22

A Novel Secure Routing Protocol for MANETs

Zhongwei Zhang
*University of Southern Queensland
Australia*

1. Introduction

Ad hoc networks is a special kind of wireless network mode. A mobile ad hoc network (known as MANET) is a collection of two or more devices equipped not only with wireless communications and networking capability, but also with mobility. Most applications of MANETs are primarily concentrated at the military, tactical and other security-sensitive operations (Somebody, 2000).

In MANETs, there is no need having fixed infrastructure such as base stations or mobile switching canters. That is to say, all nodes of MANETs are mobile hosts with similar transmission power and computation capabilities. The feature having no fixed infrastructure makes MANETs to exhibit two antagonistic characteristics. For instance, this feature popularize MANETs to be deployed at some place where wired networks are impossible to be laid down on one hand, this feature also renders MANETs in jeopardies that attackers can easily break-in on other hand.

Although many deployments of MANETs are highly sensitive to the message transmitted in the application layer, MANETs 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 in MAC and PHY layers. The mobility of hosts within MANETs adds another dimension of complexity in the network layer such as routing and security. The complexity is reflected by the fact that the security level of mobile devices or nodes always change all the time.

Most research efforts are concentrated on how to secure routing information on the mobile nodes. It is desirable that a good secure routing algorithm should not only prevent each of possible attacks, but also ensure that no node can prevent successful route discovery and maintenance between any other nodes other than by non-participation.

Methodologically looking at many researches which were working towards the security of wireless ad hoc networks, these studies are based on two types of approaches. One approach is to develop the 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. Further to the already implemented schemes, in case that there are two or more routes, none of them guarantee the communication nodes with the most secure route. Another problem is that the schemes are not capable of adapting to the changing in their topology.

In this chapter, we develop a new scheme of secure routing protocol for MANETs. In Section 2, we present an overview of possible attacks on wireless networks. Routing on MANETs is more challenging than conventional wireless networks, a set of routing protocols have been reviewed in Section 3 along with several algorithms of achieving the security. Our implementation is given in Section 5. We demonstrate the feasibility of the proposed scheme and perform a set of simulation experiments using NS2 in Section 5. The chapter is concluded in Section 6 by a discussion, followed by a list of possible questions for the future,

2. Security concerns in wireless networks

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

The use of wireless links makes wireless networks susceptible to many attacks. For instance, eavesdroppers can access secret information, violating network confidentiality. Hackers can either 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 wireless networks is through the authentication of message among the communicating nodes, while another approach to enhance security on wireless networks is through intrusion detection (ID). Intrusion detection is a reactive approach, which has been used with relative maturity in the traditional wired networks.

Associated with routing is that 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 wireless networks. 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.

2.1 Protocol based approach

Many routing protocols have been developed to defend against link attacks. Dynamic source routing(DSR) is a simple routing algorithm, in which a sending or source 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 broadcast packets from routes.

2.2 Architecture based approach

Hierarchical Hybrid(HH) architecture is an infrastructure for wireless networking. In a HH wireless 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.

2.3 Hybrid approach

This approach is to combine the advantages of on-demand (AODV) and optimized link-state routing (OLSR) 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 synchronies and maintains the neighbor 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.

3. Routing protocols and security algorithms for MANETs

Different than conventional wired networks, routing on MANET is characterized by constant changing of route and susceptibility of attacks. Existing routing algorithms include DSR (D. B. Johnson & Hu 2003), AODV (Charles E. Perkins & Das 2003) and SAODV (Zapata 2004).

3.1 Efficient routing protocols for MANETs

In this section, we review one efficient routing protocol for MANETs. Among other routing protocols, Ad hoc On-Demand Distance Vector Routing (AODV) is regarded as the most efficient. With AODV, 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 MANETs. All nodes that received this RREQ packet will update their information for the source node.

Figure 1 describes the format of a RREQ packet.
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.

