An Intelligent Scheme of Secure Routing for Mobile Ad Hoc Networks

Zhongwei Zhang
Department of Mathematics and Computing
University of Southern Queensland
zhongwei@usq.edu.au

***Abstract*— An ad hoc network is a peer-to-peer network without no centralised server. Mobile Ad Hoc Network(MANETs) is a promising new wireless communications paradigm in which network device may move around and end hosts may function as a router. It is a key of success of being deployed to properly address the security problems. Although many research focus on how to deliver packets from one node to another, research into the security will surely overtake the trend and play the leading role. Current techniques of addressing security on the fixed structured wired network are only useful to protect the transmitted message on the end nodes, the security of routing information among the mobile nodes in the hostile environment where mobile Ad Hoc networks are usually used [4] has been inadequately addressed.**

Security and routing on the wired networks have been treated separately due to that Security is concerned with how to defend nodes from hackers attack, while routing is about how to efficiently determine optimal routes. Recent research shown that the security and routing on mobile Ad hoc networks need to be considered altogether, that is, the routing needs to be done with the capability of preventing various attacks from compromised or malicious nodes.

Towards a solution of secure routing on MANETs, we discuss a new scheme, which is reliant on the fuzzy logic, capable of determining the most secure route during the routing discovery in this paper. Similar to the AODV or SAODV in the route discovery, the algorithm will decide a secure path among all the possible routing paths based on the knowledge about its neighbour nodes. The nodes will forward or reply the route with the highest security level. The feasibility of the proposed scheme of secure routing will be demonstrated by using simulation on NS2. In addition, the performance of the new secure routing protocol on the simulation experiments are presented.

I. Introduction

Ad hoc networks is a kind of special wireless network mode. A mobile ad hoc network (MANET) is a collection of two or more devices equipped with wireless communications and networking capability. Primary applications of Ad Hoc networks are the military, tactical and other security-sensitive operations.

In an Ad Hoc network, there is no fixed infrastructure such as base stations or mobile switching canters. Nodes of an ad-hoc network are mobile hosts with similar transmission power and computation capabilities. This feature of no fixed infrastructure makes MANET exhibit two antagonistic characteristics. For instance, this feature popularise MANET to be deployed at some place where wired networks are impossible to be laid down on one hand, this feature also renders MANET in jeopardies that attackers can easily break-in on other hand.

Although most applications are highly sensitive to message transmitted, mobile Ad-hoc networks often lack security mechanism in place within the network layer or MAC layer. For instance, MANETs are vulnerable to many kinds of attacks with IEEE 802.11 standard. The mobility of hosts adds another dimension of complexity in routing and security e.g. the security level of mobile nodes always change all the time. Most of research are concentrated on the problem of how to secure routing information on the mobile nodes. A good secure routing algorithm should prevent each of the attacks. It must ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation.

Though many researchers are working towards the security of wireless networks. These studies are based two type of approaches. One approach is to develop Secure protocols for instance, secure routing algorithms. Another approach is to design secure architecture such as Hierarchical Hybrid architecture. In past decades, there are many schemes of secure routing protocols designed for MANETs, unfortunately a limited number of these schemes are practically implemented, their feasibility and performance are yet to be studied. In case that there are two or many routes, these implementations can not guarantee the communication nodes with a most secure route. Another problem is that they are not capable of adapting to the changing in their topology.

In this paper, we develop a fuzzy logic based scheme of secure routing protocol on MANETs. In Section II, we present an overview of possible attacks on MANETs. Routing on MANETs are more challenging than conventional networks, a set of routing protocols have been reviewed in Section III along with several algorithms of achieving the security. Our implementation is given in Section V. We demonstrate the feasibility of the proposed scheme and perform a set of simulation experiments using NS2 in Section IV. The paper is concluded in Section VI by a discussion, followed by a list of possible questions for the future,

II. Security Concerns in MANETs

Wireless networks are more vulnerable to link attacks than wired networks due to the wireless transmission media. A scrutinise reveals that security concerns in MANETs involve two separate problems: secure routing discovery and secure data transmission over the MANETs.

The use of wireless links makes MANETS susceptible to many attacks. For instance, eavesdroppers can access secret information, violating network confidentiality. Hackers can directly attack the network to delete messages, inject erroneous messages, or impersonate a node, which violates availability, integrity, authentication, and non-repudiation. Compromised nodes also can launch attacks from within a network.

