International Journal of Distributed Sensor Networks, 3: 105–117, 2007

ISSN: 1550-1329 print/1550-1477 online
DOI: 10.1080/15501320601069846

Taylor & Francis
Taylor & Francis Group

Anonymous Routing for Mobile Wireless Ad Hoc Networks

ARJAN DURRESI and VAMSI PARUCHURI

Department of Computer Science, Louisiana State University, USA

MIMOZA DURRESI and LEONARD BAROLLI

Faculty of Information Engineering, Fukuoka Institute of Technology, Japan

Wireless Mobile Ad Hoc Networks are particularly vulnerable due to their fundamental characteristics such as an open medium, dynamic topology, distributed cooperation, and constrained capability. Location information of nodes can be critical in wireless ad hoc networks, especially in those deployed for military purposes. In this paper, we present two Protocols for anonymous routing to prevent location disclosure attacks. The Protocol for Anonymous Routing (PAR) guarantees absolute anonymity, which itself might cause problems as it would become hard to identify malicious and misbehaving nodes. PAR-Enhanced trades off some anonymity to enable detection of malicious and misbehaving nodes.

Keywords Location Disclosure Protection; Anonymity; Security; Ad Hoc Networks

1. Introduction

Recent wireless research indicates that wireless Mobile Ad Hoc Networks (MANET) present a larger security problem than conventional wired and wireless networks [1,2]. In the traditional Internet, routers within the central parts of the network are owned by a few well-known operators and are therefore assumed to be somewhat trustworthy. This assumption no longer holds in an Ad Hoc network, since all nodes entering the network are expected to take part in routing. Also, because the links are usually wireless, any security that was gained because of the difficulty of tapping into the network is lost. Furthermore, because the topology in such a network can be highly dynamic, traditional routing protocols can no longer be used. Thus, Ad Hoc network has much harder security requirements than the traditional network and the routing in Ad Hoc networks is an especially hard task to accomplish securely, robustly, and efficiently.

In general, the wireless MANET is particularly vulnerable due to its fundamental characteristics of open medium, dynamic topology, absence of central authorities, distributed cooperation, and constrained capability. The existing security solutions for wired networks cannot be applied directly in wireless MANETs.

Applications that make use of ad hoc routing have heterogeneous security requirements. *Authentication*, *message integrity*, and *non-repudiation* to an ad hoc environment

Address correspondence to Arjan Durresi, Dept of Computer Science, Louisiana State University, Baton Rouge, LA 70803, USA. E-mail: durresi@csc.lsu.edu

are part of a minimal security policy. Apart from these, there are several other security issues [1, 3] such as *black hole attacks, denial of service*, and *information disclosure*.

A location disclosure attack can reveal something about the locations of nodes or the structure of the network. The information gained might reveal as to which other nodes are adjacent to the target, or the physical location of a node. In the end, the attacker knows which nodes are situated on the route to the target node. If the locations of some of the intermediary nodes are known, one can gain information about the location of the target as well.

In many cases, the location information might be very crucial. In MANETs installed for tactical/military missions in a hostile and/or unknown territory, these types of attacks have to be prevented. In many cases, the communicating nodes need to be anonymous—no other node in the network should know who is communicating with whom. Initially, we present a solution that achieves complete anonymity and discuss trade-offs between complete anonymity and difficulty in identifying misbehaving nodes. We then present enhancements to our protocol to prevent these attacks albeit at the cost of complete anonymity.

2. Goals

2.1 Anonymity

There are three types of anonymous communication properties that can be provided: sender anonymity, receiver anonymity, and unlinkability of sender and receiver [21, 22]. *Sender anonymity* means that the identity of the party which sent a message is hidden, while its receiver (and the message itself) might not be. *Receiver anonymity* similarly means that the identity of the receiver is hidden. *Unlinkability of the sender and the receiver* means that though the sender and receiver can each be identified as participating in some communication, they cannot be identified as communicating *with each other*.

