Securing Internet Gateway Discovery Protocol in Ubiquitous Wireless Internet Access Networks*

Bok-Nyong Park[1], Wonjun Lee[1**] and Christian Shin[2]

[1] Dept. of Computer Science and Engineering,
Korea University, Seoul, Republic of Korea
wlee@korea.ac.kr
[2] Department of Computer Science
State University of New York at Geneseo, USA

Abstract. Ubiquitous wireless Internet access networks (UWIANs) integrate mobile ad hoc networks into the Internet to achieve ubiquitous Internet connectivity. The Internet connectivity is provided by Internet gateways in the UWIANs. Most of the Internet connectivity research has not considered a malicious environment. However, UWIANs will not be able to succeed without an effective security solution due to wireless links and energy constraints. Thus, security is a critical factor to the success of ubiquitous Internet connectivity. In this paper, we propose a secure Internet gateway discovery protocol in order to provide the secure Internet connectivity. A registration mechanism is also proposed to secure a foreign network and an ad hoc mobile node when it connects within the network. The efficiency of the protocol is shown via simulation.

1 Introduction

As various wireless/mobile networks evolve into the next generation, we need a new network technology that provides better services. In order to realize the next generation network, we introduce a ubiquitous wireless Internet access network (UWIAN) that is a mobile ad hoc network (MANET) integrated with the Internet. Ubiquitous wireless Internet access networks consist of Internet gateways (IGs) and ad hoc mobile nodes (AMNs) interconnected by multihop path. These characteristics can provide flexibility and scalability. In the area of integration with Internet and MANET, IGs may be deployed in order to provide the Internet connectivity. An Internet gateway acting as a bridge between a wired network and a MANET can provide ubiquitous Internet connectivity for AMNs. Thus, the Internet gateway discovery is an important research issue in the UWIAN.

Most of the research so far has focused on efficiency with security being given a lower priority [5]. Existing schemes are carried out in a trusted environment in which all nodes are honest. Without adequate security, however, unauthorized

* This work was supported by grant No. R01-2005-000-10267-0 from the Korea Science and Engineering Foundation in the Ministry of Science and Technology.
** Corresponding Author.

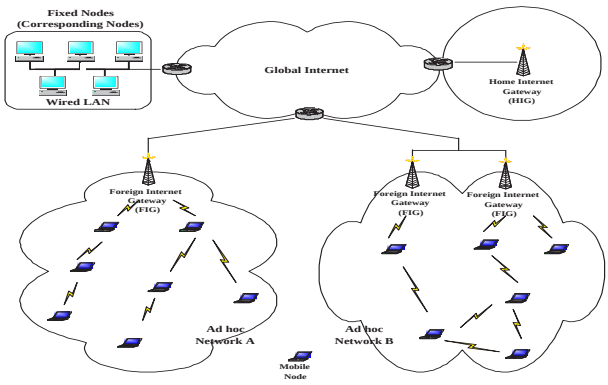

Fig. 1. System Architecture for ubiquitous wireless Internet access networks.

access and usage may violate the Internet connectivity. The nature of broadcasts in wireless networks potentially results in more security exposures. The physical medium of communication is inherently insecure. In general, attacks on the Internet connectivity are caused by malicious nodes that modify, drop or generate messages related to mobile IP such as advertisement, registration request or reply that disrupt the ubiquitous Internet connectivity. Hence, security mechanisms for the secure Internet connectivity are needed. In order to support the secure Internet connectivity, we propose a secure Internet gateway discovery (SDP) protocol for ubiquitous wireless Internet access networks. In the secure IG discovery process, an AMN first registers its public/private key pair to a home Internet gateway, and then the AMN finds paths to an IG in a foreign domain. After the AMN finds an optimal path to the IG, it registers to the foreign IG. The Internet gateways serve as a distributed trust entity. The secure IG discovery protocol uses the modified ISMANET protocol [2] that utilizes identity-based signcryption with a paring over an elliptic curve [8].

The rest of this paper is organized as follows. Section 2 provides an overview of the ubiquitous wireless Internet access networks. Section 3 proposes a secure Internet gateway discovery protocol. In Sections 4 we present our performance evaluation and our analysis of the efficiency and safety of the proposed protocol, respectively. Finally, we draw out our conclusions in Section 5.