One approach to address the security on MANETs is through the authentication of message among the communicating nodes, while another approach to enhance security on MANETs is through intrusion detection. Intrusion detection is a reactive approach, which has been used with relative maturity in the traditional wired networks.

All secure routing protocols do not specify a scheme to protect data or sensitive routing information. Any centralised authority could lead to more vulnerability in MANETs. Accordingly, a secure routing protocol must be based on the principle of distributed trust. That is for each mobile hosts, there is a relationship of trust to others. Each host has a certain level of trust to other hosts.

Designing of secure routing protocols on MANETs has been based on two approaches.

A. *Protocol based approach*

Many protocols have been developed to defend against link attacks. Dynamic source routing(DSR) is a simple routing algorithm, in which a sending node must provide the sequence of all nodes through which a packet will travel. Each node maintains its own route cache, essentially a routing table, of these addresses. Source nodes determine routes dynamically and only as needed; there are no periodic broadcasts from routes.

B. *Architecture based approach*

Hierarchical Hybrid architecture is an infrastructure for wireless networking. In a HH network, all mobile nodes are partitioned into groups. Each group has a group agent and some group members. A group agent itself can be a group member of higher level group.

C. *Hybrid approach*

This approach is to combine the advantages of on-demand and optimised link-state routing for wireless sensor networks. The algorithm discovers the route to each node only when it is necessary, but route discovery is based on multipoint relays. It works as follows: the algorithm defines three types of nodes: (1) master, (2) gateway, and (3) plain. A group of nodes selects a master to form a piconet and then synchronises and maintains the neighbour list. A node can be a master in only one piconet, but it can be a plain member in any number of piconets. Gateway nodes belong to two or more piconets. Only masters and gateways forward routing information; plain nodes receive and process this information, but they do not forward it.

III. Routing protocols and security algorithms

Different than conventional wired networks, routing on MANET is characterisised by constant changing of route and susceptibility of attacks. Routing algorithms include DSR [2], AODV [1], and SAODV [7].

A. *Efficient routing protocols for MANETs*

In this section, we review an efficient routing protocol for MANETs. Among other routing protocols, Ad hoc On-Demand Distance Vector Routing(AODVR) is regarded as the most efficient. With AODVR, a source node checks its routing table whether there is a route, if there is no existing route, it then broadcasts an RREQ packet across the MANET. All nodes that received this RREQ packet will update their information for the source node.

Figure 1 describes the format of a RREQ packet.

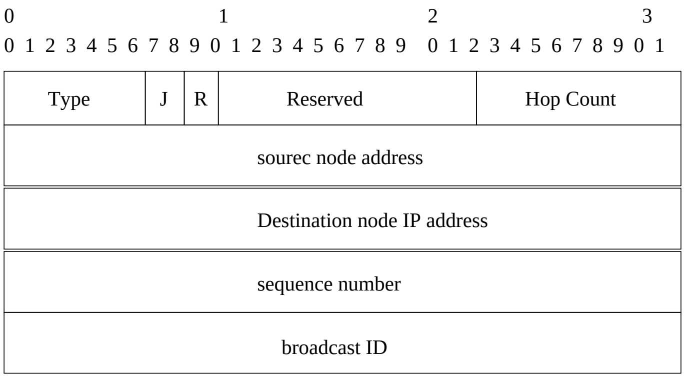

Fig. 1.   RREQ packet format

Where `Type` is 1, J is joint flag and R is repair flag. `HCount`: refers to the number of hops from the Source IP Address to the node handling the request.

`BID`: is a sequence number uniquely identifying the source node's IP address. `DIP`: IP address of destination for which a route is desired. `DSN`: is the last sequence number received in the past by the source for any route towards the destination. `SIP`: is the IP address of the node which originated the route request. `SSN`: the current sequence number to be used for route entries pointing to the sequence of the route request.

More importantly, AODV has a number of operations, for instance, the unicast communication of nodes include: nodes generating of RREQ and RREP and how the fields in the message are changed.

Figure 2 describes the AODV's route discovery. Node S intends to explore a route to destination node D.