We also specify two degrees of anonymity—*absolute* and *quasi-absolute*. For simplicity, we describe these with respect to sender anonymity, but they can be extended to receiver anonymity and unlinkability as well. With *absolute privacy*, the attacker can in no way distinguish the situations in which a potential sender/receiver actually sent/received communication and those in which it did not. That is, sending a message results in no observable effects for the attacker. The identity and the location of each node in the network remain anonymous and the sender and the receiver are unlinkable. In case of *quasi-absolute privacy*, the neighboring nodes of the sender would be able to identify it, when it instantiates a connection and each node in the path of an established connection knows its next and previous hop neighbors' identities. Nonetheless, the receiver remains anonymous* and the sender and receiver remain unlinkable unless all the nodes in the path collaborate.

It might be impossible to conceal the location itself—upon receiving a packet from a neighbor, as a node can easily approximate the location of the neighbor by measuring the received signal strength [29] and angle of arrival [28]. But, here we focus on making it impossible for a node to make a correspondence between the locations and the identities of the nodes. Thus, even though a node is able to figure out that some node is present at a particular location, it would not be able to find out the identity of that node.

*The node that is a neighbor of the receiver and that is also in the path of the established connection, knows the identity of the receiver, but it would not be able to distinguish the receiver from any other next hop node.

2.2 What We Achieve

Initially, we present the Protocol for Anonymous Routing (PAR), based on public key cryptography, to provide absolute anonymity. With this we achieve complete sender and receiver anonymity. Also, the sender and the receiver cannot be linked to each other even if all the nodes in the established path collaborate. However, with absolute anonymity, defending against denial-of-service attacks by compromised nodes becomes very difficult. We discuss this issue in more detail in section 2.3. Hence, to detect and defend against these attacks, we present PAR-Enhanced, a variation of the above protocol, which only provides quasi-absolute anonymity as discussed in section 5.

We consider the anonymity properties provided to an individual node against two distinct types of attackers:

- A *local eavesdropper* is an attacker who is also the neighbor of the sender/receiver and hence, can observe all (and only) communication to and from the sender/receiver.
- *Collaborating nodes* are *other* nodes that can pool their information.

The security offered by PAR and PAR-E against each of these attackers is summarized in Table 1 and justified in the rest of this paper. In this table, LE-S denotes *local eavesdropper of the sender* and LE-R denotes *local eavesdropper of the receiver*. Also, it should be noted that Table 1 consists of collaborating nodes and does not consist of local eavesdroppers. Of course, against an attacker who is comprised of both of the attackers described above, the protocol yields degrees of sender and receiver anonymity that are the minimum provided against the attackers present. For example, if a LE-S and a LE-R collaborate in an attack, then the protocol achieves neither sender anonymity nor receiver anonymity.

2.3 What We Do Not Achieve

Our objective is to provide anonymity for the sender and the receiver. In MANETs deployed specifically for military and tactical reasons, the identity and location information of the sender and the receiver might be critical. With absolute anonymity, the identities of every node in the network are completely anonymous. But, absolute anonymity makes it difficult, if not impossible, to detect misbehaving and compromised nodes in the network. A malicious node can refuse to forward packets or may just inject unnecessary packets into the network thus resulting in denial-of-service. Even intrusion detection systems [18, 19, 20] will be of little use. For networks where absolute anonymity is not as critical as in military networks, we can trade absolute anonymity a little so as to make detection of misbehaving nodes easy.

The protocol PAR that we present for achieving absolute anonymity makes no effort to defend against denial-of-service attacks. We believe that such attacks are inherent to networks where nodes are completely anonymous. But, with PAR-E, which provides quasi-absolute anonymity, intrusion detection systems [18, 19, 20] can be used with little or no modifications to detect misbehaving nodes.

3. Related Work

Ad hoc wireless networks assume that no pre-deployed infrastructure is available for routing packets end-to-end in a network, and instead rely on intermediary peers. Securing ad hoc routing presents challenges because each user brings to the network their own mobile

TABLE 1 Anonymous properties provided by PAR and PAR-E

	PAR			PAR-E		
Attacker	Sender Anonymity	Receiver Anonymity	Unlinkablity	Sender Anonymity	Receiver Anonymity	Unlinkablity
Local eavesdropper	Absolute privacy	Absolute privacy	Absolute privacy	Exposed to LE-S	Exposed to LE-R	Absolute privacy
Collaborating nodes	Absolute privacy	Absolute privacy	Absolute privacy	Absolute privacy	Absolute privacy	Absolute privacy

unit, without the centralized policy or control of a traditional network. Many ad hoc routing protocols such as Dynamic Source Routing (DSR), Ad Hoc On Demand Distance Vector (AODV), Zone Routing Protocol (ZRP), and Location Aided Routing (LAR) have been proposed previously, but none of the proposals have defined security requirements, and all inherently trust all participants.