2 Ubiquitous Wireless Internet Access Networks

Mobile ad hoc networks (MANETs) allow users to establish low-cost, limited coverage networks for the purpose of sharing data among devices. They can be used to extend the coverage of WLANs or cellular networks. An Internet gateway (IG) in ubiquitous wireless Internet access networks (UWIANs) provides Internet connectivity for ad hoc mobile nodes (AMNs), and enables ubiquitous Internet services. AMNs are typically connected to the Internet via IGs. The IG is part of both ad hoc networks and the Internet, and acts as a bridge between

the two networks. Packets from an AMN are forwarded first to an IG that further transmits them to their destination within the Internet. The IG is equipped with both interfaces: wired interface for the Internet and radio interface for ad hoc networks. Thus, IGs run ad hoc routing protocols in order to act as an AMN, and it simultaneously operates as a member of a fixed subnet connected to the Internet. Fig. 1 illustrates an example of the UWIAN architecture. The IG provides ubiquitous Internet connectivity to mobile users without having to rewire or change hardware interfaces. AMNs within ad hoc networks communicate with each other and with the IG via multihop paths.

When an AMN wants to connect to the Internet, it can connect to an Internet gateway. Key issues for supporting Internet connectivity include the IG discovery and selection. A number of research have proposed IG discovery mechanisms based on proactive, reactive, and hybrid approaches [7, 10–12]. In the proactive approach, IGs broadcast periodic advertise messages during a time interval that are flooded through the whole. Thus, the proactive scheme costs more overhead, but it allows good connectivity with low delay because it instantly knows better paths to IGs. On the contrary, the reactive approach incurs fewer overhead than the proactive approach because AMNs request IG information by sending out request messages only when necessary. However, whenever there is a need for sending a packet, AMNs must find IGs if the IGs are not already known. This IG discovery process may cause considerable delay. As a result, it causes longer delay and lower ratio of packet delivery. The hybrid approach combines the proactive and reactive approaches, reaping the best of both schemes: good connectivity and low delay. After discovering multiple relay routes, AMNs select the best IG to communicate with Internet hosts outside the ad hoc networks. An AMN needs to consider several metrics when selecting an optimal IG that maximizes the network performance among the available IGs.

3 Secure Ubiquitous Internet Connectivity

In this section, we propose a secure Internet gateway discovery protocol (SDP) for ubiquitous wireless Internet access networks, and discuss authentication method for secure registration.

3.1 Basic Operations

Ubiquitous wireless Internet access networks (UWIANs) consist of ad hoc mobile nodes (AMNs) and Internet gateways (IGs). Each AMN shares a security association (SA) with an IG within its own home network. For example, An AMN always shares a trust relationship with its home Internet gateway (HIG) even when it moves to a foreign domain. We assume that authorization information is always handled by a foreign IG (FIG) in the visited network. Most likely, the authorization information is obtained originally from an HIG in AMN's home networks. The secure IG discovery process for the UWIAN includes three phases: i) the initialization phase, ii) secure discovery phase, and iii) registration with

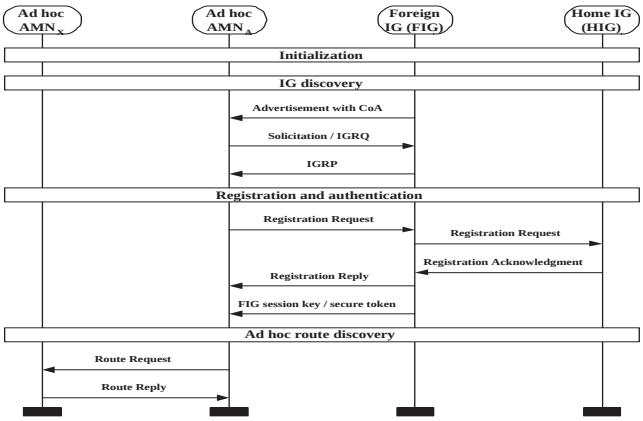

Fig. 2. Sequence diagram for the secure ubiquitous Internet connectivity.

Table 1. Notations used for the Proposed Protocol

Symbol	Definition	Symbol	Definition
ID_X	Identification of node X	$H(m)$	One-way hash function
SK^*	System master key	SK_X, PK_X	Private key and public key of X
t	Secure token	K	Shared secret key
$\hat{e}(P,Q)$	Bilinear map based on the Weil	P, P_{pub}	Generator, Master secret key $\cdot$ P

FIG phase. Before an AMN gains its successful mobile IP registration and a secret key from a FIG, it cannot participate in ad hoc routing protocol. After the AMN registers with the FIG successfully, the FIG issues a secret key to the AMN. Meanwhile the FIG is responsible for verifying AMNs' information at the request of an AMN. Each AMN shares a system master key with its HIG and a secret key with its FIG for the calculation and validation of a secure token which uses Message Authentication Code (MAC). Table 1 lists the notations used for the development of the proposed protocol. The sequence diagram in Fig. 2 illustrates the basic process of the secure connectivity in the UWIAN. In the following sections, each step is discussed in detail.