- Generating route requests: A node broadcast a RREQ when it determines that it needs a route to a destination and does not have one available. After broadcasting a RREQ, a node waits for a RREP. If the RREP is not received within a constant time, the node may rebroadcast the RREQ, up to a fixed number of times. Note that each broadcast will increment the broadcast ID in the RREQ.
- Forwarding route requests: When a node receives a broadcast RREQ, it first checks to see whether it has

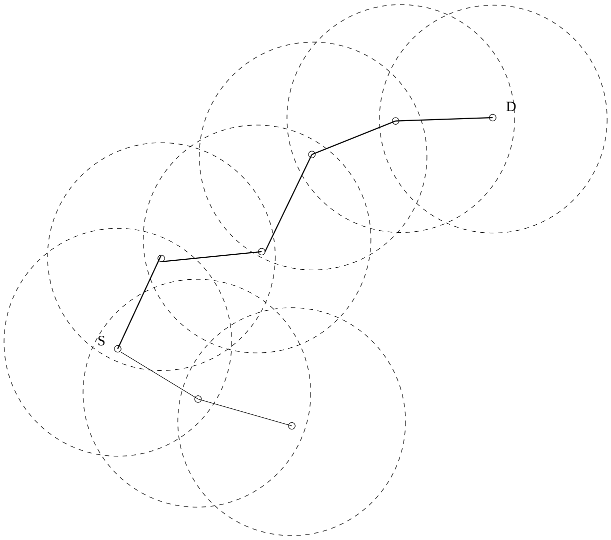

Fig. 2. Route discovery

received a RREQ with the same source IP address and a broadcast ID field of equal unsigned integer value within the last. If the checking result is invalid, then it forwards the RREQ packet to its neighbour nodes. The routing table in these nodes will be updated and a reverse path is added.
- Piggyback route reply: When this broadcasted RREQ eventually reach an intermediate node on which the checking result is valid or simply the destination node, the intermediate node or the destination node would create a RREP packet, and piggyback it back to the source node.

The primary objective of AODV and its routing algorithms is to discover routes for the packets to be delivered from the source node to the destination node, with best efficiency they ever can achieve. The security in the discovered routes was not seriously considered. AODV is an efficient routing protocol on MANETs which is necessary, but not good enough. If it can not ensure the security, the usability of MANETs would be severely reduced.

B. *Secure Routing Protocols for MANETs*

Efficient routing on MANETs is a primary challenge. Conventional routing protocols which depend on distance-vector or link-state usually use periodic broadcast advertisements of all routers to keep routing table up-to-date. Secure routing on MANETs faces several problems:

- periodically updating the network topology increase bandwidth overhead;
- repeatedly awakening hosts to receive and send information quickly exhausts batteries;
- the propagation of routing information causes overloading, thereby reducing scalability;
- communication systems often cannot respond to dynamic changes in the network topology quickly enough.

Most of secure routing protocols for MANETs use multihop rather than single-hop routing to deliver packets to their destination. The security of mobile nodes is guaranteed by the hop-by-hop authentication, and all intermediate nodes need to cryptographic-ally validate the digital signatures appended with a routing message.

Secure routing protocols usually are based on the efficient routing protocol such as the AODV protocol discussed in Section III-A. For instance, to add security to AODV, an extension to AODV called SAODV has been designed in recent time [7]. SAODV has extended the AODV by designing a few new extension messages, and a few operations on these new extension message.

Secure routing protocols significantly improve the usefulness of the efficient routing protocol. The idea was to incorporate more information in the routing message and routing table, there are security related operations introduced in the protocols. If a secure routing protocol incurs too much overheads, it is possible to render the protocol practically unusable.

C. *Examples of Secure Routing Protocols for MANETs*

A secure on-demand routing protocol for ad hoc networks is developed in [3]. Ariadne can authenticate routing message using one of three schemes: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication, or digital signatures.

SEAD: Secure efficient distance vector routing protocol [6]. SEAD is robust against multiple uncoordinated attacks creating incorrect routing state in any other node, even in spite of active attackers or compromised node in the network. The SEAD was designed based on the Destination-Sequenced Distance-Vector(DSDV).

During the route discovery process, the source node first selects a random seed number and sets the Maximum Hop-count(MHC) value. By using a hash function, h, the source computes the hash value as h(seed) and

Ariadne: A secure on-demand routing protocol for ad hoc networks. This protocol provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptography.

IV. A New Scheme of Secure Routing Protocol

FL-SAODV protocol is a secure routing protocol in which the security level is determined by fuzzy logic. FL-SAODV protocol assume that each mobile host uses a secure key with its neighbour nodes. Unlike existing strategies which always assume some security association, our proposed strategy is to rely on the knowledge about the secret key and node's environment such as the wireless link bandwidth and the number of neighbour nodes.

A. *Node's security association*

In spite of the intricate relationship between the security level with these factors, it is obvious that the security level is in the proportional to the number of the neighbouring nodes and the length of the key. After having an arduous investigation, we discovered the following knowledge.