All proposed protocols have security vulnerabilities and exposures that easily allow for routing attacks. These vulnerabilities are common to many protocols. The fundamental differences between ad hoc networks and standard IP networks necessitate the development of new security services. In particular, the measures proposed for IPSec [7] help only in end-to-end authentication and security between two network entities that already have routing between them; IPSec does not secure the routing protocol. While mechanisms similar to those used in IPSec can be adapted to secure the routing, IPSec alone does not suffice.

This point has been recognized, and others have started to examine security problems in ad hoc networks. A solution that uses threshold cryptography as a mechanism for providing security to the network is presented in [8]. A method that ensures equal participation among members of the ad hoc group, and that gives each node the authority to issue certificates is presented in [9]. An effort to secure an existing ad hoc routing protocol has also recently been made available [10].

Apart from the above protocols, which try to deal with minimal security requirements like Authentication, message integrity, and non-repudiation, several other protocols were presented to deal with specific security issues encountered in MANETs. [4] presents the resurrecting duckling security policy model, which describes secure transient association of a device with multiple serialized owners. [5] presents a solution to prevent black hole attacks, [6] presents strategies for intrusion detection.

Anonymous communication for wired networks is a well-studied aspect. The concept of a mix is introduced in [23]. A single processor in the network, called a mix, serves as a relay. Each processor P that wants to send a message m to a processor Q encrypts m using Q's public key to obtain m'. Then P encrypts the pair (m', q) using the public key of the mix. The mix decrypts the message and forward m' to q. This scheme has been extended in [24, 25, 26] where several mixes are used to cope with the possibility of compromising the single mix. Another approach is to interpose an additional party (an anonymizer [27]) between the sender and receiver to hide sender's identity from the receiver. Both the approaches are not viable in an ad hoc network for several reasons. First, they are based on the assumption that the information of mixes is known a priori and hence, the sender can select the mixes appropriate to the receiver. This assumption is impractical in an ad hoc network. Second, the mixes/anonymizers are entrusted with more responsibility and they can become single points of attack. Third, forwarding a packet through mixes/anonymizers results in much longer paths than the shortest paths possible, thus resulting in inefficient utilization of resources.

We address one routing attack that could easily happen in MANETs, the information disclosure problem. Specifically, we deal with the attack in which a malicious node may leak location information of other nodes.

4. Protocol for Anonymous Routing

In this section, we present a protocol to achieve absolute anonymity—the identities of the source and destinations are not known to any other node; after a connection is established, a node involved in the path does not even know its adjacent nodes in the path. Instead of containing source and destination information, packets moving along an anonymous connection contain only obscure information about next hop and previous hop.

4.1 Notation and Definitions

Public and Private Keys. We assume the presence of a Public Key Infrastructure. We denote the private and public keys of a node i as E_i and D_i. We denote the E(M, k) and D(M, k) to denote the encryption and decryption of message M with key k.

A Hash function, H, is assumed to be used globally; i.e., every node is aware of H and uses H to get the hash values.

Invisible Address (IA_i). We would also like to define the *invisible address* (IA_i) of a node i for a packet with a *flow identifier* FID is constructed by encrypting the address along with FID first with the private key of i and then, with the public key of i.

$$IA_i = \mathrm{E}(\mathrm{E}((i, \mathrm{FID},\ \mathrm{timestamp},\ \mathrm{RP}), \mathrm{E}_i), \mathrm{D}_i)$$

where RP is the redundancy predicate. Node N to have its invisible address get verified, just presents m=E((i, FID, timestamp, RIP), E_i) to the verifier. For the message to be verified successfully the unencrypted message D(m, D_i) must fulfill the redundancy predicate and E(m, D_i) must be same as IA_i.