3.2 Initialization

Initialization phase is the operation that an AMN must complete before it can connect to the network. Initialization through HIG registration takes place between an AMN and its home Internet gateway. After the HIG registration process, each AMN and its HIG share a security association to create a secure token for the IG discovery and registration. The secure token is computed as follows:

$$t = (H(ID_{AMN} \parallel SK^*))$$

1.	FIG -> broadcast:	$IGAM \parallel ID_{FIG} \parallel Sig_{FIG}\{H(IGAM \parallel ID_{FIG} \parallel t_{FIG})\}$
2.	AMNs -> AMNx:	$IGRQ \parallel ID_{AMN_S} \parallel t \parallel Sig_{AMN_S}\{H(IGRQ \parallel ID_{AMN_S} \parallel t)\}$
3.	AMNs -> FIG:	$IGRQ \parallel ID_{AMN_S} \parallel ID_{AMN_X} \parallel t \parallel t_X \parallel Sig_{AMN_S}\{H(IGRQ \parallel ID_{AMN_S} \parallel t)\}$
4.	FIG -> AMNx:	$IGRP \parallel ID_{FIG} \parallel t \parallel t_{FIG} \parallel Sig_{FIG}\{H(IGRP \parallel ID_{FIG} \parallel t \parallel t_{FIG})\}$
5.	AMNx -> AMNs:	$IGRP \parallel ID_{FIG} \parallel ID_{AMN_X} \parallel t \parallel t_{FIG} \parallel t_{AMN_X} \parallel Sig_{FIG}\{H(IGRP \parallel ID_{FIG} \parallel t \parallel t_{FIG})\}$

Fig. 3. Secure IG discovery protocol.

HIGs act as an authentication server for AMNs by sharing security association between the HIG and AMN or FIG. Key establishment among participations uses the ECDH key exchange. The ECDH [8] key exchange allows two entities to exchange keys on an unsecured communication path.

3.3 Secure Internet Gateway Discovery

Before the FIG discovery, an AMN establishes public-private keys with a HIG (PK_{AMN}, SK_{AMN}). The AMN starts route discovery to a FIG. In the secure discovery protocol, we follow the ISMANET protocol [2] which uses identity-based signcryption to discover IG, and all intermediate nodes must be registered. Fig. 3 shows the process of the secure IG discovery.

IGs periodically announce their presence in an ad hoc network by broadcasting Internet Gateway Advertisement Messages (IGAMs) containing their state information and authentication information at every periodic interval:

$$< IGAM \parallel ID_{FIG} \parallel Sig_{FIG}\{H(IGAM \parallel ID_{FIG} \parallel t_{FIG})\} >$$

where t_{FIG} is $H(ID_{FIG} \parallel SK^*)$ which FIG's secure token, and IGAM is including FIG's address, sequence number, CoA, etc. To prevent flooding the network, these advertisements are limited within n-hop neighborhood using a time-to-live (TTL) field. This range determines the FIG's discovery scope, called a proactive area. In [3], we proposed a load-adaptive Internet gateway discovery (LAID) scheme which dynamically adjusts the range of proactive IG advertisements. The proposed discovery protocol is based on the LAID. AMN_S within the proactive area of x hops receive the periodic IGAM messages from IGs. If they are out of range, the AMN_S broadcast Internet Gateway Request messages (IGRQ). The AMN_S chooses a random number r, and computes $k = \hat{e}(P, P_{pub})^r$ for the message's origin. The AMN_S sends IGRQ, a secure token, and created values, all of which are signed. The signature Sig is defined as follows: Sig=*Signcrypt*(*security parameters, private key, message*). Notice that signing does not involve any pairing calculations and thus it can be done very quickly even on low-end processors.

