly suitable for large and dense networks as the technique of MPRs works well in this context.

- **Topology Dissemination Based on Reverse-Path Forwarding (TBRPF)**

  The Topology Dissemination Based on Reverse-Path Forwarding (TBRPF [49]) is a proactive, link-state routing protocol designed for mobile ad-hoc networks, which provides hop-by-hop routing along shortest paths to each destination. Each node running TBRPF computes a source tree (providing paths to all reachable nodes) based on partial topology information stored in its topology table, using a modification of Dijkstra's algorithm. To minimize overhead, each node reports only *part* of its source tree to neighbors. TBRPF uses a combination of periodic and differential updates to keep all neighbors informed of the reported part of its source tree. Each node also has the option to report additional topology information (up to the full topology), to provide improved robustness in highly mobile networks. TBRPF performs neighbor discovery using "differential" HELLO messages which report only *changes* in the status of neighbors. This results in HELLO messages that are much smaller than those of other link-state routing protocols such as OSPF.

2.3.3 Current Research Directions

So far, researchers in ad hoc networking have typically studied the routing problems, but a wide variety of research topics are attacked: e.g., security [20, 7], power management [10, 70, 36], medium access control technologies [19, 30], provisioning QoS [37], route discovery [69, 16], node mobility models [26, 71], etc. Another MANET research tries to explore characteristics and effects on routing using directional antennas as wireless communication media [3]. Studies for providing global internet connectivity for MANET have been done in both area of IPv4 and IPv6 [4, 68]. Although most of prior studies of routing protocols and methods are simulation based, research with real implementations and validating MANET algorithms in real systems are taking place recently [14, 31]. Several commercial MANET products have been released and deployed but yet small-scale [41, 59].

However, **most of the above mentioned research and products are assuming and targetting a general-purpose and uniform network setting: uses one specific MANET routing protocol, consists of members having the same purposes or properties, there is one MANET in the same area, etc**. These assumptions are unrealistic, validating the algorithms in real setting and environments is necessary for their deployment in the real world.

2.4 Ubiquitous Computing and Bubble Networking

In this section, we introduce the future ubiquitous computing and bubble networking as our research background and expectation. We here define MANETs for ubiquitous spontaneous computing as bubble networks. It seems to be a novel networking paradigm.

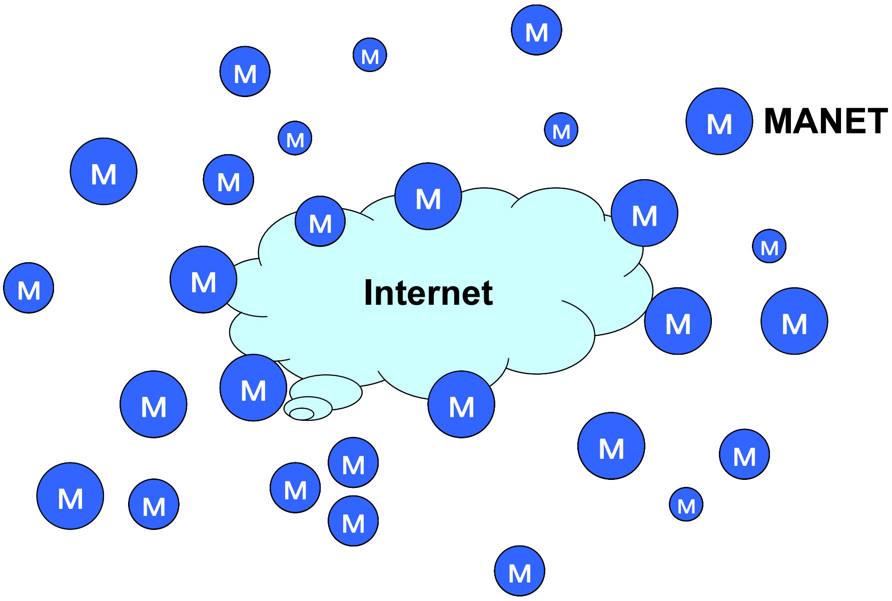


Figure 2.3: A prospective picture of Internet and MANETs, we name it Bubble networking.

2.4.1 UbiComp and BubNet

Ubiquitous computing (UbiComp) is an environment where communicating computers, devices, and sensors are ubiquitous unevenly. People and our social life are expected to proliferating more by UbiComp environments. In such a environment, all the nodes need not necessarily connect the Internet, but independent local area private communications are possibly taking place everywhere. These networking and communications seem to be short-lived compared to current wired networks and access points based wireless LAN communications. They are just like bubbles, constructing spontaneously, and disappearing instantly. This Bubble Network (BubNet) is built from MANET technologies, and we think that BubNet is one specific form of MANETs. To realize such ubiquitous private spontaneous networking, our secure MANET management technology is really needed. Figure 2.3 shows the future world of the Internet and BubNets.

2.4.2 Applications

We present several future applications of BubNets. Most of them are same as the possible applications of MANET. They include (1) personal area networking by mobiles, PDAs, and wearable computers, (2) civilian environment networking including car networks, sensor networks, robot networks for sharing data and messages instantly or playing entertainment computing, (3) emergency operations such as search-and-rescue, policing, or fire fighting, (4) enemy environment networking in military or business, etc. However, to deploy and use these applications readily, ubiquitously and safely, we need to think **group management and security** in BubNets. We try to describe the reasons and details in the next Chapter.

Chapter 3

Group Management and Security in Mobile Ad Hoc Networks

This chapter describes several related work of group management and security in MANET. We present an overview of group management for MANET at first. After we demonstrate problems of the previous research especially on the initial phase of MANET formation relating to group management and security, we summarize problem definitions that this thesis works on.

3.1 Overview of 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.

3.2 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. On the other hand, security research for MANET has recently gathered many attention. We present some work on secure routing, key management, and cooperation in MANET,

3.2.1 Group Management

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. [11] 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. [39] 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 is not clear and considered well. The node addressing issue should also be raised. We believe that in designing ubiquitously spontaneous MANET system, considering group management, node addressing, and routing simultaneously is highly required to realize reasonable and sustainable system.

Not assuming MANET environment, Reiter [58] have proposed a secure group membership protocol for application-level distributed systems. Also, some efficient protocols for a group key exchange have been presented (e.g., [12, 1]).

3.2.2 Security

Several researchers have proposed secure routing protocols, but none of work have been considering group membership management. For instance, Hu et al. [20] propose a secure on-demand ad hoc network routing protocol using an efficient broadcast authentication scheme, and a attacking model for routing in MANET. Buchegger and Boudec [7] present the issue of node cooperation using detection and isolation misbehaving nodes, thereby making it unattractive to deny cooperation. Capkun et al. [8] describe a fully self-organized public-key management system that allows users to generate their public-private key pairs, to issue certificates, and to perform authentication regardless of the network partitions and without any centralized services. While these research have not assumed group membership management, the individual focusing aspects are related to our work.

3.3 Problem Definitions

We try to solve the following problems on secure group membership management in MANETs.

1. **Not taking into account heterogeneous network settings and uses of MANET.**
2. **Not realizing secure and spontaneous MANET communication.**
3. **Not considering the relations between group management, routing, and addressing.**
4. **Not assuming the interoperability of proposed multiple routing protocols.**

Chapter 4

Design of Wireless Overlay Networks (WoN)

This chapter describes the detailed 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. Finally, we explain the application of WoN to ad hoc routing protocols, to allow the different routing algorithms to coexistent in the same area.

4.1 Introduction to WoN

In the face of deployment of ad hoc networking, it is necessary to consider such a situation shown in Figure 4.1. These situations could happen in the various contexts of office and home life, emergency operations, or military work. In the near future, these are likely to occur throughout the realistic environments of our daily life. 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.