Routing Flow Table. Each node maintains a *routing flow table* (RFT), through which it is able to forward a packet to the next node in the path. The information stored in each entry of the table is:

- Flow Identifier (FID) set to the unique request identifier present in the route request.
- Invisible Previous node Address (IPA) set to the invisible address of the node from which the route request is received.
- Invisible Next node Address (INA) set to the invisible address of the node from which the route received is received (if at all received).
- Timer (T) initialized upon the reception of a non-duplicate route request to *Th**. The entry is deleted if a route reply is not received before the timer expires.

We also assume that the network is very loosely synchronized. This assumption is just to prevent replay attacks.

4.2 Route Requests

Whenever a node S wishes to communicate with a node D, it initiates the route discovery process. Route discovery allows any node in the ad hoc network to dynamically discover a route to any other node in the ad hoc network, whether directly reachable within wireless transmission range or reachable through one or more intermediate network hops through other nodes. A node initiating a route discovery broadcasts a route request, which may be received by those nodes within wireless transmission range of it.

The route request has the following fields:

- FID (U*nique request identifier*, also referred to as *unique flow identifier*) is set by the source by encrypting its address (S), destination address (D) and a locally

*This time *Th* depends on the diameter of the network and could be set to the maximum Round Trip Time that could be possible in the network between any two nodes.

maintained sequence number (SEQ) with the public key of S. This is used to detect duplicate *route requests* received at an intermediate node.

$$\text{FID} = \text{E}((\text{S},\ \text{D},\ \text{SEQ}),\ \text{D}_\text{s})$$

- ESA (Encrypted Source Address) is constructed by encrypting source address, hash of FID, timestamp and the Redundancy Predicate (RP) with the destination's public key. The hash of FID and the timestamp are to prevent replay attacks.

$$\text{ESA} = \text{E}((\text{S},\text{H}(\text{FID}),\ \text{timestamp},\ \text{RP}),\ \text{D}_\text{D})$$

- EDA (Encrypted Destination Address) is constructed by encrypting destination address, hash of FID, timestamp and the Redundancy Predicate (RP) with destination public key.

$$\text{EDA} = \text{E}((\text{D},\ \text{H}(\text{FID}),\ \text{timestamp},\ \text{RP}),\ \text{D}_\text{D})$$

- ITA (Invisible Transmitter Address) is the invisible address of the node *i* transmitting the route request.

$$ITA = \text{E}(\ \text{E}((i,\ \text{FID},\ \text{timestamp},\ \text{RP}),\ \text{E}_i),\text{D}_i)$$

Whenever a node *i that is not the destination* receives a non-duplicate* route request packet, it performs the following operations:

RQ1. A new entry is added to the routing flow table with FID and IPA fields set to FID and ITA values of the route request packet.†
RQ2. The node checks if the route request is intended for it by decrypting the EDA with its private key E_i and if it is the case it proceeds to send a route reply (described below) and steps 3 and 4 are not executed.
RQ3. The timer is initiated
RQ4. Invisible address is computed for the packet and the route request is retransmitted with its ITA set to the invisible address computed.

4.3 Route Replies

The destination after receiving the route request also adds a new entry to its RFT in a similar manner as above. The destination also validates the source by decrypting ESA with E_i. Then, the destination in order to establish a connection, constructs a route reply packet with the following fields:

- FID is set to the FID of the route request.
- ESA (Encrypted Source Address) is constructed by encrypting D (destination of route request), hash of FID, timestamp and the Redundancy Predicate (RP) with the

*Only FID is considered in deciding if a route request is a duplicate or not.
†INA field is set only when a corresponding route reply packet is received.

source's public key. The hash of FID and the timestamp are to prevent replay attacks.

$$ESA = E((D, H(FID), timestamp, RP), D_s)$$

- EDA (Encrypted Destination Address) is constructed by encrypting S (source of route request), hash of FID, timestamp, and the Redundancy Predicate (RP) with the source's public key.

$$EDA = E((D, H(FID), timestamp, RP), D_s)$$

- ITA (Invisible Transmitter Address) is the invisible address of the node *i* transmitting the route request.

$$ITA = E(E((i, FID, timestamp, RP), E_i), D_i)$$

- IFA (Invisible Forwarder Address) is initially set to the ITA of the corresponding route request packet.

