Available online at www.sciencedirect.com
SCIENCE DIRECT
Fuzzy Sets and Systems 157 (2006) 1704–1712
FUZZY sets and systems
www.elsevier.com/locate/fss

An adaptive fuzzy logic based secure routing protocol in mobile ad hoc networks☆

Jing Nie*, Jiangchua Wen, Ji Luo, Xin He, Zheng Zhou

Wireless Network Lab, Beijing University of Posts and Telecommunications, 5 Beijing, China

Received 25 May 2005; received in revised form 17 October 2005; accepted 6 December 2005
Available online 9 January 2006

Abstract

In ad hoc networks, designing a secure routing protocol is critical. The FLSL (Fuzzy Logic Based Security-Level Routing Protocol) routing protocol is proposed in this paper. The basic idea of FLSL is to utilize the "local multicast" mechanism and the Security-Level to select the highest Security-Level route. The proposed algorithm of Security-Level is an adaptive fuzzy logic based algorithm that can adapt itself with the dynamic conditions of mobile hosts. Simulations show that the FLSL routing protocol can improve security of mobile ad hoc networks. The FLSL routing protocol is feasible to the weak security character of MANETs (mobile ad hoc networks).

Keywords: Fuzzy numbers; Analysis; Fuzzy system model; Routing; Security

1. Introduction

Ad hoc [7] is a kind of special wireless network mode. A MANET (mobile ad hoc network) is a collection of two or more devices equipped with wireless communications and networking capability. Such devices can communicate with another device that is immediately within their radio range or one that is outside their radio range not relying on access point. A mobile ad hoc network is self-organizing, self-discipline and self-adaptive. The main characteristics of mobile ad hoc network are:

- Dynamic topology. Since nodes in the network can move arbitrarily, the topology of the network also changes.
- The bandwidth of the link is constrained and the capacity of the network is also variable tremendously. Because of the dynamic topology, the output of each relay node will vary with the time and then the link capacity will change with the link change.
- Power limitation in mobile devices is a serious factor. Because of the mobility characteristic of the network, devices use battery as their power supply. As a result, the advanced power conservation techniques are very necessary in designing a system.
- The security is limited in physical aspect. The mobile network is easier to be attacked than the fixed network. Overcoming the weakness in security and the new security trouble in wireless network is on demand.

☆ This research was supported by National Natural Science Fund of China (60372097), National Natural Science Fund of China-key project (60432040), Beijing Municipal Natural Science Fund (4052021).
* Corresponding author. Tel.: +86 1062285460.
E-mail address: ibcf@sohu.com (J. Nie).

0165-0114/$ - see front matter © 2006 Elsevier B.V. All rights reserved.
doi:10.1016/j.fss.2005.12.007

A side effect of the flexibility is the ease with which a node can join or leave a MANET. Lack of any fixed physical and, sometimes, administrative infrastructure in these networks makes the task of securing these networks extremely challenging.

Routing is essential for a MANET to operate correctly, and a lot of routing protocols have been proposed in the literature, including proactive (table-driven), reactive (demand-driven), and hybrid solutions. Most of the existing protocols have assumed a MANET as a trusted environment. Unfortunately, in the presence of malicious nodes, a MANET is highly vulnerable to attacks due to its open environment, dynamically changing topology, and lack of centralized security infrastructure. To address this concern, several secure routing protocols have been proposed recently [1,5,8–10], such as SAODV [10], SRP [5], SAR [9]. But these secure routing protocols are mostly based on authentication and encryption algorithm. The Security-Level of mobile hosts is not fully considered.

This article intends to present a secure routing protocol for an MANET. The proposed secure routing protocol is derived based on the AODV protocol [6]. The protocol incorporates the Fuzzy Logic Based Security-Level [4] of the MANET.