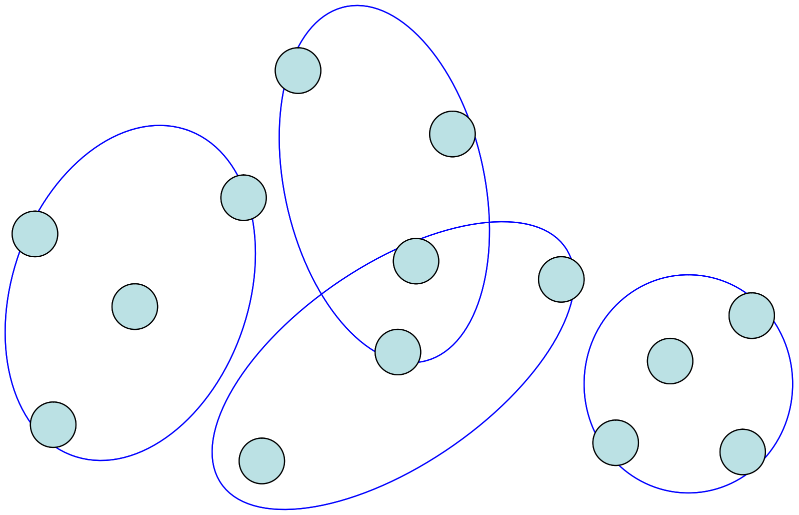


Figure 4.1: There are four ad hoc group networks close in an area; each of them may have the sharing purposes, applications, tasks, or location-dependent services.

Most of prior MANET research have focused on ad hoc routing issues and assumed a general network setting and environment. For example, all the nodes in a certain area are members of one ad hoc networks, and exploiting one particular ad hoc routing protocol. Such assumptions are justly unrealistic and inefficient. Ad hoc groups may be formed at any time, by any entity, and at any place. Also, if we set such assumptions, security and privacy problems may occur and such networks can be a complicated and resource consuming system.

In this thesis, we propose a routing-based membership management system for ubiquitous ad hoc networks, called WoN. WoN focuses on the first step to build such spontaneous networking, which involves addressing, naming, and multi-hop routing of the participants in the network. For the flash and straightforward operation, we combine the above three functions into group ID based routing system. The IDs identify and separate each group to allow multiple ad hoc networks to co-exist in the same regions. WoN also realizes secure group management and multiple routing protocol interoperabilities in ad hoc networks.

4.2 MANET Building Process

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 4.2 presents the difference of the end-node behavior when joining networks between infrastructure-based networks and ad hoc networks.

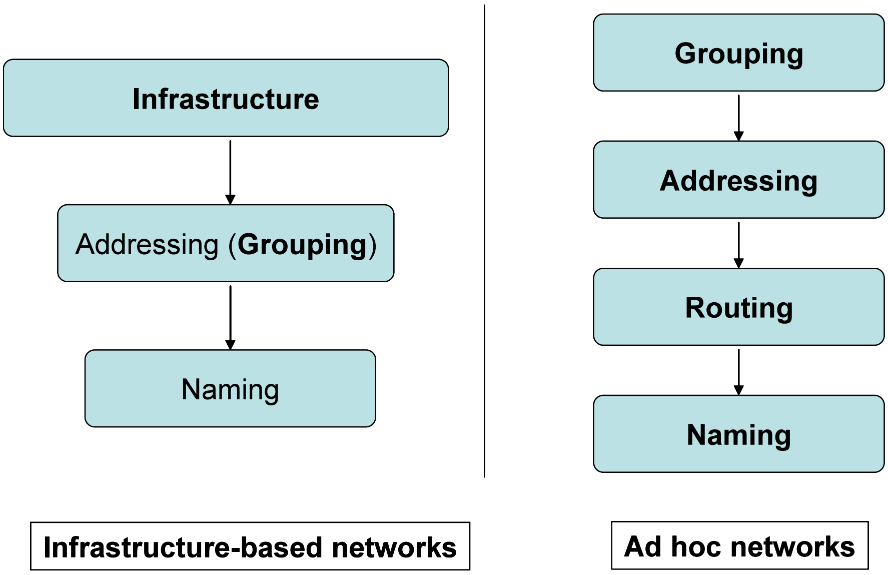


Figure 4.2: Required functions of the end-node when joining networks in infrastructure-based networks and ad hoc networks.

Although grouping functions are generally implementing at the application layers in wired networks, due to the nature of ad hoc networking, we should consider which layers those should be realized on. 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 an ad hoc network from the scratch.
- Join an ad hoc network which are already created.

When one node decides to create a MANET, it generates a group name or consensus name. Its name is inserted to WoN routing module on each node. Then, each member having that node do the broadcasting to discover the members. In the routing modules of nodes who is not in “group A”, silently discard the discovery packets.

Then, only the members of “group A” are discovered for each other. At the same time, WoN allocates the temporal IP addresses uniquely. Note that since already allocating the “group A”, it is not needed to consider the issue of convergence and partition of networks.

However, group ID could possibly be duplicated with other group (or MANET). Where we should do the encryption of messages. group ID based encryption method may be resource consuming task because encryption processes is running every receiving packets.

4.2.1 MANET ID (MID)

In MANET, the network age may be so short that the fully-featured addressing (as in Internet) is not likely and needed, rather temporal addressing may be appropriate. Thus, we take an approach such as GID (MANET ID). Also, MID approach is appropriate for user oriented computing. Basically, the decision maker to group multiple nodes or participants may be users who own the nodes (or devices, computers). This is to define the boundary of an ad hoc network.

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 4.3,4.4. The more detailed operations are described in the next chapter.

```
Loop {
    ReceivingIDfromApplication(ManetID)
    if (ManetID is not in ‘‘ManetIDList’’)
        OrigMessage = MakeMessage(ManetID, MyIPAddress,
                                           DefaultTtl, Seq);
        Message = Encrypt(ManetID, OrigMessage);
        WaitRandomTime();
        SendBroadcasting(Message);
}
```

Figure 4.3: WoN Sending Algorithm

4.3 MID-based Routing

To manage MIDs in ad hoc networks, WoN layer takes the task and interacts with IP routing protocols. Figure 4.5 shows the relations, it also presents user groups utilizing specific routing algorithms.

Since WoN is the separated layer from routing 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 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 ad hoc nodes 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.

```
Loop {
    ReceiveBroadcastingPackets(Message);
    foreach ( ManetID in ManetIDList) {
        if ( Decrypt(Message, ManetID) == true )
            if (SrcIPAddress == MyIPAddress) {
                MyIPaddress = ChangeMyIPAddress(MyIPAddress);
                Message = Encrypt(ManetID, OrigMessage);
                SendBroadcasting(Message);
            } else {
                AddMemberList(ManetID, MacAddress, SrcIPAddress);
                if (TTL >= 1)
                    Message = Encrypt(ManetID, OrigMessage);
                    SendForwardBroadcasting(Message)
                else /* TTL == 0 */
                    Message = Encrypt(ManetID, OrigMessage);
                    SendForwardBroadcasting(Message,
                                               SubnetIDofIPAddress)
            }
       else Discard(Message);
    }
}
```

Figure 4.4: WoN Receiving Algorithm

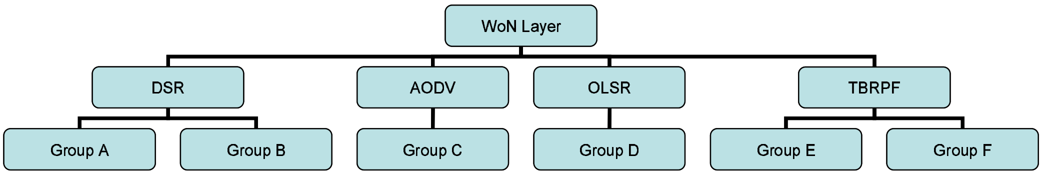


Figure 4.5: Relations between WoN Layer, IP routing protocols, and grouping.

Chapter 5

Implementation of WoN

This chapter describes the implementation of Wireless Overlay Network (WoN) architecture. In this thesis, although we do not present the evaluation results of WoN prototype implementation (we are currently working on it), we show the system architecture, and the protocol descriptions and structures of WoN components. Then, we present the descriptions of WoN simulator implementation and the implementation of the proposed two node mobility generation models.