Whenever a node *i* that is not the source, receives a route reply packet, it performs the following operations:

RP1. An entry corresponding to FID is searched for in the RFT. If no entry is found, the packet is dropped and all further steps are skipped.
RP2. The IFA value is verified by checking for RP, its address, FID and the timestamp in D(D(IFA, D_i), E_i). If the verification fails, the packet is dropped and all further steps are skipped.
RP3. The INA value of the entry corresponding to FID in RFT is set to ITA of the route reply and the timer of the corresponding entry is nullified.
RP4. The INA value of the route reply packet is set to the ITA value of the entry corresponding to FID and ITA value of the route reply is set to the invisible address of *i*. The route reply is then forwarded.

When the source receives the route reply, it can verify the destination address by decrypting the ESA and EDA fields in the route reply with its private key. After the verification, the source and destination can securely communicate with each other.

It should be noted that, no node in the network could make out the source or the destination of any packet/connection. Also, each node in the network does not even know the address of its neighboring node to which it is forwarding the packet. Thus, communication that is completely anonymous can be achieved. Also, apart from the overhead imposed due to the implementation of public key infrastructure, no extra overhead is imposed by our protocol. It should also be noted that, for each new connection, the route request is flooded over the whole network. So, instead of pure flooding, flooding protocols like distance based flooding [15], gossip based flooding [16] can be used. These flooding algorithms, depending on network size and other parameters, require 30% to 60% lesser number of retransmissions than pure flooding.

5. Enhanced Protocol for Anonymous Routing (PAR-E)

With PAR, a malicious node can misuse the complete anonymity gained by transmitting fake routing requests. A misbehaving node, which drops the packets instead of retransmitting

packets, can also go undetected. It is always a trade off between privacy and security. We propose a few enhancements to detect malicious and misbehaving nodes, albeit at the cost of complete anonymity.

With the enhancements, a node will know the identity of any of its neighbors only if those two nodes lie on the same path of some connection. For instance, consider two neighboring nodes A and B. A will know the identity of B only if A and B lie in the path of some connection. If no such connection exists, then A does not know B and vice versa.

5.1 Diffie-Hellman Key Exchange Algorithm

The Diffie-Hellman protocol was the first public key algorithm ever invented [17, 12]. Diffie-Hellman can also be used for key distribution—two nodes A and B can use this to generate a secret key. We briefly present the protocol here. For further details we refer the reader to [17, 12].

First, A and B agree on a large prime, n and g, such that g is primitive mod n. These two integers do not have to be secret; they can even be common among a group of users. Then, the protocol is as follows:

(i) A chooses a large integer x and sends B

$$X = g^x \bmod n$$

(ii) B chooses a random large integer y and sends Alice

$$X = g^x \bmod n$$

(iii) A computes $k = Y^x \bmod n$
(iv) B computes $k' = X^y \bmod n$

Both k and k' are equal to $g^{xy} \bmod n$. No one listening on the channel can compute that value, unless they can compute the discrete logarithm and recover x or y. So, k is secret key that A and B computed independently.

We assume that all the nodes are aware of some symmetric key encryption algorithm and all nodes use the same symmetric key encryption algorithm. We denote the symmetric encryption and decryption processes of a message M with key k as $E_s(M, k)$ and $D_s(M, k)$.

5.2 Enhancements

Routing flow table: Five new fields are added to each entry of RFT

- n, a large prime chosen by the source.
- g, such that g is primitive mod n.
- x, a large integer chosen for each entry by the node maintaining the RFT.
- PPK (Previous node Partial Key) set to the partial key of the node from which the route request is received.
- NPK (Next node Partial Key) set to the partial key of the node from which the route reply is received (if at all received).

Route Request. Three new fields are added to the route request packet

- n, a large prime chosen by the source.
- g, such that g is primitive mod n.