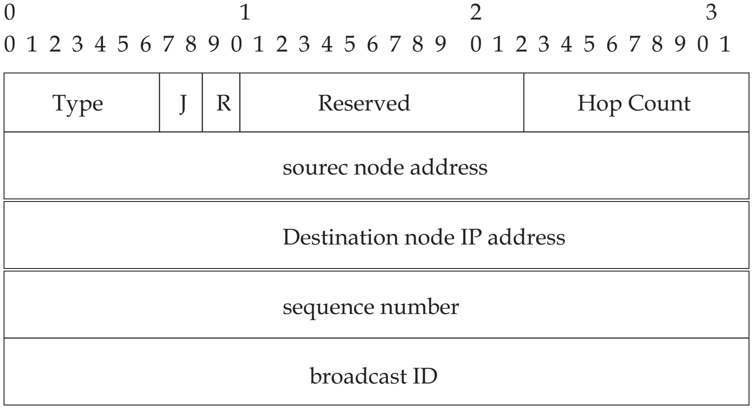

Fig. 1. RREQ packet format

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

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

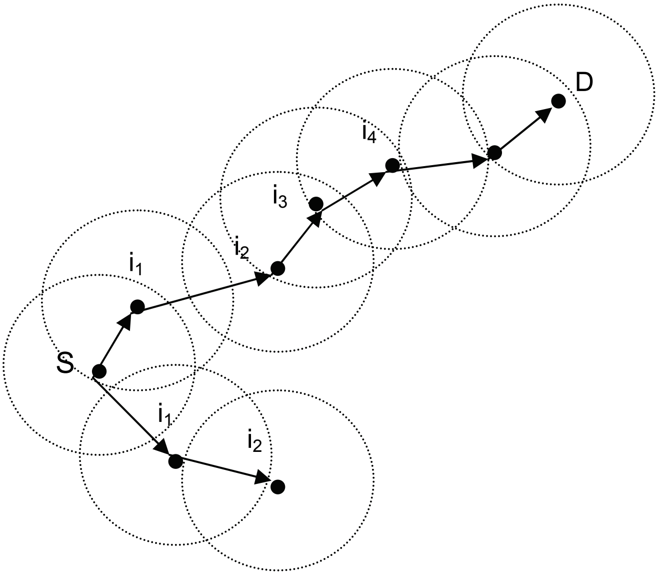

Fig. 2. Route discovery

- Generating route requests: The node S broadcasts a RREQ packet when it determines that it needs a route to a destination and does not have one available in its routing table. After broadcasting a RREQ packet, the node waits for a RREP packet. If the RREP packet is not received within a constant time, the node may rebroadcast the RREQ packet, the rebroadcasting will be repeated up to a fix number of times. Note that each broadcast will increment the broadcast ID in the RREQ packet.
- Forwarding route requests: When a node receives a broadcast RREQ packet, it first checks to see whether it has received a RREQ packet with the same source IP address and a broadcast ID field of equal unsigned integer value within the last RREQ packet. If the checking result is invalid, then it forwards the RREQ packet to its neighbor nodes. The routing table in these nodes will be updated and a reverse path is added.
- Piggyback route reply: When this broadcasted RREQ packet eventually reach an intermediate node on which the checking result is valid or simply the destination node, The intermediate node or the destination node (D) would create a RREP packet, and piggyback it back to the source node (S).

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. Unfortunately, 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.

3.2 Secure routing protocols for MANETs

Designing efficient routing protocols on MANETS is a primary challenge, but useful for conventional routing protocols. Conventional routing protocols which depend either on distance-vector or link-state usually use periodic broadcast advertisements of all routers to keep routing table up-to-date. In summary, efficient routing on MANETs faces several problems as follows.

- periodically updating the network topology increase bandwidth overhead;
- repeatedly awakening mobile nodes to receive and send information quickly exhausts batteries, which are the main power supply of the mobile nodes.
- 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 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 cryptographically 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 3.1. For instance, to add security to AODV, an extension to AODV called SAODV has been designed in recent time (Zapata, 2004). 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 simply incorporate more information in the routing message and routing table, in addition, there are security related operations introduced in the protocols. However, if a secure routing protocol incurs too much overheads, it is possible to render the protocol practically unusable.

3.3 Examples of secure routing protocols for MANETs

A secure on-demand routing protocol for MANETs is developed in (Hu et al, 2002), which is called Ariadne. 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*.

3.3.1 SEAD: Secure efficient distance vector routing protocol

SEAD (Yih-Chun Hu & Perrig, 2002) 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 node computes the hash value as `h(seed)`.

3.3.2 Ariadne: A secure on-demand routing protocol

This protocol provides security against one compromised node and arbitrary active attackers, and relies only on efficient symmetric cryptography.

4. Proposed secure routing protocol

We propose a new secure routing protocol for MANETs. It is known as FL-SAODV. The broadcast RREQ packet is an extension of RREQ packet described in Section 3.1, refer to Section 5.1.2.1 for more details. The routing table in each node is same as AODV, more details are given in Section 5.1.2. The 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 neighbor 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 neighbor nodes.

4.1 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 neighboring 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 neighbor nodes, the number of possible adversary nodes is higher. The security level the node has can not be very high. The security level of the mobile node $SL \propto \frac{1}{n}$, where n is the number of neighbour nodes.
- if a node has a secret key, its length is *l*, intuitively, the security level of this node must have a relationship as follows: $SL \propto l$.

4.2 New secure routing protocol operations

FL-SAODV is a new scheme of secure routing protocol for MANETs. 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 neighbor that receives verifies the signature. FL-SAODV has three operations: (1) determination of the node security level, (2) route discovery, and (3) route maintenance.