5.1 WoN System Architecture

Figure 5.1 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 [46], 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. In this architecture, we also may need to incorporate security functions such as encrypting messages.

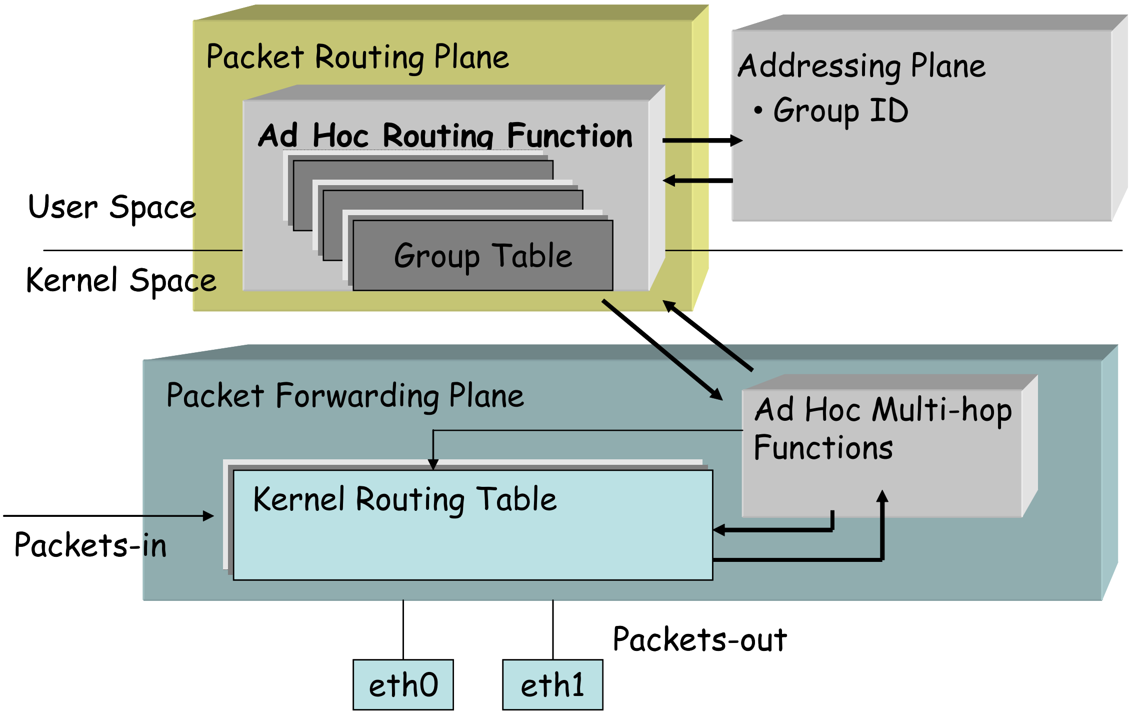


Figure 5.1: WoN system architecture

5.1.1 Sending and Receiving Components

We describe the node operation of the initialization phase to membership grouping more systematically. In the Figure 5.2 and 5.3, we assume ManetIDs are acquired through secure channels such as personal contact or location-dependent indicators. The “ManetIDList” and “MemberList” structures are described in the next subsection.

```
/* obtain ManeID from applications */
Loop {
    ReceivingIDfromApplication(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 )
            SendBroadcasting(Message);
        else
            Discard(Message);
}
```

Figure 5.2: Pseudo-code of WoN Sending Operation

In the initial step, we are not knowing each other nor setting its own IP addresses, hence, we use the global broadcast forwarding (i.e., 255.255.255.255) and use the subnet broadcasting when expiring the TTL of the global broadcasting. It is because the weakly duplicate address detection and discovering group of one MANET ID processes do complete when the TTL of the global broadcast forwarding reaches the zero. As a symmetric-key encryption scheme, we have used DES based on MANET ID.

```
/* already share ManetID through personal contact, etc */
Loop {
    ReceiveBroadcastingPackets(Message);
    foreach ( ManetID in ManetIDList) {
        if ( Decrypt(Message, ManetID) == true )
            if ( AlreadyRecvdSeq(Message, ManetID) == true)
                Discard(Message);
            Ttl = ExtractTtl(Message, ManetID);
            MacAddres = ExtractMac(Message, ManetID);
            SrcIPAddress = ExtractSrc(Message, ManetID);
            MemberList = ExtractList(Message, ManetID);
            if (SrcIPAddress == MyIPAddress) {
                /* generate accurately different number */
                MyIPaddress = ChangeMyIPAddress(MyIPAddress);
                /* arrage the difference of members */
                AddMemberList(ManetID, MacAddress, MemberList);
                OrigMessage = MakeMessage(ManetID,
                                      MyIPAddress, DefaultTtl);
                Message = Encrypt(ManetID, OrigMessage);
                SendBroadcasting(Message);
            } else {
                AddMemberList(ManetID, MacAddress, SrcIPAddress);
                if (TTL >= 1)
                    OrigMessage = MakeMessage(ManetID,
                                 MemberList+MyIPAddress, Ttl-1);
                    Message = Encrypt(ManetID, OrigMessage);
                    SendBroadcasting(Message)
                else /* TTL == 0 */
                    OrigMessage = MakeMessage(ManetID,
                            MemberList+MyIPAddress, DefaultTtl);
                    Message = Encrypt(ManetID, OrigMessage);
                    SendSubnetBroadcasting(Message,
                                           SubnetIDofIPAddress)
            }
       else Discard(Message);
    }
}
```

Figure 5.3: Pseudo-code of WoN Receiving Operation

5.1.2 MID Message Format and Structures

To search group members and formate an ad hoc network with the members, nodes having shared MANET IDs broadcast Hello messages. The messages the following format: *<ManetID, SrcID, DstID, TTL, ManetIDMemberList, Seq>*. They are encrypted using DES Cipher Block Chaining (CBC) mode which requires initialization vector.

One node can belong multiple ad hoc groups at the same time. The "ManetIDList" is maintained on each nodes of WoN as list structure and it includes MANET IDs that are currently used to build the ad hoc groups. The "MemberList" structures are also maintained on every node and consisted of several members as shown in Figure 5.4. The NumOfManetID variable is the number which included in "ManetIDList." Even if the MANET ID groups have not used longer time. the cache information should be stored on each nodes for the future use or as a member profile data.

```
struct manetMemberList {
    u_int32_t   manetid[8];
    u_int32_t   IpAddress[NumOfManetID];
    u_int8_t    MacAddress[NumOfManetID][6];
}
```

Figure 5.4: AdHocMemberList structure

5.2 Simulator Implementation

This section describes our implementation of WoN adding to DSR and AODV, and the realistic node mobility models we used in our simulations. We have ran WoN implementation in the *ns-2* network simulator environment.

5.2.1 DSR and AODV Implementation Decisions

Since the MID based member decisions of WoN are basically independent of ad hoc routing protocols, WoN have embedded into AODV and DSR protocols in a similar manner. Regarding the membership establishing function of WoN using broadcast technique, it has been incorporated in both the Route Discovery functions with simple addressing and encryption functions. Because AODV in *ns-2* is implemented as a user-land application daemon, the modifications are somewhat different than those incorporated for DSR. Though we need to implement the APIs to specify MIDs from application layer, we have used the MID specification profiles in the simulation. Considering the trade-off between security intensity and efficiency, we have chosen 256 bit-length ID space in WoN simulation.

For comparison with DSR fortified by WoN, we chose to implement WoN on AODV-LL (Link Layer) [6] using only link layer feedback from 802.11 as well as DSR, completely eliminating AODV Hello messages.