- TPK, Transmitter partial key, computed and set by the transmitter as

$$TPK = g^x \bmod n$$

Route reply. Five new fields are added to the route reply packet

- n, large prime chosen by S, the source of the route request.
- g, such that g is primitive mod n and chosen by S, the source of the route request.
- NPK, next node partial key set by the transmitter.
- TV, Transmitter Verifier, set to the cipher text obtained by encrypting the transmitter's address and its signature* with SK as key. SK is computed using PPK and x as $SK=(PPK^x \bmod n)$

$$TV = E_s((\text{Transmitter address}, \text{signature}^*), SK)$$

- TV', Previous Transmitter Verifier, set to the cipher text obtained by encrypting the transmitter's address and its signature* with SK' as key. SK' is computed using NPK and x as $SK=(NPK^x \bmod n)$

$$TV' = E_s((\text{Transmitter address}, \text{signature}^*), SK')$$

Initially, the source node S chooses a large prime, n and g, such that g is primitive mod n and initializes the corresponding fields in the route request to these. Any other node, that is not the destination, upon reception of a route request, apart from steps RQ1 – RQ4 (Section IVB), performs an additional step RQ3a.

RQ3a. The node chooses a large integer x and sets the field x in the newly created entry to that integer. Set the PPK field in the RFT entry to TPK of the route request and reset the TPK entry of route request to $g^x \bmod n$.

The destination D upon receiving the route request creates a new entry in its RFT and sets its fields to the corresponding fields of the route request. It then generates a large integer x and computes the shared key according to the Diffie-Hellman key Exchange algorithm as follows:

$$SK = TPK^x \bmod n$$

Then, D constructs the route reply as explained in section IVC with the new fields set in the following way:

- n, set to the large prime present in the route request.
- g, set to g present in the route request.
- NPK, next node partial key, set to $(g^x \bmod n)$, x being a large integer, chosen by D.
- SK, shared key, is calculated as $SK=(TPK^x \bmod n)$, TPK being transmitter partial key obtained from the route request.
- TV, Transmitter Verifier, set to the cipher text obtained by encrypting the transmitter's address and its signature with SK as key.

$$TV = E_s((D, \text{signature}), SK)$$

- -TV', Transmitter Verifier

*The signature can be constructed by encrypting the node address, hash of the packet with the node's private key.

A node *i*, that is not the source, upon reception of a route reply, apart from steps RP1 – RP4 (section 4C), performs an additional step RP3a:

RP3a. The node computes the shared keys, SK and SK' as (NPK^x mod n) and (PPK^x mod n), *x* being the value in the RFT entry corresponding to FID. Using SK, TV is verified by decrypting it with the SK. Upon verification, it sets NPK field of route reply to (g^x mod n), *x* taken from RFT entry. Using TPK from the RFT entry, the node calculates SK=(TPK^x mod n) and resets the Transmitter Verifier in the route reply to TV=E_s((*i*, signature), SK). It then retransmits the route reply.

Also, after retransmitting the route reply, then node *i* overhears* the route reply its neighbor retransmits for TV' and verifies the signature. In case of a node next to source, the source explicitly transmits TV' for the node to verify its identity.

When the source receives the route reply, it verifies the destination address by decrypting the ESA and EDA fields in the route reply with its private key. Thus, a secure communication channel between the source and the destination is established. It should be observed that each node in the path established knows nothing more than the identities of its neighboring nodes in the path established. The identities of even other neighboring nodes are revealed.

As each node knows the identity of its neighboring nodes in the paths established, the Intrusion Detection Systems like [18, 19, 20] can be implemented successfully to detect malicious and misbehaving routers.

6. Conclusion

In this paper we presented protocols for achieving anonymous routing in mobile ad hoc networks and thus, prevent location disclosure attacks. The protocol for Anonymous Routing (PAR) guarantees absolute anonymity, which itself might cause problems as it would become difficult to identify malicious and misbehaving nodes. PAR-Enhanced trades off some anonymity to enable detection of malicious and misbehaving nodes.

About the Authors

Arjan Durresi received the BE, MS, and Ph.D. (all summa cum laude) all in Electronic-Telecommunications, in 1986, 1991, and 1993, respectively and a Diploma of Superior Specialization in Telecommunications from La Sapienza University in Rome, Italy and Italian Telecommunications Institute in 1991. From 1991 to 1995, he served as a senior software analyst at Telesoft S.p.A, Rome, Italy. From 1995 to 1996, he was a faculty member in the Department of Electronics and Vice Dean of Electrical Faculty at Polytechnic University of Tirana. From 1996 to 2003, he was a research scientist at the Department of Computer and Information Science in the Ohio State University. In 2003, he joined Louisiana State University, where he is currently an assistant professor in the Department of Computer Science. His current research interests include network architectures, heterogeneous wireless networks, security, QoS routing protocols, traffic management, optical and satellite networks, multimedia networking, performance testing, and bioinformatics.

