# Performance Comparison of the AODV, SAODV and FLSL Routing Protocols in Mobile Ad Hoc Networks

Lu Jin Zhongwei Zhang
*Department of Mathematics and Computing*
*University of Southern Queensland*
*{jin,zhongwei}@usq.edu.au*

Hong Zhou
*Faculty of Engineering and Surveying*
*University of Southern Queensland*
*hzhou@usq.edu.au*

## Abstract

*Mobile ad-hoc networks operate in the absence of any supporting infrastructure. The absence of any fixed infrastructure in mobile ad-hoc networks makes it difficult to utilize the existing techniques for network services, and poses number of various challenges in the area. The discovery and maintenance of secure route is the most flinty challenge.*

*In this paper, we first deliberate and implement one secure routing protocol FLSL (Adaptive Fuzzy Logic Based Security Level Routing Protocol) and study its performance under different scenarios. Then we carry out a number of experiments using NS-2 to compare the performance of AODV, SAODV and FLSL in terms of security level and routing discovery time under different setups. From these experiments, we can see that FLSL outperforms than AODV and SAODV.*

## 1. Introduction

An ad hoc network is a group of wireless mobile computers (or nodes), in which nodes cooperate by forwarding packets for each other to allow them to communicate beyond direct wireless transmission range. Ad hoc networks require no centralized administration or fixed network infrastructure, and can be quickly and inexpensively set up as needed, such as military exercises and disaster relief. However, secure and reliable communication is a necessary prerequisite for such applications.

In early time, researchers in ad hoc networking have generally studied the routing problems in a non-adversarial network setting, assuming a trusted environment, relatively little research has been done in a more realistic setting in which an adversary may attempt to disrupt the communication. Consequently, current mobile ad hoc networks have no security mechanism, this could possibly lead active attackers to easily exploit or possibly disable the mobile ad hoc network. So far, secure routing protocols emerged but largely relied on the key management, authentication and encryption algorithm. These traditional routing protocols such as SAODV [2], SRP [3] and SAR [4] don't adapt to a higher security level route even if there are a few routing paths, since the security level and selection of route are not part of their normal operations. Therefore, special secure routing protocols, which is security conscious, are needed for mobile ad hoc networks.

In this paper, the implementation of a new security conscious routing protocol, FSLS, is described. The rest of this paper is organized as follows. In Section 2, we provides an overview of AODV, SAODV and FLSL routing protocols. In Section 3, we describe the settings for the simulations and experiments. Results and discussions are presented in Section 4. Conclusions are given in Section 5.

## 2. Protocol Description

In this section, we briefly describe the AODV, SAODV and FLSL routing protocols.

### 2.1. AODV Protocol

The *Ad Hoc on Demand Distance Vector Routing Protocol* (AODV) is a source initiated, on demand driven, routing protocol [6]. Since the routing is on demand, a route is only traced when a source node wants to establish communication with a specific destination. The route remains established as long as it is needed for further communication. Furthermore, another feature of

AODV is its use of a destination sequence number for every route entry. This number is included in the RREQ (Route Request) of any node that desires to send data. These numbers are used to ensure the freshness of routing information. For instance, a requesting node always chooses the route with the greatest sequence number to communicate with its destination node. Once a fresh path is found, a RREP (Route Reply) is sent back to the requesting node. AODV also has the necessary mechanism to inform network nodes of any possible link break that might have occurred in the network [7].

## 2.2. SAODV Protocol

The *Secure Ad hoc On-Demand Distance Vector Routing Protocol* (SAODV) [8] is an extension of the AODV [9] routing protocol that can be used to protect the route discovery mechanism providing security features like integrity, authentication and non-repudiation.

SAODV assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Further, each ad hoc node is capable of securely verifying the association between the address of a given ad hoc node and the public key of that node. Achieving this is the job of the key management scheme.

Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information (the only mutable information in the messages). This is because for the non-mutable information, authentication can be performed in a point-to-point manner, but the same kind of techniques cannot be applied to the mutable information.

Route error messages are protected in a different manner because they have a big amount of mutable information. In addition, it is not relevant which node started the route error and which nodes are just forwarding it. The only relevant information is that a neighbor node is informing to another node that it is not going to be able to route messages to certain destinations anymore.

Therefore, every node (generating or forwarding a route error message) uses digital signatures to sign the whole message and that any neighbor that receives verifies the signature.