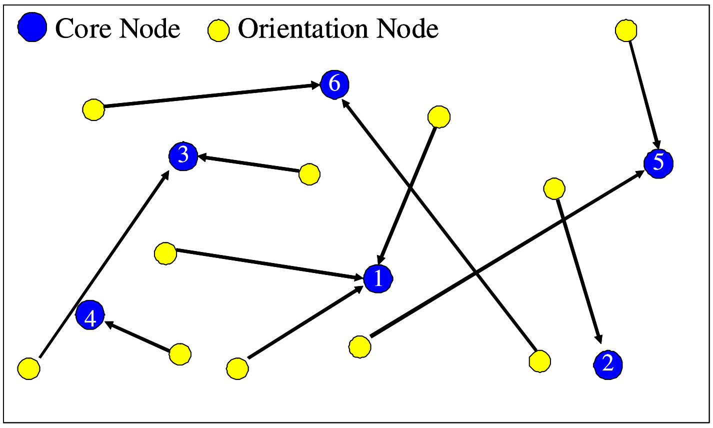
5.2.2 Realistic Node Mobility Models

To investigate how WoN scheme performs in the *realistic* node mobility pattern, we have used the two node mobility models [40]: "random orientation mobility model (ROM)" and "random escape mobility model (REM)." These models are based on the *random way-point model* [28] used in most of the previous simulation research. In the *random way-point model*, each node begins the simulation by remaining stationary for *pause time* seconds. It then selects a random destination in the specified field space and moves to the destination at a speed distributed uniformly between *0* and some maximum speed. On reaching the destination, the node pauses again for *pause* *time* seconds, selects another destination, and proceeds there as previously described, repeating this behavior for the duration of the simulation.

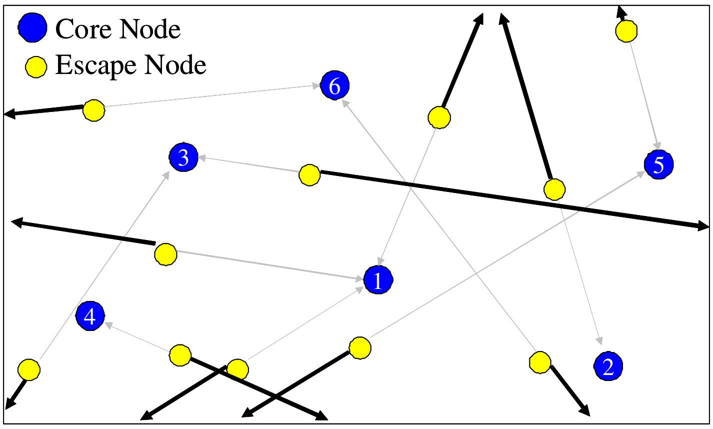
In contrast, our two node mobility model generate more realistic movement patterns. ROM is assuming people pursuing something (e.g., *peace*, *money*, *hope*) or attracted something(e.g., *gravity*, *power*). On the other hand, REM is literally assuming people are escaping from something (e.g., *disaster*, *ghost*). The movement patterns are shown in Fig. 5.5(a) and 5.5(b).

In the proposed models, mobile nodes are classified into three types: CORE_NODE (CN), ORIENTATION_NODE (ON), and ESCAPE_NODE (EN). CNS move around simulation field based on the random way-point model. On the other hand, ONS select one destination from the coordinate positions of CNS randomly instead of a perfectly random destination, and pursue the CN at a speed distributed uniformly between *0* and some maximum speed (e.g., *not all people pursue money*). If a ON reaches the selected destination, then it selects another destination among that of CNS again. This cycle continues until the end of simulation. In REM, ENS desperately try to leave from one of the CNS. ENS choose the exact opposite side of the destination position of a randomly selected CN as the destination, and move towards the destination. In this model, we assume human mobility in situations as disaster to where ad hoc networks expect to apply. Note that, when node mobility files are generated for simulation, we need to specify the ratio of ONS or ENS to CNS as one argument. If the stated ratio is 0.0, the generated node mobility pattern is accurately based on the random way-point model.

Recently, another realistic node mobility model is proposed in [26]. This model attempts to model the behavior of nodes in a realistic environment where there exits any



(a) Random orientation mobility (ROM)



(b) Random escape mobility (REM)

Figure 5.5: Examples of random orientation and escape movement

number of obstacles that obstruct data forwarding paths (e.g., buildings, vegetation). While this model is reasonable from the micro view of realistic environments, ROM and REM models are rather targetting at the macro model of human mobility. The similar approach incorporating obstacles is partly described in [27].

Chapter 6

Performance Evaluation

In this chapter, we show several simulation results of WoN. We simulate WoN on several large mobile topologies to qualify and quantify the scaling behavior and overhead of WoN in Network Simulator (ns2) [63]. To study how WoN scheme performs in *realistic* node mobility patterns, we measure the effectiveness of WoN using the proposed two practical mobility models.

6.1 Simulation Environments

6.1.1 Simulation Model

We have decided to use *ns-2* simulator in our evaluation since in the simulator the Monarch research group in CMU developed support for simulating multi-hop wireless networks complete with physical, data link and MAC layer models [6]. The distributed coordination function (DCF) of the IEEE standard 802.11 for wireless LANs is used as the MAC layer. The 802.11 DCF uses Request-to-Send (RTS) and Clear-to-Send (CTS) control packets [5] for "unicast" data transmission to a neighboring node. The radio model uses characteristics similar to a commercial radio interface, Lucent's WaveLAN [50, 65]. WaveLAN is a shared-media radio with a nominal bit-rate of 2 Mb/sec and a nominal radio range of 250 meters.

The routing protocol model handles all data packets transmitted or forwarded, and responds by invoking routing activities as appropriate. The Route Request (RREQ) packets are treated as broadcast packets in the MAC. Route Reply (RREP), Route Error (RERR) and data packets are all unicast packets with a specified neighbor as the MAC destination. DSR and AODV protocols detect link breakage using feedback from the MAC layer. A signal is sent to the routing layer when the MAC layer fails to deliver a unicast packet to the next hop. In this evaluation, no additional network layer mechanism such as *HELLO Messages* [54] is used.

Table 6.1 and 6.2 provide all the simulation parameters of both protocol extended by WoN. These parameters are remained default parameters of *ns-2* current distribution and previous salient research work for reasonable comparison.

Table 6.1: DSR Simulation Parameters

Time between retransmitted Route Requests (exponentially backed off)	500 ms
Size of source route header carrying n addresses	$4n + 4$ bytes
Timeout for non-propagating search	30 ms
Time to hold packets awaiting routes	30 s
Max rate for sending gratuitous Replys for a route	1/s

Table 6.2: AODV-LL Simulation Parameters

Time for which a route is considered active	50 sec
Lifetime on a Route Reply send by destination node	1 sec
Number of times a Route Request is retried	3
Time before a Route Request is retried	10 s
Time for which the broadcast id for a forwarded Route Request is kept	6 sec
Time for which reverse route information for a Route Reply is kept	10 sec
Time before broken link is deleted from routing table	3 sec
MAC layer link breakage detection (Hello Packets OFF)	yes

6.1.2 Traffic and mobility models

Traffic and mobility models use similar to previous published results using *ns-2* ([6], [27], [15]) for appropriate performance comparisons. Traffic sources are CBR (constant bit rate). The source and destination pairs are spread randomly over the network. Only 512 byte date 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.

The mobility model uses the *random way-point model*, our proposed random oriented model and random escape model in a rectangular area. One field configurations are used - (i) $1500m \times 300m$ field with 50 nodes. Thus, each node starts its travel from a random location with a randomly chosen speed (uniformly distributed between $0 - 20$

m/sec except in the random escape model). 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. Each data point represents an average of five runs with identical traffic models, but different randomly generated mobility scenarios. For fairness, identical mobility and traffic scenarios are used across protocols.

6.2 Evaluation Results

In this section, we present the results of our simulation comparing the performance of DSR, AODV, DSR and AODV extended by WoN. We verify the effectiveness of WoN.

6.2.1 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 6.1 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.