The rest of this paper is organized as follows. Some backgrounds are given in Section 2. In Section 3 an adaptive Security-Level algorithm for MHs (mobile hosts) which is based on fuzzy logic is proposed and described. Section 4 proposes a new distributed multicast FLSL routing protocol based on the MH's Security-Level and focus on the main route selection mechanism of FLSL–how to select the shorter and more secure route. In Section 5, we compare its performance to the ad hoc on-demand distance vector routing (AODV) protocol by simulations. Section 6 analyzes the FLSL protocol. Conclusions are drawn in Section 7.

2. Preliminaries

In a MANET, two security issues need to be addressed: one is to protect transmitted data and the other is to make the routing protocol secure. The former can be done through end-to-end protection and has been well addressed in wired networks. The latter is particularly challenging for MANETs with dynamically changing topologies. If we have a MANET whose members are a "team" and know a priori a "team-key", this is not a big problem. However, if we want to create a MANET where everybody can participate, secure routing is necessary because there is no way to enforce everybody to be honest.

The SAODV (Secure Ad hoc On-demand Distance Vector Routing) protocol [10] is an extension of AODV [6]. Adversary nodes may forge AODV packets, listen to others, reply packets in their own interests, and report errors where there are none. To defend these attacks, it is assumed that each node has a certified public key. Hop-by-hop authentication is used to protect routing messages, and all intermediate nodes need to cryptographically validate the digital signatures appended with a routing message.

Assuming the existence of a security association between each pair of source and destination nodes, the SRP (Secure Routing Protocol) [5] guarantees that fabricated, compromised, or relayed route replies would either be rejected or never reach back the querying source. Compared to SAODV, the verification is not needed for intermediate nodes, thus removing the overheads. The security association can be obtained via the knowledge of the communication counterpart's public key. SRP is robust in the presence of misbehaving nodes, and provides accurate routing information in a timely manner.

The SAR (Security-Aware Routing) protocol [9] incorporates security attributes as parameters in route discovery. SAR ensures that a route only consists of nodes at the same trusted level. However, such routes may not always exist.

The aforementioned protocols all assume the existence of some security associations among hosts, which must be pre-established or established on-line. This poses difficulty in a MANET.

3. Adaptive fuzzy logic based security-level

In this section, an adaptive fuzzy logic based Security-Level algorithm is presented. To simplify the model, the following assumptions are made:

(1) The IEEE 802.11 standard and WEP (Wired Equivalent Privacy) [3] are used in MANETs.
(2) The links are bidirectional.

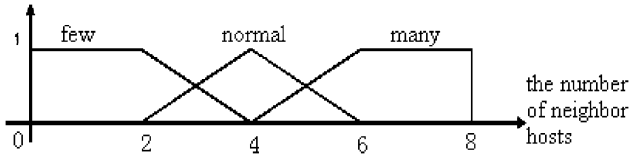

Fig. 1. Membership function of fuzzy variable n.

The security afforded by the algorithm relies on the difficulty of discovering the secret key through a brute-force attack. We discuss the correlative factor of MH's Security-Level:

(1) The longer the secret key is, the stronger to withstand serious brute force attack. There are two kinds of keys in IEEE 802.11 standard: 128-bits key and 40-bits key. A mobile host using a 128-bits key is more secure than a mobile host using a 40-bits key.
(2) The more quickly the secret key changes, the more secure the mobile host is. It is more difficult to decipher the key in a shorter time. A mobile host changing secret key frequently is more secure than a mobile host using a constant secret key.
(3) The more neighbor hosts the mobile host has, the more potential attacker. That is, the possibility of being attacked is larger.

There are many other factors to affect the security of mobile hosts, e.g., bandwidth. The Security-Level of mobile hosts is a function with multiple variables and affected by more than one condition.