- for each mobile node, if its secret key is frequently changed, it is pretty hard for adversary node to decipher the key. In other word, the mobile node concerned is of higher level of security.
  if we represent the frequency of key change by f, then the security level of a mobile node N will has a relationship as $SL \propto f$.
- if a node has many neighbour nodes, the number of adversary nodes is higher. The security level the node has can not be very high. The security level of the mobile node $SL \propto \frac{1}{n}$
- if a node has a secret key, its length is l, intuitively, the security level of this node must have a relationship as follows: $SL \propto l$.

B. New Secure Routing Protocol Operations

FL-SAODV is a new scheme of secure routing protocol. Like SAODV that is based on the AODV protocol, FL-SAODV is also an extension to the SAODV. FL-SAODV assumes that each mobile node has a signature key pair from a suitable asymmetric cryptosystem. Each node is capable of securely verifying the association between the address of a given mobile node and the public key of that node. Two mechanisms are used to secure the message: digital signatures to authenticate the non-mutable fields of the message, and hash chains to secure the hop count information, which is the only mutable information in the messages. Every node uses digital signatures to sign the whole message and that any neighbour that receives verifies the signature.

1) Mobile Node's Security Level: The security level of a mobile node in MANETs is determined by the length of the secret key, the frequency of the key change, and the number of its neighbour nodes at a particular time. Its value can be calculated by using a fuzzy system described in Algorithm 1.

Algorithm 1 Security level

```
$n \leftarrow$ number of neighbouring nodes
$f \leftarrow$ the frequency of key change
$l \leftarrow$ the length of the key
for all rules in the ruleset do
    get fuzzified value of $n$, $f$ and $l$.
    calculate the individual security level using fuzzy reasoning
    add the individual security level to the total security level
end for
get the defuzzified value of the total security level
```

2) Route discovery: The route discovery consists of two processes: (1) route request from the source node to the destination node, and (2) route reply from the destination to the source node. This algorithm of route discovery is described in Algorithm 2.

3) Route maintenance: A node uses HELLO message to maintain the local connectivity. The route maintenance is described in Algorithm 3.

Algorithm 2 FL-SAODV Route Discovery

```
$S \leftarrow SourceNode$, $T \leftarrow DestinationNode$
$SL_i$ is the security level of node $i$.
$SL_p$ is the security level in the RREQ packet {The Destination node sends RREP back}
Source node broadcasts a RREQ to all of its neighbours
repeat
    for neighbour nodes do
        if there is a route to the destination node then
            authenticate the RREQ using MD5
            calculate its security level using Algorithm 1.
            if $SL_i > SL_p$ then
                update the security level in the RREQ packet
                overwrite the SL in RREQ with $S_{ij} = min(S_{ij}, SL_p)$
                update other fields in RREQ
            end if
        else
            broadcast the RREQ to its neighbour nodes
        end if
    end for
until Destination node is reached {The Destination node sends RREP back}
for all RREQ received do
    if Broadcast ID && Security Level in RREQ then
        create a RREP
        unicast RREP back to S
    else
        drop the RREQ
    end if
    the destination determines which route is the best
    $SL_k = max(S_i)$
end for
```

V. Implementation and experiments

In this section, we describe an implementation of FL-SAODV, built as an augmentation to the SAODV protocol in the NS2 network simulator [8].

A. Routing message format and routing table

1) Routing request and reply packet: We modify the RREQ and the RREP packet formats to carry additional security information. The common fields in RREQ and RREP include:

- Destination IP address
- Source IP address
- Broadcast ID
- Expiration time for reverse path route entry
- Source sequence number

We simply adopt other messages such as HELLO message, RERR without modification.

2) Routing table: Every entry in the routing table contains seven fields as follows,

- Destination IP Address
- Destination Sequence Number

Algorithm 3 Route maintenance

```
S the source node
D the destination node
repeat
  S send a HELLO message to each neighbouring nodes
  for all neighbour nodes do
    if the neighbour node does not receive any packets within a certain time then
      the node assume the link is lost
      the node send an RERR message to all precursors
    end if
  end for
until Route Expired
S starts a new route discovery described in Algorithm 2.
```

- Valid Destination Sequence Number flag
- Security Level
- Hop Count
- Next Hop
- List of Precursors
- Lifetime

Where the field of Security Level is an additional than the ones in the routing table of AODV protocol. It is designed to represent the minimum security level of all nodes in the route.

The field of list of precursors contains those neighbouring nodes to which a route reply was generated or forwarded. In our implementation, a data structure called linked list is used.