6.2.2 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

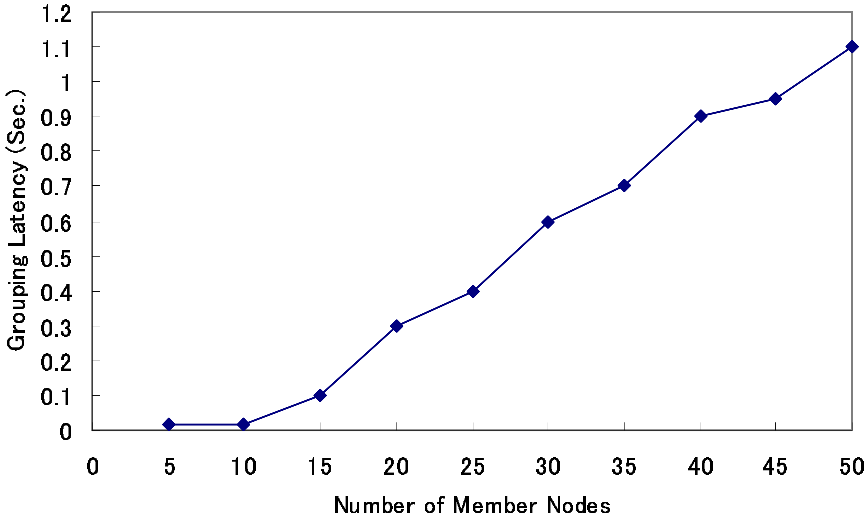


Figure 6.1: The grouping construction latency as a function of the number of group members.

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 the 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.

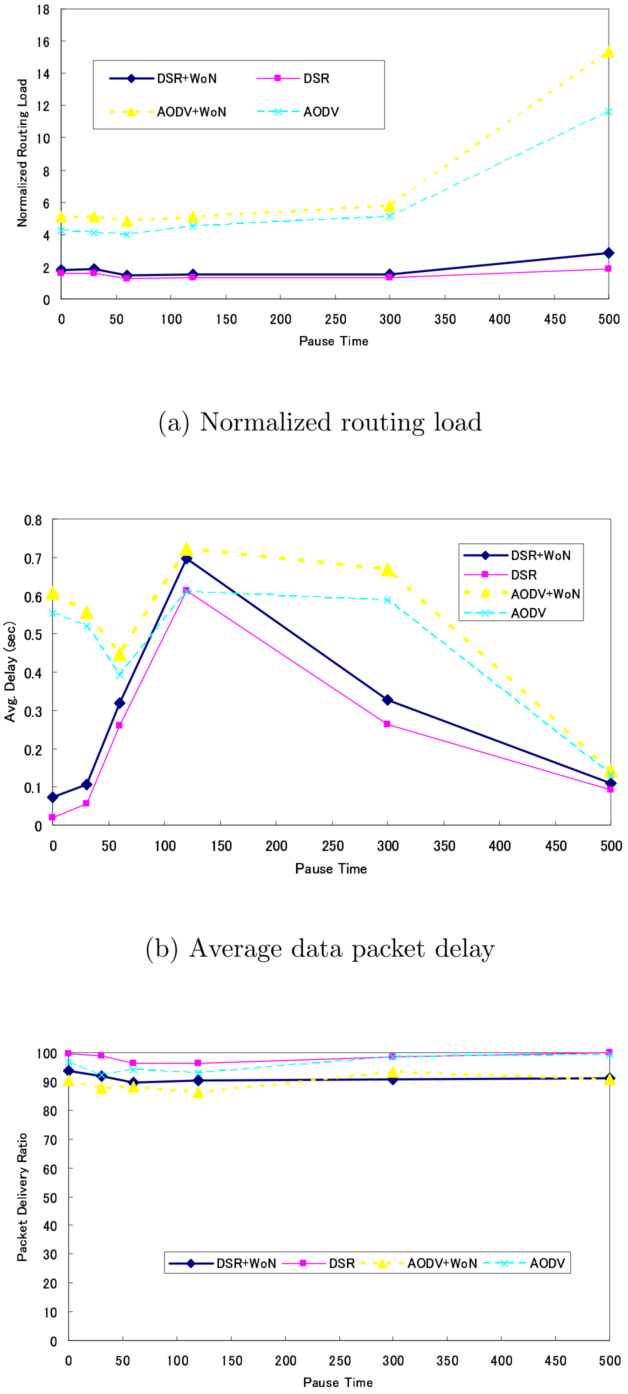
To study the performance of WoN in the realistic group node mobility, we conducted performance evaluations in the two proposed realistic node mobility. These node mobility models generate some network congestion points and network partitioning areas, respectively. These generated nodes may be some group having certain purposes.

Group Orientation Mobility

This model typically makes several network and node congestion points. Thus, we can assume the effectiveness of the active shortening in such a area. In Figure 6.2(a), 6.2(b) and 6.2(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 frequently link failure and relatively speedy node mobility. As Figure 6.3(a), 6.3(b) and 6.3(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*.

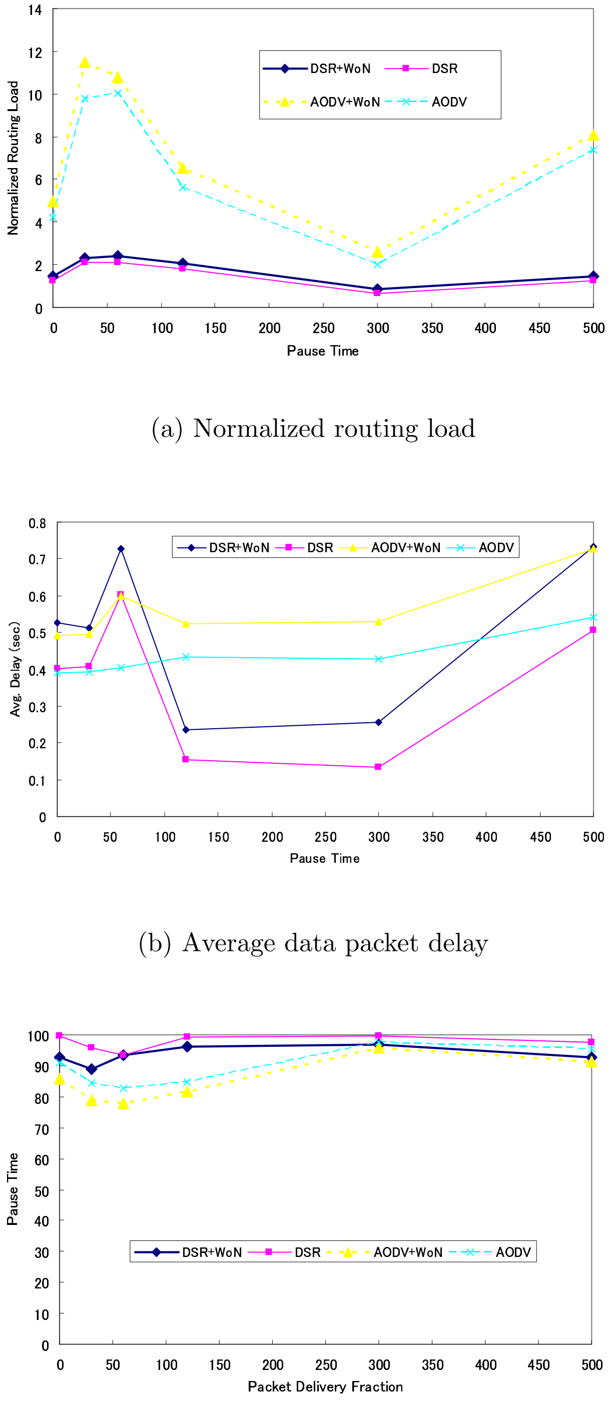


(a) Normalized routing load

(b) Average data packet delay

(c) Packet delivery fraction

Figure 6.2: Group orientation mobility model.



(a) Normalized routing load

(b) Average data packet delay

(c) Packet delivery fraction

Figure 6.3: Group escape mobility model.

Chapter 7

Conclusions and Future Work

We conclude this thesis with a summary of our contributions and directions for future work.

We have proposed a routing-based membership management system for ubiquitous ad hoc networks, called WoN. While prior ad hoc network research have mainly focused on routing problems, we have studied the first step to build ad hoc spontaneous networking, WoN have identified and separated each group to allow multiple ad hoc networks to co-exist in the same regions. WoN also realized secure group management and multiple routing protocol interoperabilities in ad hoc networks.