When an intermediate node $\mathrm{AMN_X}$ receives the IGRQ, the $\mathrm{AMN_X}$ first verifies the signature of source node, and then the node computes $k' = \hat{e}(P, SK_{AMN_S}) \cdot \hat{e}(P_{pub}, PK_{AMN_S})^r$ for the message's origin and checks $t = H(ID_{AMN_S} \parallel SK^*)$ for the validity of sender node. The verification of signature is defined as follows: *valid=Unsigncrypt(Sig, public key, security parameters, message)*. *Valid* is a binary value that is set to 0 if the signature is invalid and to 1 if the signature is valid. If the confirmation is successful, the $\mathrm{AMN_S}$ and the $\mathrm{AMN_X}$ will trust each other and this process completes successfully. After authentication, the intermediate node computes t_{AMN_X} using the same method above with its ID_{AMN_X} and the system master key. Finally, the node broadcasts the message to the next nodes. When the FIG receives the message, it verifies the signature and computes t and t_{AMN_X}. If the authentication is successful, the FIG is ready to reply a message. Otherwise, packet is dropped. Then, $\mathrm{AMN_X}$ inside the proactive area of a FIG responds with Internet Gateway Response messages (IGRP) to the soliciting AMN or relays the IGRQ to IGs. Upon receipt of IGRQ messages, IGs send an IGRP message which contains the IGs' prefix and other authentication information back to the soliciting AMN. The computation method of the authentication information in the discovery reply follows the similar say in IGRQ. When the $\mathrm{AMN_S}$ receives the IGRP packet with a message for authentication, it verifies authentication information returned by the FIG as well as the FIG's signature. If the verification of the digital signature and the secure token is successful, the secure route to FIG can be established over the channel. An AMN collects all IGAM messages sent from the available IGs in the foreign network. From these IGAM messages, the AMN can obtain information for each FIG (e.g. the hop count, network load, and security association). Using the IG information, the AMN makes an available FIG list and registers to an FIG with optimal metric. The secure token is introduced for a preliminary check in order to start the registration request without having to wait for re-authentication and re-authorization results from the HIG.

3.4 Secure Registration

When an AMN sends a registration request to a new FIG in a foreign network, it includes the system master key in the secure token so that the FIG can check this master key distributed from the HIG through the secure token. This operation begins with AMN broadcasting the registration request. The FIG checks the security information of the AMN and decides whether to forward the signaling message. If this simple check is passed, the FIG regards the AMN as a registered and credible node and starts its registration process. Before an AMN gains its successful registration from a FIG, it cannot participate in ad hoc routing protocol. Upon successfully registration, the AMN will obtain the FIG information such as ID_{FIG}, shared secrets, etc. from the FIG, and set the FIG to be its default IG.

3.5 Secure Ad Hoc Route Discovery

On receiving an ad hoc route discovery message from a neighbor, an AMN checks the neighbor's ID. Then the AMN computes the secure token by using the extracted ID and the system master key to verify neighbor nodes. After the verification is successful, the AMN checks the signature of the route message by using the neighbor's public key. If the signature is matched, it shows that the neighbor is a certified node. Otherwise the neighbor with its ID is invalid, and the received packet must be discarded during the processing of ad hoc route discovery. The secure ad hoc route discovery is based on the ISMANET [2].

4 Performance Evaluation

The goal of the simulation is to evaluate the effects of integration of the secure discovery protocol into load-aware IG discovery (LAID) scheme [3]. In this section, we show the simulation results of the secure discovery protocol.

4.1 Simulation Setup

We used the ns-2 simulator [9] for our evaluation. The LAID protocol [3] is used as a benchmark to study the performance evaluation of the proposed secure discovery protocol. The radio model uses characteristics similar to a commercial radio interface, Lucent's WaveLAN [4]. WaveLAN is a shared-media radio with a nominal bit-rate of 2Mb/sec and a nominal radio range of 250 meters. The number of source-destination pairs and packet sending rate varies for modeling different network loads. As a mobility model, we used the random waypoint model in rectangular field with 700m×700m where a node starts its journey from a random location to a random destination with a randomly chosen speed. Each node moves at a speed is 10 m/s. Seven different pause times were used: 0, 10, 50, 100, 200, 400, and 800 seconds. Constant Bit Rate (CBR) traffic sources are used with different packet generation rates. The data packet size is 512 bytes. The set of experiments uses differing numbers of sources with a moderate packet rate and varying pause times. For the 50 node experiments, we used 5 and 20 traffic sources and a packet rate of 4 packets/s. We simulated some simple scenarios by varying pause times in order to see the throughput in 900 second simulation time. We varied the pause time where high pause time means low mobility and small pause time means high mobility. The IG is placed in the middle of the grid [i.e., coordinate (350, 350)] for the simulation scenarios. To manage AMNs' mobility between ad hoc networks, AMNs as well as IGs run MIP [6], where MIP FA and HA are hosted in the IG.