The field of lifetime represents the expiration time of the route, the filed of Hop Count is the number of hops needed to reach the destination.

3) Fuzzy system of determine the security level: The security level of each mobile node is determined by a fuzzy reasoning system. The fuzzy system is implemented using the analysis and knowledge we obtained in section IV-A. The membership functions of each factor are selected as follows.

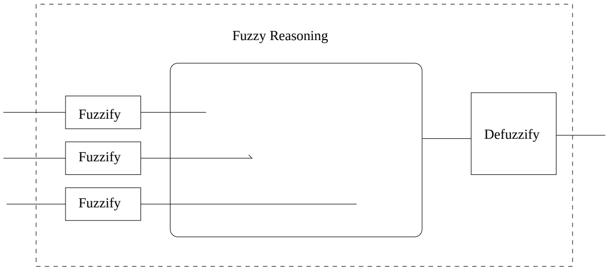

Fig. 3. Fuzzy system

Fuzzy membership function for three factors are defined as:

1) key_length: short and long; They are represented in Figure 4.
2) frequency: slow and fast; The membership functions looks quite the same as the one above. We would not present them here.
3) number_neighbour: few, normal, and many; These membership functions are shown in Figure 5.

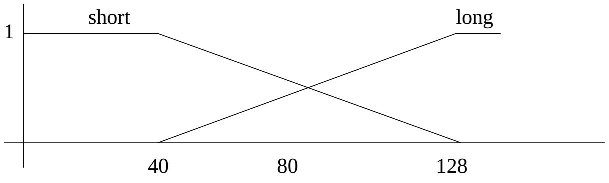

Fig. 4. Membership functions for Key Length

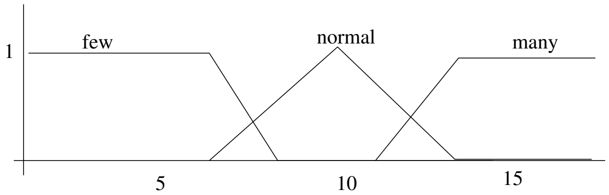

Fig. 5. Membership functions for the density of neighbour nodes

.

Fuzzy membership for the security level for each node are: lowest, low, normal, high and highest.

A fuzzy rule is a representation of knowledge in the form of **IF x is Big and y is Slow Then z is High**. According to the understanding about the mobile host in MANETs, we have modelled the relationship between the security level and factors, and presented them in Table I.

TABLE I
FUZZY RULES

key_length	frequency_key_change	n	likelihood_security_level
short	slow	few	low
short	fast	normal	normal
short	fast	many	low
long	slow	few	high

The security level of each mobile node is based on Algorithm 1.

B. Experiments and results

The results generated in this section are based on the simulation experiments set up for 4×4, 5×5 and 8×8 nodes moving around in 670m by 670m area. Nodes move according to the random way-point model.

When a node sends out the RREQ, it is assigned a random number between 0 to 100 as initial security level. The security level at each node *en route* is varying along the time due to the number of neighbour nodes changes. According to FL-SAODV, the next hop node will be either selected or determined from a few candidate nodes, based on the current security level. If there is only one neighbour node, FL-SADOV will choose that one; The relationship between FL-SAODV and AODV is that AODV is a special case, where on the route at each next hop, from the source node to the destination node, there is only candidate node.

We carried out a number of experiments. In our experiments, we shown the security level and the overheads of determining the next hop node. Figure 6 shows the security level at each

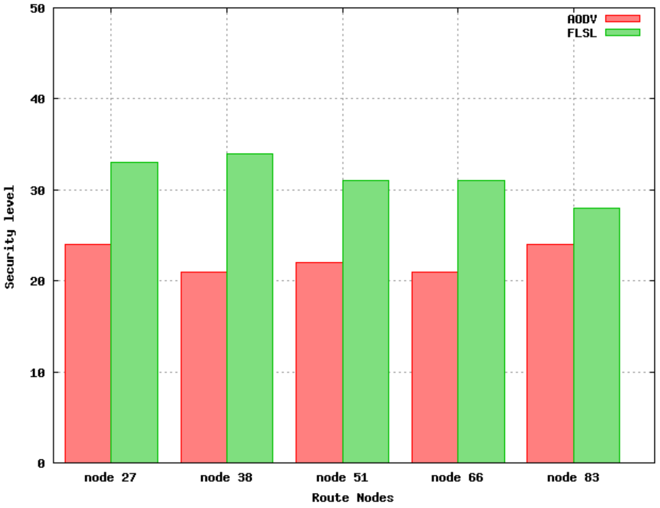

Fig. 6. Security Level on Route Nodes

intermediate node on the route from the source node to the destination node. Figure 7 shows the routing overheads (ie. the calculating time in μsec).