Here a fuzzy logic system is defined [2]. Inputs of the fuzzy logic system are the length of the secret key (l), the frequency of changing keys (f) and the number of neighbor hosts (n). Output of the fuzzy logic system is the Security-Level of MH (S). It is assumed that the three factors are independent with each other. The relationship of them is as follows:

$$S \propto l \bullet f \bullet \frac{1}{n}. \tag{1}$$

It means that the Security-Level of MH is in direct proportion to the length of the key and the frequency of changing keys, in inverse proportion to the number of neighbor hosts. The S value is updated by the fuzzy logic system. When the key length is short, the Security-Level of MH should be low; otherwise the Security-Level of MH should be high.

- The input fuzzy variable "the number of neighbor hosts" has three fuzzy sets—few, normal and many. The membership function of n is illustrated in Fig. 1.
- The input fuzzy variable "the length of the secret key" has two fuzzy sets—short and long. The membership functions of l is showed in formulation (2)

$$l = \begin{cases} short & \text{the key is 40 bits,} \\ long & \text{the key is 128 bits.} \end{cases} \tag{2}$$

- The input fuzzy variable "the frequency of changing keys" has two fuzzy sets—slow and fast. The membership functions of f is showed in formulation (3)

$$f = \begin{cases} slow & \text{the secret key is constant,} \\ fast & \text{the secret key is variable.} \end{cases} \tag{3}$$

- The output fuzzy variable "the Security-Level of MH" has five fuzzy sets -lowest, low, normal, high, highest.

It should be noted that modifying the membership functions will change the sensitivity of the fuzzy logic system's output to its inputs. Also increasing the number of fuzzy sets of the variables will provide better sensitivity control but also increases computational complexity of the system. Table 1 shows the rules used in the fuzzy logic system.

Table 1
Fuzzy logic system rules

Input			Output
l	f	n	S
Short	Slow	Few	Low
Short	Slow	Normal	Lowest
Short	Slow	Many	Lowest
Short	Fast	Few	Normal
Short	Fast	Normal	Low
Short	Fast	Many	Low
Long	Slow	Few	High
Long	Slow	Normal	Normal
Long	Slow	Many	Low
Long	Fast	Few	Highest
Long	Fast	Normal	High
Long	Fast	Many	High

4. Security-level based distributed ad hoc routing protocol

4.1. The basic idea of FLSL (Fuzzy Logic Based Security-Level) routing protocol

The FLSL routing protocol is a source-initiated on-demand routing protocol. It aims to find out the route with the highest Security-Level in the MANET.

Because the Security-Level of a route is decided by the node which has the lowest Security-Level in that route, the node with the lowest Security-Level in the highest Security-Level route has higher security level than the node with the lowest Security-Level in other routes. In another word, the route with the highest Security-Level is comparably most secure.

To scale the security, the lowest, low, normal, high, highest of Security-Level correspond to 5, 4, 3, 2, 1 in value. We define the source node as s and the destination node as t. There are $R_1, \ldots, R_n$, totally n possible routes from the source s to the destination t. In R_i, there are relay node $n_1, \ldots, n_j, \ldots, n_m$, totally m possible relay nodes to forward the packets from the source to the destination.

Suppose the current Security-Level of the jth node in the ith route is S_{ij}, then the SL (Security-Level) of the ith route is:

$$SL_i = \min\ S_{ij}, \quad j \in (1, \ldots, m)\,. \tag{4}$$

Therefore, the desired route k can be obtained from

$$SL_k = \max_{i \in A}\ SL_i \tag{5}$$

where A is the set containing all possible route.

$$A = \{R_1, R_2, \ldots, R_n.\} \tag{6}$$

4.2. The routing process of FLSL routing protocol

4.2.1. Route discovery

The FLSL routing protocol is a source-initiated on-demand routing protocol, so nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges.