We are currently working on experimental implementation and evaluations of WoN, and also plan to enhance the security and robustness to allow WoN to prompt the interoperability between current MANET routing protocols.

7.1 Summary and Contributions

We have argued the several points as our contributions in this thesis.

- **Most of ad hoc network research have generally focused routing issues.**

  Most previously proposed routing protocols in mobile ad hoc networks do not take heterogeneous network settings and uses of MANET into account. They also have not consider the relations between group management, routing, and addressing, thus not realizing secure and spontaneous MANET communication nor assuming the interoperability of proposed multiple routing protocols.

- **WoN is the novel approach to ad hoc group management.**

  We proposed a routing-based membership management system for ubiquitous ad hoc networks, called WoN. WoN focuses on the first step to build such spontaneous networking, which involves addressing, naming, and multi-hop routing of the participants in the network. For the flash and straightforward operation, we combine the above three functions into group ID based routing system.

- **Prior proposed routing protocols were effectively enhanced by WoN.**

  As a case study, we have incorporated Won to conventional well-studied DSR and AODV. Although these two protocols are on-demand routing approaches, WoN architecture does not depend on specific routing algorithms.

- **WoN presented little overhead to routing protocols and good scaling behavior.**

  Simulation studies for several scenarios of node mobility and traffic flows have revealed that adding WoN to prior proposed routing protocols (DSR and AODV) produces little overhead of routing control packets and has the good scaling behavior. In addition, we have shown that MID-based routing protocols maintains the independence behavior to other routing protocols.

- **WoN realized secure group management and ad hoc routing protocol interoperabilities.**

  WoN have allowed secure group communication by encrypting messages based on MANET IDs, and allows multiple MANET routing protocols to coexistent in the same area, by conducting MID-based routing separation. The MIDs identify and separate each ad hoc group to allow co-located ad hoc networks to achieve logically and securely separated networking.

- **We evaluated WoN using the two realistic node mobility models.**

  In most previous simulation research of ad hoc networks, simulated nodes move according to the random way-point model [28]. This model generates the random movement of nodes based on a random destination and a speed distributed uniformly between 0 and some maximum speed. In order to investigate how WoN scheme performs in more *realistic* movement pattern, we utilized the two node mobility models: the "random orientation model" and "random escape model." These model generate the movement patterns assuming people pursuing something (e.g., *dreams*, *love*, *power*, etc) and escaping from something (e.g., *a fire*, *disaster*, *due date*, etc).

7.2 Future Directions

We are going to study and evaluate WoN in the various simulation environments such as high volume and high-speed node mobility networks. we also 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 Optimized Link State Routing (OLSR [13]) and Topology Dissemination Reverse Path Forwarding (TBRPF [49]) and evaluate its effectiveness. In 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. In case thinking deployment of MANET into our real life, the interoperability issue can be something that must be done. Specifically, we try to clarify the protocol behaviors and performance in the mixed routing environments, while using WoN due to the independent operations of each routing protocols.

In addition, we are now working to extend the ns2 network simulator to accurately model the physical layer behavior of the IEEE 802.11b and 802.11a wireless LAN standard [61], so that we can simulate environments of the wireless raw bandwidth from 11 Mbps (802.11b) to 54 Mbps (802.11a). Since WoN attempts to utilize broadcasting frequently, the effects of Medium Access Control and Physical Layers should be also grasped well. We may need to re-design novel MAC protocols.

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 [64] and ad hoc routing protocols. Also, the application of WoN to group management of ad hoc sensor networks should be interesting research.

Acknowledgments

First and foremost, I would like to thank my supervisor, Professor Hide Tokuda, for his technical and professional advice, thoughtful guidance, and encouragement.

I would like to thank Professor Jun Murai for his valuable supports on this thesis and be extremely thankful to Professor Yoshito Tobe and Hiroto Aida for their daily supports, and valuable advice and discussions. I also thank Mika Minematsu for helping to improve the quality of this thesis.

I am grateful to Dr. Kazu Takashio and Dr. Jin Nakazawa for their constructive supports and comments.

Finally, I thank the numerous members of Tokuda, Murai, Kusumoto, Nakamura, and Minami Laboratories, especially the members of ECN research groups for their valuable supports and stimuli.

January 14, 2004

Masato Saito

References

Published Papers Related to this Thesis

- Masato Saito, Hiroto Aida, Yoshito Tobe, and Hideyuki Tokuda
  “A Proximity-based Dynamic Path Shortening Scheme for Ubiquitous Ad Hoc Networks, ” IEEE International Conference on Distributed Computing Systems (ICDCS 2004), Mar. 2004.
- 斉藤匡人, 間博人, 徳田英幸
  “アドホックネットワークにおける動的経路短縮機構の評価, ”
  情報処理学会 マルチメディア通信と分散処理 (DPS) ワークショップ, pp. 37-42, Dec. 2003. **ベストペーパー賞**
- 斉藤匡人 “無線アドホックネットワーク, ”
  慶應義塾大学大学院 政策・メディア研究科 テクニカルレポート,
  http://www.ht.sfc.keio.ac.jp/˜masato/pub/adhoc-techreport_masato.pdf, Aug. 2003.
- Masato Saito, Hiroto Aida, Yoshito Tobe, Yosuke Tamura, and Hideyuki Tokuda
  “OR2: A Path Tuning Algorithm for Routing in Ad Hoc Networks, ”
  IEEE LCN Workshop on Wireless Local Networks (WLN ’01), pp. 560-567,
  Nov. 2001.
- Masato Saito, Hiroto Aida, Yoshito Tobe, Yosuke Tamura, and Hideyuki Tokuda
  “A Dynamic Path Shortening Scheme in Ad Hoc Networks, ”
  情報処理学会 マルチメディア通信と分散処理 (DPS) ワークショップ, pp. 169-174,

Oct. 2001. **Winner of the Best Presentation Award and the Young Researcher's Award**

- 斉藤匡人, 間博人, 田村陽介, 徳田英幸
  "モバイルアドホックネットワークにおけるTCPの性能解析, "
  情報処理学会 第62回 全国大会, Vol. 3, pp. 469-470, Oct. 2000.

Other Published Papers

- 金田裕剛, 峰松美佳, 斉藤匡人, 間博人, 徳田英幸
  "P2Pネットワークゲームのための階層型遅延最適化機構ミドルウェアの実装と評価, " 情報処理学会 第66回 全国大会, Mar. 2004.
- 青柳禎矩, 滝澤允, 斉藤匡人, 間博人, 徳田英幸
  "異種セグメント端末による分散型仮想LAN構築機構の設計と実装, " 情報処理学会 第66回 全国大会, Mar. 2004.
- Makoto Takizawa, Hiroto Aida, Masato Saito, Yoshito Tobe, and Hideyuki Tokuda
  "MaCC: Supporting Network Formation and Routing in Wireless Personal Area Networks, " The 18th International Conference on Advanced Information Networking and Applications (AINA 2004), Mar. 2004.
- 佐川昭宏, 高橋ひとみ, 斉藤匡人, 間博人, 徳田英幸
  "スイッチ間の連携による内部ネットワークセキュリティ向上機構, "
  情報処理学会 マルチメディア通信と分散処理(DPS)ワークショップ, pp. 209-214, Dec. 2003.
- Hitomi Takahashi, Masato Saito, Hiroto Aida, Yoshito Tobe, and Hideyuki Tokuda
  "Estimated-TCP-throughput Maximization based Routing, "
  IEEE Local Computer Networks (LCN '03), pp. 120-129, Oct. 2003.