## 2.3. FLSL Protocol

The *Adaptive Fuzzy Logic Based Security Level Routing Protocol* (FLSL) [5] is developed basing on SAODV protocol, and security level algorithm has been used to assess the reliability (so-called *Security-Level*)of mobile hosts and determine the most secure route among a few possible routes.

In FLSL, An new attribute, Security Level, is introduced in the format of protocol control messages and routing table to denote the reliability and dependability of certain mobile host or route. Meantime, because FLSL protocol enable the destination node to accept multi-Route Request message, the security level is also used by source node and destination node to determine the most secure route.

In MANET environment, the security-level of a mobile host is affected by many conditions. We have investigated three factors which are irrespective and independent with each other though [10], as follows:

1. Secret key length ($l$). Longer the secret key is, stronger to defend serious brute force attack.

2. Changing frequency of secret key ($f$). If mobile host's secret key is changeable, the difficulty of decryption must be increased and security level of mobile hosts also get enhanced.

3. Amount of active neighbor hosts ($n$). More active neighbor hosts existing will increase the percentage of potential attackers existing.

Apparently, the security level of a single mobile host has a relation with these three factors as follows:

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

The Security-Level of a route is decided by the node which has the lowest Security-Level in that route. In another word, the route with the highest Security-Level is comparably most secure. More precisely, if we define the source node as $S$ and the destination node as $D$ and assume that there are totally $n$ possible routes, i.e. $R_1, R_2, \ldots, R_n$, from the source $S$ to the destination $D$ . In the route $R_i$, there are intermediate nodes $n_1^i, n_2^i, \ldots, n_j^i, \ldots, n_m^i$, totally $m$ possible relay nodes to forward the packets from the source to the destination.

If the current Security-Level of the $j^{th}$ node in the $i^{th}$ route is $S_{ij}$, the Security Level of the $i^{th}$ route is defined as:

$$SL_i = \min(S_{ij}), j \in (1, \ldots, m) \tag{2}$$

The most desired route $R_k$ is the maximum value of all those route [10], i.e.:

$$SL_k = \max_{i \in \{1,2,\ldots,n\}} (SL_i) = \max_{i \in \{1,2,\ldots,n\}} ( \min_{j \in \{1,2,\ldots,n\}} (S_{ij})) \tag{3}$$

Therefore,the FLSL protocol is capable of determining a more secure route among possible routes by comparing the security level while the security level of each individual node is evaluated. The procedures of route discovery is described in Algorithm 1.

**Algorithm 1** FLSL Route Discovery

```
Source node S calculates SL_S and generates RREQ
Source node S broadcasts RREQ to all of its neighbors
while Neighbor node i is not destination node D do
    Authenticate and verify the RREQ
    Calculate node i's security level SL_i
    if SL_i < SL_q then
        Update the security level in the RREQ packet by overwriting
        the SL_q in RREQ with SL_i
    end if
    Broadcast the RREQ to node i's neighbour nodes
end while
for all RREQ messages received by destination node D do
    if There is available route to source node S then
        if SL_q > SL_RT then
            Update routing table using the latest data in RREQ
        else
            Drop the RREQ
        end if
    else
        Create entry in routing table using the latest data in RREQ
    end if
    Increase sequence number by 1
    Create a RREP
    Unicast RREP back to source node S
end for
for all RREP messages received by source node S do
    Update routing table using the latest data in RREP
end for
```

## 3. Simulation and Experiment

In this section, we carry out some experiments using network simulation technology. Our objective is to firstly demonstrate the feasibility of FLSL which can effectively discover a routing and then update the corresponding routing tables on the nodes on route. Another objective is to evaluate performance in the security-level and timing of route discovery.

Up to date, we are not aware of any implementation of SAODV. To this end, we modified some modules in AODV-UU for SAODV by utilizing Libgcrypt library [11].

### 3.1. Experiment Platform Setup

The experiments and simulations are conducted in NS-2 platform[9]. The network topology consists of $(N^2+2)$ nodes, where $N = \{4,5,6,7,8,9\}$. For all sessions, one Constant Bits Rate (CBR) sessions generate UPD packets from node 0 to node $(N^2+1)$. The detailed parameters are shown in Table 1.