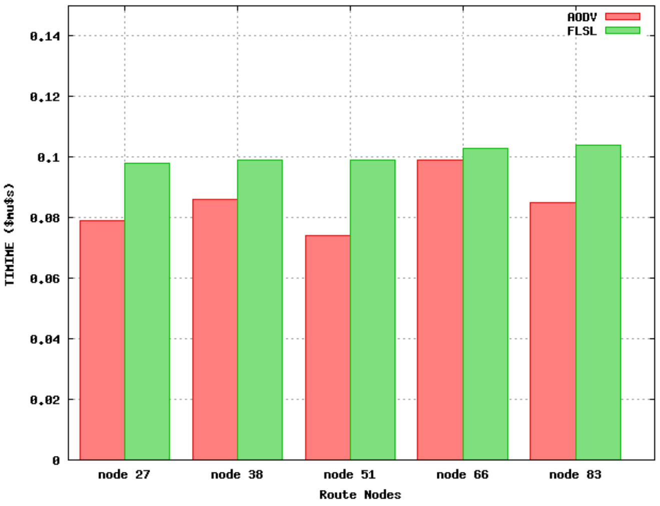

Fig. 7. Times in μs Spent on the Route Nodes

C. Analysis

We can see from Figure 6 and Figure 7, using FL-SADOV, the security level on each intermediate node on the route to the destination node has been improved, consequently the security level of the route is of higher value, comparing with the route determined by AODV.

At each intermediate hop node on the route, an additional overheads is needed for FL-SADOV to calculate the security level before the next hop node is determined. It is worthy pointing out that FL-SADOV has achieved a fair improvement to the route security at a small expense of extra overheads.

In summary, this scheme of secure routing protocol has the following features.

- Protecting routing information from attackers by using hop-by-hop authentication techniques: digital signature and hash. This avoids using a CA other secure routing protocols.
- It can adapt itself to the changing environment which is the most salient characteristics of the MANETs.
- FL-SAODV also improves MANETs security from two aspects:
  1) It selects the shortest route which decreases the transmitting time and therefore could shorten the attack time of attackers and improve the MANET's security.
  2) Using security level as metric ensures the updated route the most secure one.

VI. Discussion

In this paper, we have developed a practical solution to the secure routing on MANETs. First of all, we have reviewed the possibility of attacks to the MANETs, and the security adversaries which compromise a mobile host in ad hoc networks for the purpose of identifying a strategy to beef up hosts security level. Secondly, based on the characteristics of MANETs and requirements of secure routing, a new secure and efficient routing protocol has been developed. A set of algorithms have been designed. Thirdly, these algorithms have been implemented on the MANETs and many experiments on different scenarios have been carried out on NS2. Lastly, we listed out the security level of the nodes which are on the final route. The route found by using the FL-SAODV protocol will have higher security level than the route AODV found. In addition, we shown the timings on the it en route nodes and clearly shown that each *en route* node needs more time than AODV to decide their next hop.

There are two open questions for our future research. We believe that the performance of the protocol might be improved by using a better authentication method on one hand. On another hand, how to get the knowledge about the number of neighbour nodes needs more study.

References

[1] E. M. R. Charles E. Perkins and S. R. Das. Ad hoc on-demand distance vector (aodv) routing. RFC 3561, Nov. 2003.

[2] D. M. D.B. Johnson and Y. Hu. The dynamic source routing protocols for mobile ad hoc networks (dsr). *Internet Draft*, 4 2003.

[3] Y. C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. 2002.

[4] A. D. Nikola Milanovic, Miroslaw Malek and V. Milutinovic. Routing and security in mobile ad hoc networks. *IEEE Computer*, Feb. 2004.

[5] K. von Klitzing, G. Gorda, and M. Pepper. New method for high accuracy. *Phys. Rev. Lett.*, 45:494, 1980.

[6] D. B. J. Yih-Chun Hu and A. Perrig. Secure efficient distance vector routing in mobile wireless ad hoc networks, June 2002.

[7] M. G. Zapata. Secure ad hoc on-demand distance vector (saodv) routing. RFC 999, Mar. 2004.

[8] URL. http://www.isi.edu/nsnam/ns/ last version 2.31, March. 2007