4.2 Simulation Results

To compare IG discovery approaches, a set of simulations has been performed in terms of three metrics: packet delivery ratio, end-to-end delay, and normalized routing overhead. Various mobility and offered load scenarios have been

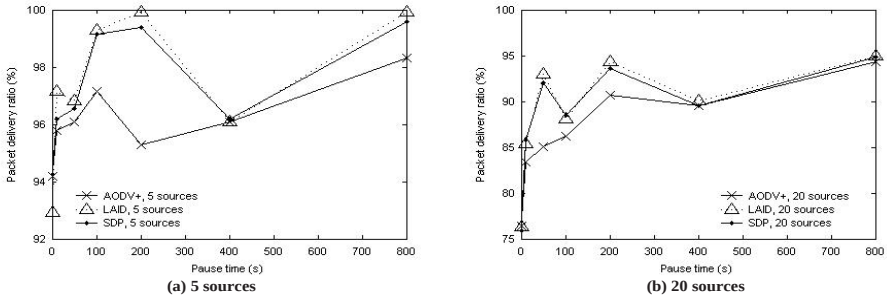

Fig. 4. Packet delivery ratio (%) for the 50-node model with various numbers of sources.

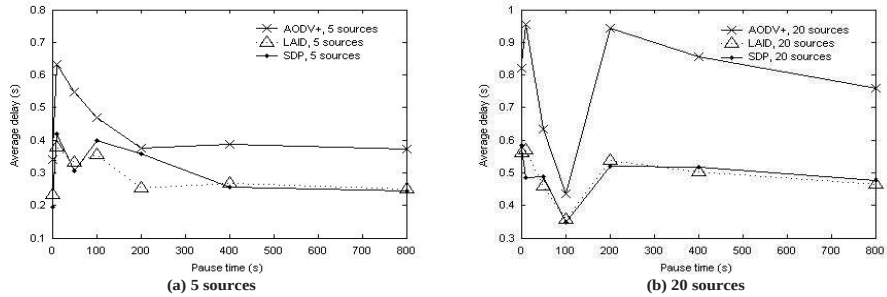

Fig. 5. Average data packet delays for the 50-node model with various numbers of sources.

simulated to understand their effects. We conducted the simulations to compare the existing Internet gateway discovery protocols without any security method to the proposed secure IG discovery protocol (SDP). Figs 4, 5, and 6 show the simulation results for the hybrid Internet gateway discovery (AODV+) [1], load-aware Internet gateway discovery (LAID), and the proposed secure IG discovery protocol (SDP). The goal of our study is to illustrate that our scheme works effectively in addressing many security issues with routing protocols without causing any substantial degradation in the network performance.

In Fig. 4, the results show that our SDP protocol works well because the effect of throughput of the network is small around 2-10%. The packet delivery ratios for LAID and SDP are very similar with 5 and 20 sources. However, if other realistic scenarios, such as disaster scenarios, battlefield scenario, or very high-speed scenarios, use our scheme, the effect of network throughput may be reduced even more. Fig. 5 shows the effect of different mobility on the average end-to-end delay. The average data packet delays are fairly low both with authentication (SDP) and without authentication (LAID) extension. SDP and LAID have similar delays with 5 and 20 sources. There is a small increase with 5 sources (Fig. 5(a)) due to the exchange of packets during the authentication

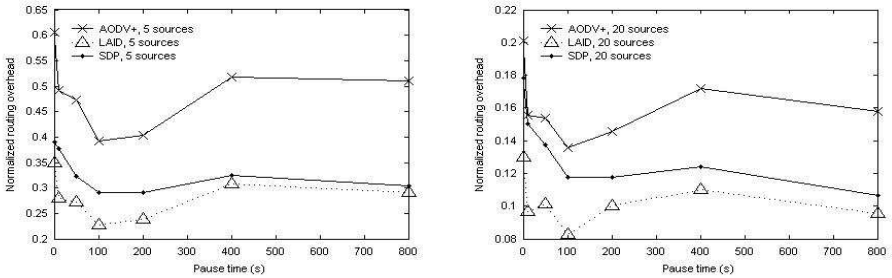

Fig. 6. Normalized routing overheads for the 50-node model with various numbers of sources.

phase of security process. In Fig. 6, the normalized overhead of the SDP is significantly larger than that of the LAID. The number of routing packets increases when our scheme is incorporated. The increase in routing load is higher at lower pause time (Fig. 6). This is because routes need to be found more frequently at lower pause time. The normalized routing overheads of the LAID and the SDP are fairly stable with an increasing number of sources. A relatively stable normalized routing load is a desirable property for the scalability of the protocols, since this indicates that the actual routing load increases linearly with the number of sources. Simulation results have shown that the SDP gives a lower average delay and normalized routing overhead than AODV+ because our SDP uses LAID as the basic discovery protocol.