Dr. Durresi has published more than forty articles in journals and seventy articles in proceedings of refereed international conference. He is an area editor for the Ad Hoc Networks Journal (Elsevier) and guest editor for the International Journal of Wireless and Mobile Computing and the International Journal of Distributed Sensor Networks. He was

*In case of an ideal channel, overhearing can be assumed. But, in case this cannot be assumed, then the nodes explicitly transmit TV' to be verified by the next node in the path.

Co-Chair and Founder of the First International Workshop in Heterogeneous Wireless Sensor Networks HWISE'2005, Program Co-Chair of AINA2006, Program Vice Chair of AINA2004 and ICPADS 2005, and Program Area Chair of AINA2005. He is the recipient of the Lumley Research Award from Ohio State University in 2002. He received the appreciation certificate from IEEE Computer Society in 2005. He is a senior member of the IEEE.

Vamsi K Paruchuri received the BTech degree in electronics and communications engineering from Sri Venkateswara University, Tirupati, India, in 2001 and the MS degree in electrical engineering from Ohio State University, Columbus, OH, USA, in 2003. He is currently a PhD candidate in computer science at Louisiana State University, Baton Rouge LA, USA. His research interests include routing and security protocol design, analysis, and implementation for wireless networks. He is a student member of the IEEE.

Mimoza Durresi received the BE, in Electronic-Telecommunications in 1989, and a Diploma of Superior Specialization in Telecommunications from La Sapienza University in Rome, Italy and the Italian Telecommunications Institute in 1991. She received the MS in Electric Computer Engineering in 2002 from Ohio State University. Since 2003 she has been teaching at Franklin University. Her research interests are in wireless networking, inter vehicle communications and routing. She is working toward her Ph.D. degree at Fukuoka Institute of Technology.

Leonard Barolli received the B.E. and Ph.D. degrees from Tirana University and Yamagata University in 1989 and 1997, respectively. From April 1997 to March 1999, he was a JSPS Post Doctoral Fellow Researcher at the Department of Electrical and Information Engineering, Yamagata University. From April 1999 to March 2002, he worked as a Research Associate at the Department of Public Policy and Social Studies, Yamagata University. From April 2002 to March 2003, he was an Assistant Professor at the Department of Computer Science, Saitama Institute of Technology (SIT). From April 2003 to March 2005, he was an Associate Professor and presently is a Professor at Department of Information and Communication Engineering, Fukuoka Institute of Technology (FIT). Dr. Barolli has published more than 100 papers in refereed Journals and International Conference proceedings. He was an Editor of the IPSJ Journal and has served as a Guest Editor for many International Journals. Dr. Barolli has been a PC Member of many International Conferences. He was the PC Chair of IEEE AINA-2004, IEEE ICPADS-2005, MNSA-2005, and NBiS-2005. He is Genral Co-Chair of IEEE AINA-2006 and MNSA-2006. His research interests include network protocols, Internet applications, wireless networks, agent-based systems, distance learning, network traffic control, fuzzy control, genetic algorithms, sensor networks, and ad-hoc networks. He is a member of SOFT, IPSJ, IEEE Computer Society, and IEEE. Dr. Barolli have received may research awards and funded research grants. He received an appreciation certificate from the IEEE Computer Society in 2004 and 2005.

References

1. Vesa Karpijoki. Security in Ad hoc Networks. In *Proceedings of the Helsinki University of Technology, Seminars on Network Security*, Helsinki, Finland, 2000. http://ntrg.cs.tcd.ie/htewari/papers/netsec00_manet_sec. pdf
2. L. Zhou and Z. J. Haas. "Securing Ad Hoc Networks," *IEEE Network Magazine*, **13**, 6, 24–30, November/December 1999.
3. Janne Lundberg. Routing Security in Ad Hoc Networks. http://citeseer.nj.nec.com/400961.html
4. F. Stajano and R.J. Anderson. The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks. *Proc. Seventh Security Protocols Workshop, Lecture Notes in Computer Science 1796*, Springer-Verlag, Berlin, 2000, 172–182.