The FLSL routing protocol uses the following fields with each route table entry:

- Destination IP Address
- Destination sequence number (guarantee the loop-freedom of all routes towards that node)
- Valid destination sequence number flag
- Security-level (the minimum security-level of all nodes in the route)
- Hop count (number of hops needed to reach destination)

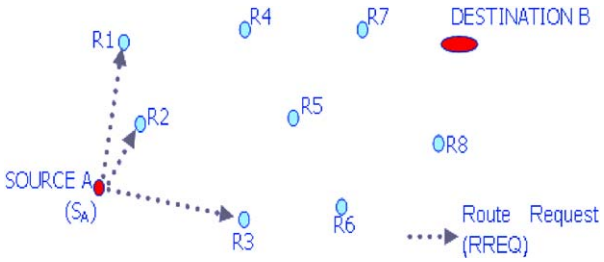

Fig. 2. Create RREQ.

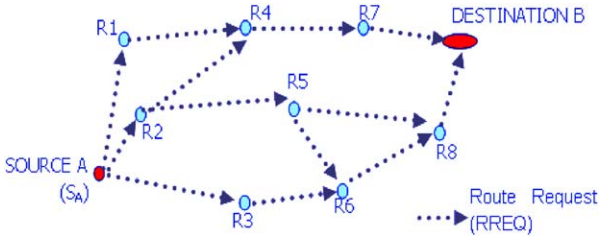

Fig. 3. Broadcast RREQs.

- Next hop
- Lifetime (expiration or deletion time of the route)

The process of route discovery is as follows.

(1) When the source node wants to send a message to the destination node and does not already have a valid route to that destination, it initiates a path discovery process to locate the other nodes. The source node disseminates a route request (RREQ) to its neighbors (Fig. 2).

The RREQ includes such information: destination IP address; destination sequence number; Security-Level (the minimum Security-Level of all nodes in the current found route); hop count; lifetime and etc.. The destination sequence number field in the RREQ message is the last known destination sequence number for this destination and is copied from the destination sequence number field in the routing table. If no sequence number is known, the unknown sequence number flag must be set. The Security-Level is equal to the source node's Security-Level. The Hop Count field is set to zero. When the neighbor node receives the packet, it will forward the packet if it matches some conditions.

(2) When an intermediate node receives the RREQ from its neighbors, it first increases the hop count value in the RREQ by one, to account for the new hop through the intermediate node if the packet should not be discarded.

The originator sequence number contained in the RREQ must be compared to the corresponding destination sequence number in the route table. If the originator sequence number of the RREQ is not less than the existing value, the intermediate node compares the Security-Level contained in RREQ to its current Security-Level to get the minimum, and then updates the Security-Level of RREQ with the minimum, which is the latest Security-Level of this route.

- If the originator sequence number contained in the RREQ is greater than the existing value in its route table, the relay node creates a new entry with the sequence number of the RREQ.
- If the originator sequence number contained in the RREQ is equal to the existing value in its route table, the Security-Level of the RREQ must be compared to the corresponding Security-Level in the route table. If the Security-Level contained in the RREQ is greater than the Security-Level in the route table, the relay node updates the entry with the information contained in the RREQ.

During the process of forwarding the RREQ, intermediate nodes record in their route tables the addresses of neighbors from which the first copy of the broadcast packet was received, thereby establishing a reserve path. If additional copies of the same RREQ are later received, these packets are silently discarded (Fig. 3).

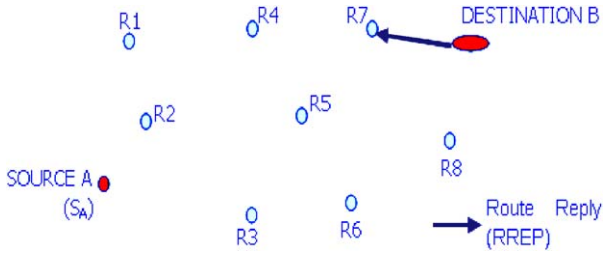

Fig. 4. Create RREP.