- 高橋ひとみ, 斉藤匡人, 間博人, 徳田英幸
  “異種無線メディア間における経路制御機構, ” 情報処理学会 マルチメディア, 分散, 協調とモバイル (DICOMO2003) シンポジウム, pp. 601-604, Jun. 2003.
- Masaki Ito, Akiko Iwaya, Masato Saito, Kenichi Nakanishi, Kenta Matsumiya, Jin Nakazawa, Nobuhiko Nishio, Kazunori Takashio, Hideyuki Tokuda
  “Smart Furniture: Improvising Ubiquitous Hot-spot Environment, ”
  The 3rd IEEE International Workshop on Smart Appliances and Wearable Computing (IWSAWC 2003), pp. 248-253, May. 2003.
- 滝澤允, 間博人, 斉藤匡人, 戸辺義人, 徳田英幸
  “MaCC: WPAN コンフィグレーション機構, ” 情報処理学会 ユビキタスコンピューティングシステム研究会 (UBI), pp. 15-22, Apr. 2003.
- Motoi Aoki, Masato Saito, Hiroto Aida, and Hideyuki Tokuda
  “ANARCH: A Name Resolution Scheme for Mobile Ad Hoc Networks, ” The 17th International Conference on Advanced Information Networking and Applications (AINA 2003), pp. 723-730, Mar. 2003.
- 峰松美佳, 斉藤匡人, 間博人, 徳田英幸
  “Hop-Wise Limited broadcast (HoWL) for Mobile Ad hoc Networks, ” 情報処理学会 マルチメディア, 分散, 協調とモバイル (DICOMO2002) シンポジウム, pp. 421-424, Jul. 2002.
- 滝澤允, 間博人, 斉藤匡人, 戸辺義人, 徳田英幸
  “MaCC: 通信状況に応じた WPAN コンフィグレーションシステム, ” 情報処理学会 マルチメディア通信と分散処理研究会 (DPS), pp. 67-72, Nov. 2002.
- Mika Minematsu, Masato Saito, Hiroto Aida, Yoshito Tobe, and Hideyuki Tokuda
  “HoWL: An Efficient Route Discovery Scheme Using Routing History in Ad hoc Networks,” IEEE Local Computer Networks (LCN ’02), pp. 20-29, Nov. 2002.

- 青木基衣, 斉藤匡人, 間博人, 徳田英幸
  “アドホックネットワークに適した名前解決機構: RANR (ランダム割り当て名前解決機構), ” 情報処理学会 モバイルコンピューティングとワイヤレス通信研究会 (MBL), pp. 233-240, Mar. 2002.
- 高橋ひとみ, 斉藤匡人, 間博人, 徳田英幸
  “モバイルアドホックネットワークにおけるTCP転送性能を考慮した経路制御機構, ” 情報処理学会 コンピュータシステムシンポジウム, pp. 9-16, Nov. 2001.
- 高橋ひとみ, 斉藤匡人, 間博人, 徳田英幸
  “モバイルアドホックネットワークにおけるパケットロス率と遅延を考慮した経路制御機構, ” 情報処理学会 第63回 全国大会, Vol. 3, pp. 297-298, Sep. 2001.
- 峰松美佳, 斉藤匡人, 間博人, 徳田英幸
  “モバイルアドホックネットワークにおけるリミテッドブロードキャストの測定と評価, ” 情報処理学会 第63回 全国大会, Vol. 3, pp. 299-300, Sep. 2001.
- Hiroto Aida, Yoshito Tobe, Masato Saito, and Hideyuki Tokuda
  “A Software Approach to Channel-State Dependent Scheduling for Wireless LANs, ” The 4th ACM International Workshop on Wireless Mobile Multimedia (WOWMOM 2001) , pp. 34-43, Jul. 2001.

Bibliography

[1] G. Ateniese, M. Steiner, and G. Tsudik. New Multiparty Authentication Services and Key Agreement Protocols. *IEEE Journal on Selected Areas in Communications*, 18(4):628–640, Apr 2000.

[2] H. Balakrishnan. *Challenges to Reliable Data Transport over Heterogeneous Wireless Networks*. PhD thesis, University of California at Berkeley, 1998.

[3] S. Bandyopadhyay, D. Saha, S. Roy, and T. Ueda. A Network-Aware MAC and Routing Protocol for Effective Load Balancing in Ad Hoc Wireless Networks with Directional Antenna. In *Proceedings of ACM MobiHoc'03*, June 2003.

[4] E. Belding-Royer, Y. Sun, and C. Perkins. Global Connectivity for IPv4 Mobile Ad hoc Networks. IETF Internet-Draft [Work in Progress], Nov. 2001.

[5] V. Bharghavan, A. Demers, S. Schenker, and L. Zhang. MACAW: A media access protocol for wireless LAN's. In *Proceedings of ACM SIGCOMM'94*, pages 212–225, Aug. 1994.

[6] J. Broch, D. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva. A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols. In *Proceedings of ACM/IEEE MobiCom'98*, Oct. 1998.

[7] S. Buchegger and Jean-Yves Le Boudec. Performance analysis of the CONFIDANT protocol. In *Proceedings of ACM MobiHoc'02*, June 2002.

[8] S. Capkun, L. Buttyan, and J.-P. Hubaux. Self-Organized Public-Key Management for Mobile Ad Hoc Networks. *IEEE Transactions on Mobile Computing (TMC)*, 2(1):52–64, Jan-Mar 2003.

[9] W. Chan, J. Chen, P. Lin, and K. Yen. Quality-of-Service in IP Services over Bluetooth Ad-Hoc Networks. *Kluwer Academic Publishers, Mobile Networks and Applications*, 8(6):699–709, 2003.

[10] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris. Span: An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks. In *Proceedings of ACM Mobile Computing and Networking 2001*, July 2001.

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

[12] Chung Kei Wong, M. Gouda, and S. Lam. Secure Group Communications Using Key Graphs. In *Proceedings of ACM SIGCOMM'98*, pages 68–79, Sept. 1998.

[13] T. Clausen and P. Jacquet. Optimized Link State Routing Protocol (OLSR). RFC 3626, Oct. 2003.

[14] D. Couto, D. Aguayo, B. Chambers, and R. Morris. Performance of Multihop Wireless Networks: Shortest Path is Not Enough. In *Proceedings of The First Workshop on Hot Topics in Networks (HotNets-I)*, pages 167–177. ACM SIGCOMM, Oct. 2002.

[15] S. Das, C. Perkins, and E. Royer. Performance Comparison of Two On-demand Routing Protocols for Ad Hoc Networks. In *Proceedings of IEEE INFOCOM'00*, pages 3–12, Mar. 2000.

[16] H. Dubois-Ferriere, M. Grossglauser, and M. Vetterli. Age Matters: Efficient Route Discovery in Mobile Ad Hoc Networks Using Encounter Ages. In *Proceedings of ACM MobiHoc'03*, June 2003.

[17] P. Garg, R. Doshi, R. Greene, M. Baker, M. Malek, and X. Cheng. Using IEEE 802.11e MAC for QoS over Wireless. In *Proceedings of the 22nd IEEE International Performance Computing and Communications Conference (IPCCC 2003)*, Apr. 2003.

[18] M. Heusse, F. Rousseau, G. Berger-Sabbatel, and A. Duda. Performance anomaly of 802.11b. In *Proceedings of IEEE INFOCOM'03*, Mar. 2003.

[19] G. Holland, N. Vaidya, and P. Bahl. A Rate-Adaptive MAC Protocol For Wireless Networks. In *Proceedings of ACM Mobile Computing and Networking 2001*, July 2001.

[20] Y. Hu, A. Perrig, and D. Johnson. Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks. In *Proceedings of ACM MobiCom 2002*, Sept. 2002.

[21] IEEE 802.11 Standard (LAN MAN Standards Committee of the IEEE Computer Society). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications.* ANSI/IEEE Std 802.11, Aug. 1999.

[22] IEEE 802.11 Standard (LAN MAN Standards Committee of the IEEE Computer Society). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 1: High-speed Physical Layer in the 5 GHz Band.* IEEE Std 802.11a-1999, 2000.

[23] IEEE 802.11 Standard (LAN MAN Standards Committee of the IEEE Computer Society). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 2: Higher-speed Physical Layer (PHY) Extension in the 2.4 GHz Band - Corrigendum 1.* IEEE Std 802.11b-1999/Cor1-2001, 2001.