4.2.1 Mobile node's security level

The security level of a mobile node in MANETs is determined by the length of the secret key *(l)*, the frequency of the key change *(f)*, and the number of its neighbour nodes *(n)* at a particular time. Its value can be determined by using a fuzzy system described in Algorithm 1, as shown in Fig 3.

Algorithm 1 Security level

```
$n \leftarrow$ number of neighboring 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
```

4.2.2 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. The operation of route discovery is described in Algorithm 2.

Algorithm 2 FL-SAODV Route Discovery

```
$S \leftarrow SourceNode, D \leftarrow DestinationNode$
$SL_i$ 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 neighbors
repeat
    for neighbor 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 packet with $S_{ij} = min(S_{ij}, SL_p)$
                update other fields in RREQ
            end if
        else
            broadcast the RREQ to its neighbor 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 packet
        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
```

4.2.3 Route maintenance

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

Algorithm 3 Route maintenance

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

5. 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 (Network Research Group, 1995). The implementation of FL-SAODV involves the changes in routing message format and routing tables.

5.1 Routing message format and routing table

The RREQ packet and RREP packet are the most important packets among others.

5.1.1 Routing request and reply packet

We modify the RREQ packet and the RREP packet formats to carry additional security information. The common fields in RREQ and RREP packet 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 and RERR packet without modification.

5.1.2 Routing table

Every entry in the routing table contains seven fields as follows,

- Destination IP Address
- Destination Sequence Number
- 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 neighboring 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.

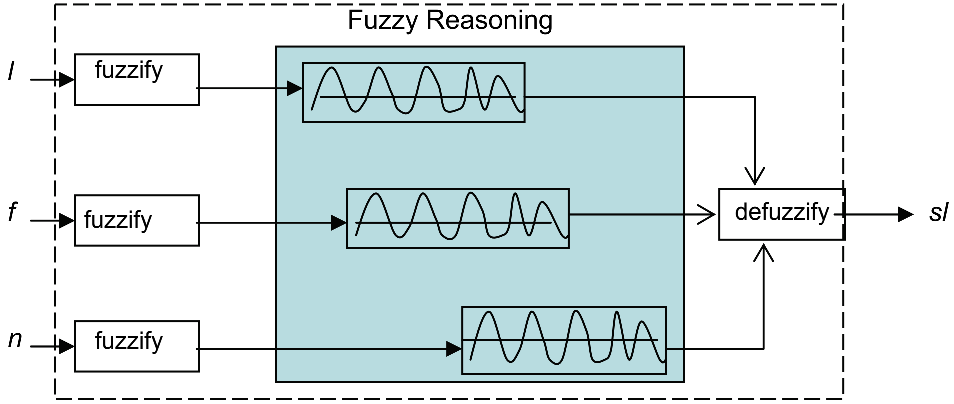

Fig. 3. Fuzzy system

5.1.3 Fuzzy system of determining 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 4.1.

The membership functions of each factor are selected as follows.

Fuzzy membership function for three factors are defined as:

1. key_length: short and long; They are represented in Figure 4.

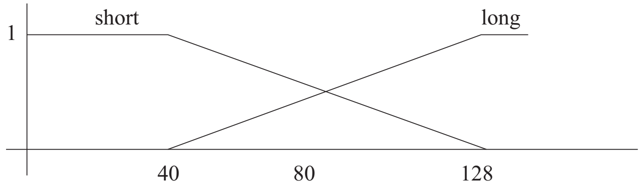

Fig. 4. Membership functions for Key Length

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.

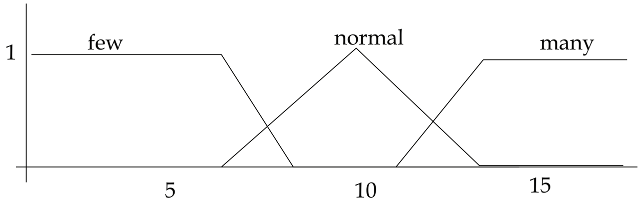

Fig. 5. Membership functions for the density of neighbor nodes.

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 nodes in MANETs, we have modeled the relationship between the security level and factors, and presented them in Table 1.

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

Key_Length (l)	Frequency_key_change (f)	Number_Neighbor_Node (n)	Likehood_security_level (sl)
short	slow	few	least
short	fast	few	low
short	fast	normal	normal
long	slow	many	normal
long	fast	many	high
long	fast	few	highest

Table 1. Fuzzy rules

5.2 Experiment results

The results generated in this section are based on the simulation experiments set up for 4 × 4, 5 × 5 and 8 × 8 and 10 x 10 nodes moving around in 670*m* × 670*m* area. Nodes move according to the random way-point model (Stallings, W., 2005).