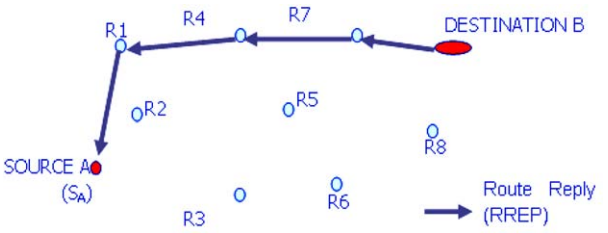

Fig. 5. Establish a route.

For each valid route maintained by a node as a routing table entry, the node also maintains a list of precursors that may be forwarding packets on this route. The list of precursors in a routing table entry contains those neighboring nodes to which a route reply was generated or forwarded.

(3) Once the RREQ has arrived the destination node or an intermediate node with an active route to the destination, the destination or intermediate node generates a route reply (RREP) packet and unicast it back to the neighbor from which it received the RREQ (Fig. 4).

If the generating node is intermediate node, it has an active route to the destination and the destination sequence number in the node's existing route table entry for the destination is not less than the destination sequence number of the RREQ and the "destination only" flag is not set.

If the generating node is the destination itself, it must update its own sequence number to the maximum of its current sequence number and the destination sequence number in the RREQ packet immediately before it originates a RREP in response to a RREQ. The destination node places its sequence number into the destination sequence number field of the RREP and enters the value zero in the hop count field of the RREP.

When generating a RREP message, a node copies the destination IP address, the originator sequence number and Security-Level from the RREQ message into the RREP message.

(4) When an intermediate node receives the RREP from its neighbors, it first increases the hop count value in the RREP by one. As the RREP is forwarded back along the reverse path, the hop count field is increased by one at each hop. Thus, when the RREP reaches the source, the hop count represents the distance, in hops, of the destination node from the source node.

The originator sequence number contained in the RREP must be compared to the corresponding destination sequence number in the route table entry. If the originator sequence number of the RREP is not less than the existing value, the node compares the Security-Level contained in RREP to its current Security-Level to get the minimum, and then updates the Security-Level of RREP with the minimum, which is the latest Security-Level of this route (Fig. 5).

- If the sequence number in the routing table is marked as invalid in route table entry or the destination sequence number in the RREP is greater than the node's copy of the destination sequence number, the intermediate node creates a new entry with the destination sequence number of RREP and marks the destination sequence number as valid. The Security-Level field in the route table entry is set to the Security-Level contained in the RREP.

Table 2
Constant parameters in simulations

Constant parameter	Value
Transmission range	200 m
Topology size	1000 m × 1000 m
Number of sources	1
Number of destinations	1
Traffic type	constant bit rate

Table 3
Varied parameters in simulations

Varied parameter	Value
The number of mobile nodes	50–500

- If the originator sequence number contained in the RREP is equal to the existing destination sequence number in the node's route table, the entry of this sequence number is updated with the information contained in the RREP and the Security-Level in the intermediate node's route table is set to the Security-Level in the RREP.

The next hop in the route entry is assigned to be the node from which the RREP is received, which is indicated by the source IP address field in the IP header. The current node can use this route to forward data packets to the destination.

4.2.2. Route maintenance

Inheriting from the AODV routing protocol, a node uses hello message which is periodic local broadcasts by a node to inform each mobile node in its neighborhood to maintain the local connectivity. A node should only use hello messages if it is part of an active route. Within the past delete period, it has received a hello message from a neighbor, and then for that neighbor does not receive any packets (hello messages or otherwise) for more than allowed_hello_loss* hello_interval milliseconds, the node should assume that the link to this neighbor is currently lost. When this happens, the node should send a route error (RERR) message to all precursors indicating which link is failed. Then the source initiates another route search process to find a new path to the destination or start the local repair.