5. H. Deng, W. Li, D. Agrawal. "Routing Security in Wireless Ad Hoc Networks," *IEEE Communications Magazine*, Oct. 2002, 70–75.
6. Lakshmi Venkatraman and Dharma P. Agrawal. "Startegies for Enhancing Routing Security in Protocols for Mobile Ad hoc Networks," *JPDC Special Issue on Mobile Ad Hoc Networking and Computing*, accepted for publication.
7. C. R. Davis. *IPSec: Securing VPNs*. McGraw-Hill, New York, 2000.
8. L. Zhou and J. Haas. "Securing Ad Hoc Networks," *IEEE Network*, **13,** 6, 24–30, 1999.
9. J. P. HuBaux, L. Buttyan, and S. Capkun. The Quest for Security in Mobile Ad Hoc Networks. In *Proc. ACM MobiHoc*, October 2001.
10. S. Yi, P. Naldurg, and R. Kravets. Security-aware ad hoc routing for wireless networks. *Technical Report UIUCDCS-R-2001- 2241, UILU-ENG-2001–1748*, University of Illinois at Urbana-Champaign, August 2001.
11. ([PKIX])Public-Key Infrastructure (X.509). IETF Working Group http://www.ietf.org/html.charters/pkix-charter.html
12. B. Schneir. *Applied Cryptography*. John Wiley & Sons, Inc., New York, 1996.
13. David B. Johnson, Davis A. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks," *IETF Draft*, 49 pages, October 1999.
14. C.E. Perkins and E.M.Royer, Ad-hoc On Demand Distance Vector Routing, *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, LA, February 1999, p 90–100.
15. S. Y. Ni et al. "The Broadcast Storm Problem in a Mobile Ad Hoc Network," *ACM MOBICOM*, 151–162, Aug. 1999.
16. Haas, Halpern, Li. "Gossip Based Ad Hoc Routing," In *IEEE INFOCOM*, June 2002.
17. W. Diffie and M.E. Hellman. "New Directions in Cryptography," *IEEE Transactions on Information Theory*, **IT-22**, 6, Nov 1976, 644–654.
18. Oleg Kachirski, Ratan Guha. "Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks," IEEE Workshop on Knowledge Media Networking.
19. R. Ramanujan, S. Kudige, T. Nguyen, S. Takkella, and F. Adelstein. "Intrusion-Resistant Ad Hoc Wireless Networks," *Proceedings of MILCOM 2002*, Oct. 2002.
20. Yongguang Zhang & Wenke Lee. "Intrusion Detection in Wireless Ad-Hoc Networks," *Proceedings of The Sixth International Conference on Mobile Computing and Networking*, Boston, MA, August 2000.
21. Pfitzmann, A. and Waidner, M. "Networks Without User Observability," *Computer Security*, **6**, 2, 1987 158–166.
22. M. K. Reiter and A. D. Rubin. "Crowds: Anonymity for Web Transactions," *ACM Transactions on Information and System Security*, **1**, 1, pp. 66–92, 1998.
23. D. Chaum. "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms," *Communication of the ACM*, **24**, 2, pp. 84–88, 1981.
24. A. Pfitzmann, B. Pfitzmann, and M. Waidner. "ISDN-MIXes – Untraceable Communication with Very Small Bandwidth Overhead. In *Proc. Kommunikation in Verteilten Systemen*, 451–463, 1991.
25. C. Rackoff and D. Simon. "Cryptographic Defense Against Traffic Analysis." In *Proc. of the 25th Annual. ACM Symp. on the Theory of Computing*, 672– 681, 1993.
26. P. F. Syverson, D. M. Goldsclag, and M. G. Reed. "Anonymous connections and onion routing," In *Proc. of IEEE Symposium on Security and Privacy*, 44–54, 1997.
27. Anonymizer – Online Privacy and Security. www.anonymizer.com
28. D. Niculescu and B. Nath. "Ad Hoc Positioning (APS) using AoA, in Proceedings of INFOCOM." 2003, San Francisco, CA, 30 March-3 April 2003.
29. P. Bahl and V. N. Padmanabhan. "RADAR: An In-Building RF-Based User Location and Tracking System." in *Proceedings of the IEEE INFOCOM 2000*, Tel Aviv, Israel March 2000.