[24] IEEE 802.11 Standard (LAN MAN Standards Committee of the IEEE Computer Society). *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY)*

Specifications - Amendment 4: Futher Higher-Speed Physical Layer Extension in the 2.4 GHz Band. IEEE Std 802.11g-2003, Dec. 2003.

[25] IETF. The Internet Engineering Task Force. http://www.ietf.org.

[26] A. Jardosh, E. Belding-Royer, K. Almeroth, and S. Suri. Towards Realistic Mobility Models For Mobile Ad Hoc Networks. In *Proceedings of ACM MobiCom'03*, Sept. 2003.

[27] P. Johansson, T. Larsson, N. Hedman, and B. Mielczarek. Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks. In *Proceedings of ACM MobiCom'99*, Aug. 1999.

[28] D. Johnson and D. 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.

[29] D. Johnson, D. Maltz, and Y. Hu. The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks. IETF Internet-Draft [Work in Progress], Apr. 2003.

[30] E. Jung and N. Vaidya. A Power Control MAC Protocol for Ad Hoc Networks. In *Proceedings of ACM MobiCom 2002*, Sept. 2002.

[31] V. Kawadia, Y. Zhang, and B. Gupta. System Services for Ad-Hoc Routing: Architecture, Implementation and Experiences . In *Proceedings of The First International Conference on Mobile Systems, Applications, and Services (MobiSys 2003).* ACM SIGMOBILE and The USENIX Association, May 2003.

[32] KDDI Corporation. CDMA 1X WIN. http://www.au.kddi.com/win/, 2003.

[33] KDDI Corporation. au: Ezweb. http://www.au.kddi.com/ezweb/, 2004.

[34] Y. Ko and N. Vaidya. Location-Aided Routing (LAR) in Mobile Ad Hoc Networks. In *Proceedings of ACM MobiCom'98*, June 1998.

[35] J.-B. Lapeyrie and T. Turletti. FPQ : A Fair and Efficient Polling Algorithm with QoS Support for Bluetooth Piconet. In *Proceedings of IEEE INFOCOM'03*, Mar. 2003.

[36] Laura Marie Feeney. An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks. *Kluwer Academic Publishers, Mobile Networks and Applications*, 6(3):239–249, 2001.

[37] S. Lee, G. Ahn, X. Zhang, and A. Campbell. INSIGNIA: An IP-Based Quality of Service Framework for Mobile Ad Hoc Networks. *Journal of Parallel and Distributed Computing (Academic Press) , Special issue on Wireless and Mobile Computing and Communications*, 60(4):374–406, Apr. 2000.

[38] H. Lundgren, E. Nordstrom, and C. Tschudin. The Gray Zone Problem in IEEE 802.11b based Ad hoc Networks. *ACM SIGMOBILE Mobile Computing and Communications Review*, 6(3), July 2002.

[39] S. Maki, T. Aura, and M. Hietalahti. Robust Membership Management for Adhoc Groups. In *Proceedings of the 5th Nordic Workshop on Secure IT Systems (NORDSEC 2000)*, Oct. 2000.

[40] Masato Saito, H. Aida, Y. Tobe, and H. 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)*, Mar. 2004.

[41] MeshNetworks, Inc. MeshLAN Multi-Hop 802.11. http://www.meshnetworks.com/.

[42] Ministry of Public Management, Home Affairs, Posts and Telecommunications. 2003 WHITE PAPER Information and Communications in Japan.

http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/html/F1101300.html, 2003.

[43] Ministry of Public Management, Home Affairs, Posts and Telecommunications. 2003 WHITE PAPER Information and Communications in Japan. *http://www.johotsusintokei.soumu.go.jp/whitepaper/ja/h15/html/F1101400.html*, 2003.

[44] Mobile Ad-hoc Networks Working Group (MANET). Charter [Work in Progress]. http://www.ietf.org/html.charters/manet-charter.html, 1998-11-29.

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

[46] T. netfilter/iptables project. netfilter. http://www.netfilter.org/.

[47] NTT DoCoMo, Inc. What's New. *http://www.nttdocomo.co.jp/new/contents/03/whatnew1202.html*, 2003.

[48] NTT DoCoMo, Inc. i-mode. http://www.nttdocomo.co.jp/p_s/imode/, 2004.

[49] R. Ogier, M. Lewis, and F. Templin. Topology Dissemination Based on Reverse Path Forwarding (TBRPF). IETF Internet-Draft [Work in Progress], Oct. 2003.

[50] Orinoco, Inc. The WaveLAN Home Page. http://www.wavelan.com, 1998.

[51] Palm, Inc. Palm Hand-helds Home Page. http://www.palm.com/us/products/handhelds/, 2004.

[52] V. Park and M. Corson. A Highly Adaptive Distributed Routing Algorithm for Mobile Wireless Networks. In *Proceedings of IEEE INFOCOM'97*, pages 1405–1413, Apr. 1997.

[53] C. Perkins and P. Bhagwat. Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. In *Proceedings of ACM SIGCOMM'94*, Aug. 1994.

[54] C. Perkins, E. Royer, and S. Das. Ad Hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, July 2003.

[55] D. Qiao, S. Choi, A. Jain, and K. Shin. MiSer: An Optimal Low-Energy Transmission Strategy for IEEE 802.11 a/h. In *Proceedings of ACM MobiCom'03*, Sept. 2003.

[56] D. Qiao, S. Choi, and K. Shin. Goodput Analysis and Link Adaptation for IEEE 802.11a Wireless LANs. *IEEE Transactions on Mobile Computing (TMC)*, 1(4):278–292, Oct-Dec 2002.

[57] T. S. Rappaport. *Wireless Communications: Principles & Practice.* Prentice Hall, 1996.

[58] M. K. Reiter. A Secure Group Membership Protocol. *IEEE Transactions on Software Engineering*, 22(1):31–42, Jan 1996.

[59] Skyley Networks, Inc. Decentra. http://www.skyley.com/.

[60] J. Stewart. *BGP4: Inter-Domain Routing in the Internet.* Addison-Wesley, 1998.

[61] M. Takai, J. Martin, and R. Bagrodia. Effects of Wireless Physical Layer Modeling in Mobile Ad Hoc Networks. In *Proceedings of ACM MobiHoc'01*, Oct. 2001.

[62] The Bluetooth SIG. The official bluetooth website. http://www.bluetooth.com, 2002.

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

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

[65] B. Tuch. Development of WaveLAN, an ISM band wireless LAN. *AT&T Technical Journal*, 72(4):27–37, 1993.

[66] ultra-wideband working group. The ultra wideband working group website. http://www.uwb.org, 2003.

[67] Vodafone K.K. J-sky. http://www.vodafone.jp/, 2004.

[68] R. Wakikawa, J. Malinen, C. Perkins, A. Nilsson, and A. Tuominen. Global Connectivity for IPv6 Mobile Ad hoc Networks. IETF Internet-Draft [Work in Progress], Nov. 2001.

[69] B. Williams and T. Camp. Comparison of broadcasting techniques for mobile ad hoc networks. In *Proceedings of ACM MobiHoc'02*, June 2002.

[70] Y. Xu, J. Heidemann, and D. Estrin. Geography-informed Energy Conservation for Ad Hoc Routing. In *Proceedings of ACM Mobile Computing and Networking 2001*, July 2001.

[71] J. Yoon, M. Liu, and B. Noble. Random Waypoint Considered Harmful. In *Proceedings of IEEE INFOCOM'03*, Mar. 2003.

[72] Z. J. Hass and M. R. Pearlman. The Performance of Query Control Schemes for the Zone Routing Protocol. In *Proceedings of ACM SIGCOMM'98*, pages 167–177, Sept. 1998.

[73] B. Zhen, J. Park, and Y. Kim. Scatternet Formation of Bluetooth Ad Hoc Networks. In *Proceedings of the 36th Annual Hawaii International Conference on System Sciences (HICSS'03)*, Jan. 2003.

[74] ZigBee Alliance. Zigbee. http://www.zigbee.org/, 2003.