4.3 Safety Analysis

Security includes the protection of the information and the resources from both inside and outside of a network. The FIG discovery process establishes a secure path between a FIG and an AMN by using authenticated nodes. It avoids those unregistered malicious nodes that mislead route or drop registration-related messages with the intention of hindering the AMN registration. The proposed discovery protocol can authenticate all nodes of routes with a secure token t. The t is computed by the system master key. Each node can verify the ID and the secure token of each node so that malicious nodes cannot hide their identity. In addition, the malicious nodes cannot fabricate the messages since they don't know the secret key of the message signed by the source. As a result, the proposed protocol is safe from fabrication attacks. Similarly, it can provide robust protection from modification. When they modify the IGAM, IGRQ, or IGRP packets, they cannot generate the correct hash value since they do not know the security parameters. By sharing a secret key between an AMN and a FIG in order to calculate a secure token, registration messages are protected from modification. Because of a shared secret key a malicious node could not register successfully with a FIG even if it can masquerade itself with a bogus CoA.

5 Conclusions

In the ubiquitous wireless Internet access network (UWIAN), security is a primary research challenge. In the UWIAN system, AMNs can access the Internet via IGs which serve distributed entities. In this paper we have proposed a secure IG discovery protocol as well as authentication method for registration in order to protect the Internet connectivity. The protocol have been developed to authenticate an ad hoc mobile node and to distribute the shared secret key. In order to secure both the foreign IG and the AMN, they mutually authenticate each other with the help of the home IG. The secure discovery protocol avoids unregistered malicious nodes and provide the secure Internet connectivity.

References

1. AODV+: "The Network Simulator: Contributed Code". *http://www.isi.edu/nsnam/ns/ns-contributed.html.*
2. B. Park and W. Lee, "ISMANET: A Secure Routing Protocol using Identity-based Signcryption Scheme for Mobile Ad-hoc Networks," IEICE Transaction on Communications, Vol. E88-B, No. 6, June 2005.
3. B. Park, W. Lee, C. Lee, J. Hong, and J. Kim, "LAID: Load-Adaptive Internet Gateway Discovery for Ubiquitous Wireless Internet Access Networks," Proceedings of the International Conference on Information Networking (ICOIN) 2006. January 2006.
4. B. Tuch, "Development of WaveLAN, and ISM Band Wirelees LAN," AT&T Tech. H. Vol. 82, no. 4, pp. 27-33, July/Aug 1993.
5. B. Xie and A. Kumar, "A Framework for Integrated Internet and Ad hoc Network Security," Proceedings of International Symposium on Computer Communication, pp. 318-324, Egypt, June 2004.
6. C. E. Perkins, "IP Mobility Support," RFC 3311 in IETF, August 2002.
7. E. M. Belding-Royer, Y. Sun, and C. E. Perkins, "Global Connectivity for IPv4 Mobile Ad-hoc Network," IETF Internet-Draft, draft-royer-manet-globlav4-00.txt, November 2001.
8. J. Lopez and R. Dahab, "Performance of Elliptic Curve Cryptosystems," Technical Report IC-00-08, 2000.
9. K. Fall and K. Varadhan, Eds., "ns Notes and Documentation," 2003; available from *http://www.isi.edu/nanam/ns/.*
10. P. Ratanchandani and R. Kravets, "A hybrid approach to Internet connectivity for mobile ad hoc networks," Proceedings of IEEE Wireless Communications and Networking Conference (WCNC) 2003, March 2003.
11. R. Wakikawa, J. T. Maline, C. E. Perkins, A. Nilsson, and A. H. Tuominen, "Global Connectivity for IPv6 Mobile Ad-hoc Networks," IETF Internet-Draft, draft-wakikawa-manet-gflobalv6-03.txt, October 2003.
12. U. Jonsson, F. Alriksson, T. Larsson, P. Johnasson, and G. Q. Maguire, "MIP-MANET: Mobile IP for Mobile Ad-hoc Network," Proceedings of the First Annual Workshop on Mobile Ad Hoc Networking & Computing (MobiHoc), Auguest 2000.