5. Simulation

5.1. Simulation scenario

The topology is a rectangle area with 1000 m length and 1000 m width. The ad hoc routing protocol is FLSL in the MANET. Two of the nodes are fixed nodes, one is the source node and the other is the destination node. The position of the source node is (20,20) and the position of the destination node is (75,80). The source node is constant bit rate (CBR) traffic source. Other nodes in this area are mobile nodes. They are distributed randomly within the MANET. The length of the secret key and the frequency of changing keys of all nodes are set random. The security-level is defined in Section 3.

The constant parameters used in all simulations are given in Table 2. In the simulations, the effect of different mobile nodes is evaluated. The varied parameters are shown in Table 3.

5.2. Simulation results

We have evaluated the performance of MANET utilizing the proposed FLSL routing protocol. The FLSL routing protocol is compared with the AODV routing protocol.

The performance evaluation criteria are average security-level of the route from source to destination and packet delivery ratio. The performance criteria are defined as follows:

- The average security-level of a route is defined as

$$\text{Average security} - \text{level} = \frac{\Sigma\text{The security} - \text{level of a node in the route}}{\text{The number of nodes in the route}}$$

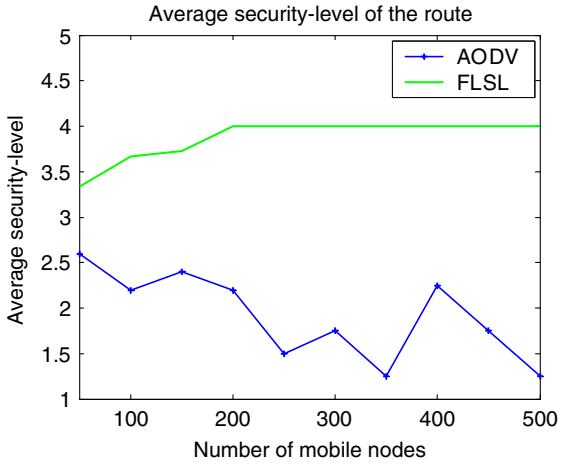

Fig. 6. The average security-level vs the number of mobile nodes.

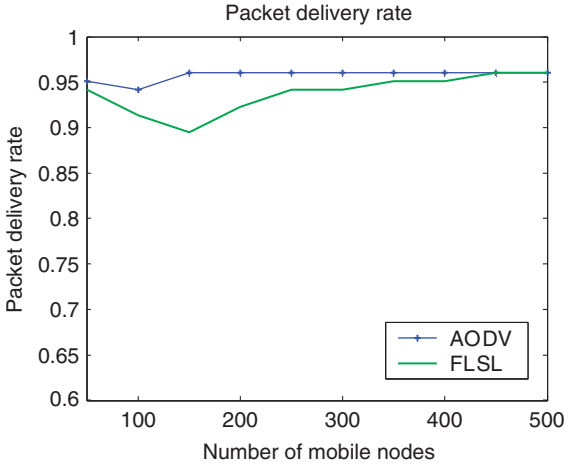

Fig. 7. The packet delivery rate vs the number of mobile nodes.

- The packet delivery rate is defined as

$$\text{packet delivery rate} = \frac{\text{The packets successfully received}}{\text{The packets generated}}$$

The simulation results are analyzed in the following paragraphs.

- *Average security-level*: Fig. 6 shows the average security level with the number of mobile nodes between 50 and 500. As the figure shows, the average security-level of FLSL route is much higher than the average security-level of AODV route, especially for many mobile nodes. This is an expected result since the more mobile nodes there are, the more neighbor hosts a node has and then the possibility of being attacked is larger.
- *Packet delivery rate*: Fig. 7 shows the packet delivery rate with the number of mobile nodes between 50 and 500. The packet delivery ratio is very high (mostly above 94%) for all two routing protocols. However, the AODV protocol has some larger packet delivery rate than the FLSL protocol, especially with few mobile nodes. The reason is that the less mobile nodes result in long transmission distance.