**Table 1. Parameters used in experiment scenario**

| Parameter | Value |
|---|---|
| Application traffic | CBR |
| Radio Range | 100 m |
| Packet Size | 512 bytes |
| Maximum speed | 1 m/s |
| Simulation time | 5 minutes |
| Number of nodes | $N^2 + 2, N \in (4,5,6,7,8)$ (Random initial topology) |
| Area | 1000 m 1000 m |

## 4. Results and Discussions

In this section, we test the feasibility of FLSL on NS-2 under different scenarios.

### 4.1. Feasibility of FLSL

Nodes located in random initial topologies.

Figure 1 and 2 show the RREQ and RREP packets transmission route of FLSL protocol in 27 nodes MANET network. The numbered lines indicate the detailed procedures of route discovery. From the simulation, we may observe that the discovered route in FLSL ($N_0 \rightarrow N_2 \rightarrow N_8 \rightarrow N_{25} \rightarrow N_3 \rightarrow N_{13} \rightarrow N_{20} \rightarrow N_{26}$) is different with the route in AODV ($N_0 \rightarrow N_5 \rightarrow N_{23} \rightarrow N_{25} \rightarrow N_{22} \rightarrow N_{13} \rightarrow N_{20} \rightarrow N_{26}$) and in SAODV ($N_0 \rightarrow N_5 \rightarrow N_{23} \rightarrow N_{25} \rightarrow N_{22} \rightarrow N_{13} \rightarrow N_{20} \rightarrow N_{26}$). Figure 3 shows the security level comparison of discovered route between FLSL protocol AODV protocol and SAODV protocol in same topology of 27 random nodes. We may observe that the security level value of final route is 49 in FLSL protocol which is 104.17% higher than 24 in AODV and SAODV protocol.

Figure 4 and 5 show the RREQ and RREP packets transmission route of FLSL protocol in 38 nodes MANET network. The numbered lines indicate the detailed procedures of route discovery. From the simulation, we may observe that the discovered route in FLSL ($N_0 \rightarrow N_{23} \rightarrow N_{25} \rightarrow N_{22} \rightarrow N_{18} \rightarrow N_{20} \rightarrow N_{37}$) is different with the route in AODV ($N_0 \rightarrow N_{23} \rightarrow N_{15} \rightarrow N_3 \rightarrow N_{13} \rightarrow N_{12} \rightarrow N_{20} \rightarrow N_{37}$) and in SAODV ($N_0 \rightarrow N_5 \rightarrow N_{17} \rightarrow N_{25} \rightarrow N_3 \rightarrow N_{13} \rightarrow N_{12} \rightarrow N_4 \rightarrow N_{37}$). Figure 6 shows the security level comparison of discov-

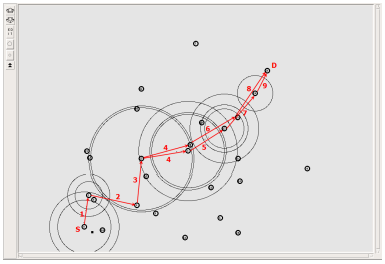

**Figure 1. FLSL RREQ packets transmission (27 random nodes)**

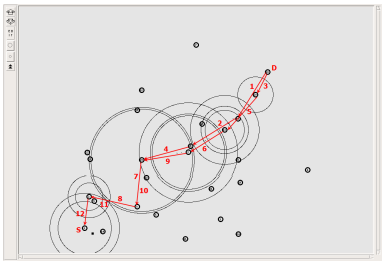

**Figure 2. FLSL RREP packets transmission (27 random nodes)**

ered route between FLSL protocol and AODV protocol in same topology of 38 nodes. The security level value is 24 in FLSL protocol, which is 4.35% increased from 23 in AODV protocol and remain same with in SAODV protocol.

Figure 7 and 8 show the RREQ and RREP packets transmission route of FLSL protocol in 51 nodes MANET network. The numbered lines indicate the detailed procedures of route discovery. From the simulation, we may observe that the discovered route in FLSL ($N_0 \rightarrow N_{46} \rightarrow N_{30} \rightarrow N_{29} \rightarrow N_9 \rightarrow N_{18} \rightarrow N_{20} \rightarrow N_{50}$) is different with the route in AODV ($N_0 \rightarrow N_{43} \rightarrow N_{25} \rightarrow N_3 \rightarrow N_{13} \rightarrow N_{12} \rightarrow N_{37} \rightarrow N_{50}$) and in SAODV