When a node sends out the RREQ packet, 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 neighbor nodes changes. According to the 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 neighbor node, FL-SADOV will choose that one; The relationship between FL-SAODV and AODV is that AODV is a special case of FL-SAODV, where on the route at each next hop, from the source node to the destination node, there is only candidate node.

In our experiments of 10 x 10 nodes, we shown the security level and the overheads of determining the next hop node. Figure 6 shows the security level at each 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).

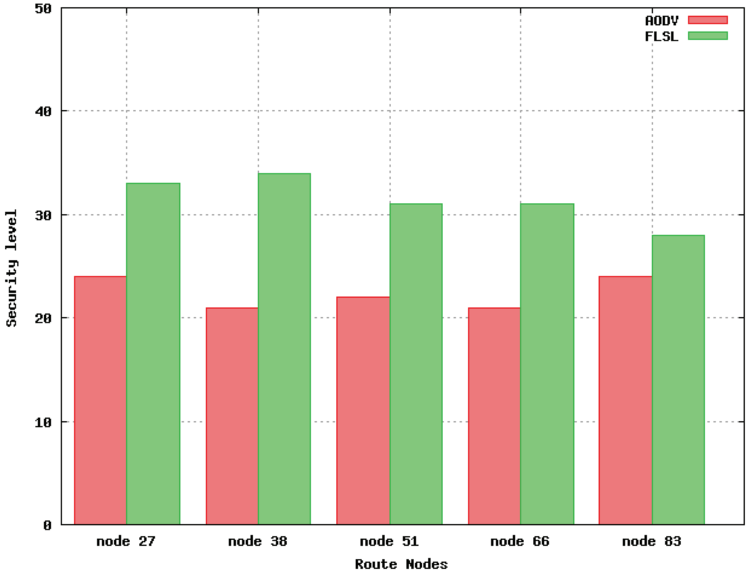

Fig. 6. Security Level on Route Nodes

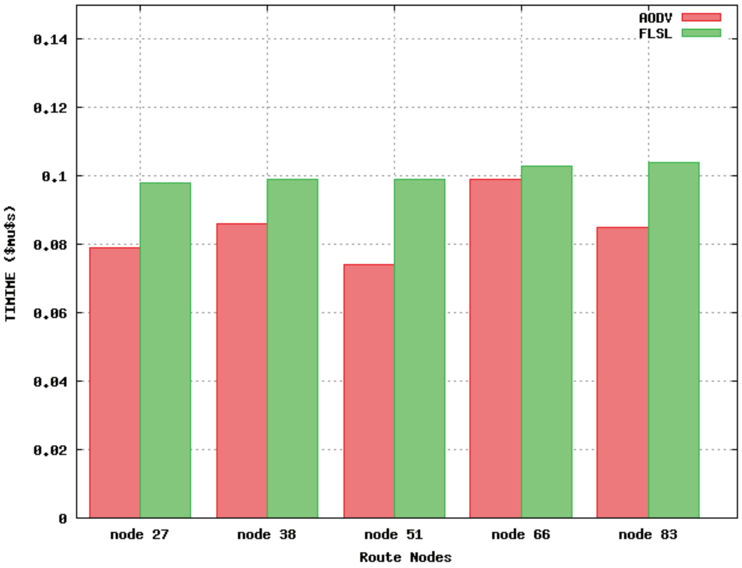

Fig. 7. Times in μs Spent on the Route Nodes

5.3 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 addition but minimum overhead 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 technique: digital signature and hash. This avoids using a CA where other secure routing protocols have to.
- 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 to be the most secure one.

6. Conclusion

In this Chapter, 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 the requirements of secure routing, FL-SAODV, a new secure and efficient routing protocol has been developed. A set of algorithms have been **designed for FL-SAODV.** 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 have higher security level than the route AODV found. In addition, we shown the timings on its 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 neighbor nodes needs more study.

7. References

Charles E. Perkins, E. M. R. & Das, S. R. (2003). Ad hoc on-demand distance vector (AODV) routing, RFC 3561.

D.B. Johnson, D. M. & Hu, Y. (2003). The dynamic source routing protocols for mobile ad hoc networks (DSR).

Hu, Y. C., Perrig, A. & Johnson, D. B. (2002). Ariadne: A secure on-demand routing protocol for ad hoc networks.

Network Research Group, L. B. N. L. (1995). The network simulator NS2, http://www.isi.edu/nsnam/ns.

Stallings, W(2005). Wireless Communications Networks (2nd ed.), Pearson Prentice Hall.

Yih-Chun Hu, D. B. J. & Perrig, A. (2002). Secure efficient distance vector routing in mobile wireless ad hoc networks.

Zapata, M. G. (2004). Secure ad hoc on-demand distance vector (SAODV) routing, RFC 999.