6. Analysis

The FLSL routing protocol is a pure on-demand routing protocol, as nodes that are not on a selected path do not maintain routing information or participate in routing table exchanges. The FLSL protocol allows mobile nodes to obtain routes quickly for new destinations and respond to link breakages and changes in network topology in a timely manner. The operation of FLSL is loop-free, and by avoiding the "counting to infinity" problem offers quick convergence when the mobile ad hoc network topology changes (typically, when a node moves in the network). When links break, FLSL causes the affected set of nodes to be notified so that they are able to invalidate the routes using the lost link. As in the AODV routing protocol, the shortest routing is found when the source initiates a route discovery with a new destination sequence number. But one distinguishing feature of FLSL routing protocol is its use of a Security-Level as selection criterion.

Since Security-Level is directly incorporated into the FLSL routing protocol, this metric prevents hostile hosts from being overused, thereby improving the security until the network is partitioned. If all nodes have similar Security-Level, it will select a shortest route.

The FLSL routing protocol selects the shortest path which decreases the transmitting time and therefore could shorten the attack time of attacker and improve the MANET's security. At the same time, the FLSL routing protocol updates the route using Security-Level as metrics, which ensures the updated route has the greater Security-Level. Given the choice between two routes to a destination, a requesting node is required to select the one with the greatest Security-Level. Thus avoids malicious nodes from being unwisely overused before the network is partitioned.

Compared with the AODV routing protocol, the FLSL routing protocol is securer in addition to providing high packet delivery rate. In a word, the FLSL routing protocol can improve MANET's security.

7. Conclusion

In this paper, we present the characteristics and security management of the MANETs.

This paper presents a Fuzzy Logic Based Secure multicast routing protocol—FLSL routing protocol for MANETs. An interesting property is that every node in the MANET has the field of Security-Level based on the fuzzy logic in the route tables to select the highest Security-Level route. The FLSL routing protocol can improve MANET's security. It is feasible to the weak security character of mobile ad hoc networks.

Acknowledgments

This research was supported by National Natural Science Fund of China (60372097), National Natural Science Fund of China-key project (60432040), Beijing Municipal Natural Science Fund (4052021).

References

[1] D. Dhillon, T. Randhawa, M. Wang, L. Lamont, Implementing a fully distributed certificate authority in an OLSR MANET, WCNC 2004 IEEE Wireless Communication and Networking Conference, Atlanta, GA, USA, March 21–25, 2004.
[2] J. Edney, W.A. Arbaugh, Real 802. 11 Security: Wi-Fi Protected Access and 802. 11i, Addison-Wesley, Reading, MA, July 15, 2003.
[3] A. Majlesi, B. H. Khalaj, An Adaptive Fuzzy Logic Based Handoff Algorithm for Interworking between WLANS and Mobile Networks, PIMRC 2002.
[4] T. Narten, E. Nordmark, W. Simpson, Neighbor Discovery for IP Version 6 (IPv6), RFC2461, 1998.
[5] P. Papadimitratos, Z. J. Haas, Secure routing for mobile ad hoc networks. Proc. SCS Communication Networks, and Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 2002.
[6] C. Perkins, E.M. Belding-Royer, S. Das, Ad hoc On-Demand Distance Vector (AODV) Routing, IETF Internet Draft, 2002.
[7] C.-K. Toh, Ad hoc Mobile Wireless Networks: Protocols and Systems, Prentice-Hall PTR, Englewood Cliffs, NJ, 2002.
[8] Yu-Chee Tseng, Jehn-Ruey Jiang, Jih-Hsin Lee, Secure bootstrapping and routing in an IPv6-based ad hoc network, Proc. 2003 Internat. Conf. on Parallel Processing Workshops (ICPPW'03).
[9] S. Yi, P. Naldurg, R. Kravets, Security-aware ad hoc routing for wireless networks, ACM Internat. Symp. on Mobile Ad hoc Networking and Computing 2001.
[10] M. G. Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, Internet Draft: draft-guerrero-manetsaodv-00.txt, 2002.