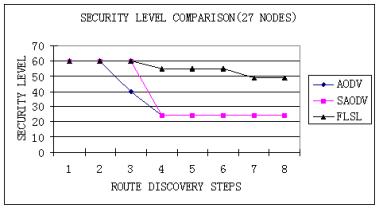


**Figure 3. Security level comparison (27 random nodes)**

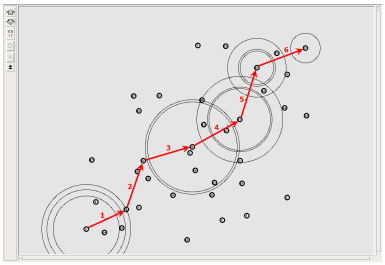

**Figure 4. FLSL RREQ packets transmission (38 random nodes)**

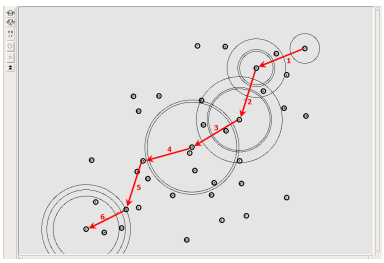

**Figure 5. FLSL RREP packets transmission (38 random nodes)**

($N_0 \rightarrow N_5 \rightarrow N_{35} \rightarrow N_{25} \rightarrow N_3 \rightarrow N_{19} \rightarrow N_{18} \rightarrow N_{12} \rightarrow N_{37} \rightarrow N_{50}$). Figure 9 shows the security level comparison of discovered route among FLSL protocol, AODV protocol and SAODV protocol in same topology of 51 nodes. The security level value is 39 in FLSL protocol, which is 85.71% increased from 21 in AODV protocol and 18.18% increased from 33 in SAODV protocol.

Figure 10 and 11 show the RREQ and RREP packets transmission route of FLSL protocol in 66 nodes MANET network. The numbered lines indicate the detailed procedures of route discovery. From the simulation, we may observe that the discovered route in FLSL ($N_0 \rightarrow N_{41} \rightarrow N_{56} \rightarrow N_{36} \rightarrow N_{13} \rightarrow N_{12} \rightarrow N_4 \rightarrow N_{65}$)

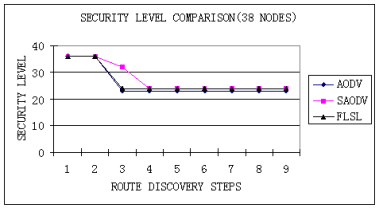


**Figure 6. Security level comparison (38 random nodes)**

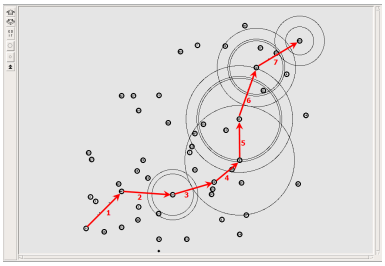

**Figure 7. FLSL RREQ packets transmission (51 random nodes)**

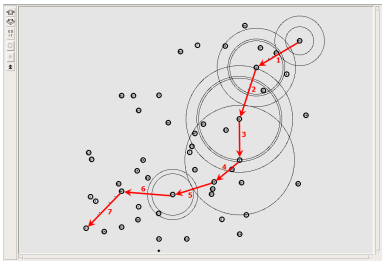

**Figure 8. FLSL RREP packets transmission (51 random nodes)**

is different with the route in AODV ($N_0 \rightarrow N_{57} \rightarrow N_{58} \rightarrow N_{29} \rightarrow N_{13} \rightarrow N_{12} \rightarrow N_8 \rightarrow N_{65}$) and in SAODV ($N_0 \rightarrow N_{43} \rightarrow N_{61} \rightarrow N_3 \rightarrow N_9 \rightarrow N_{18} \rightarrow N_{20} \rightarrow N_{65}$). Figure 12 shows the security level comparison of discovered route among FLSL protocol, AODV protocol and SAODV protocol in same topology of 66 nodes. The security level value is 54 in FLSL protocol, which is 50.00% increased from 36 in AODV protocol and 38.46% increased from 39 in SAODV protocol.

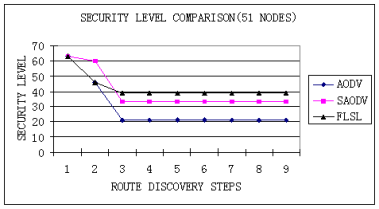


**Figure 9. Security level comparison (51 random nodes)**

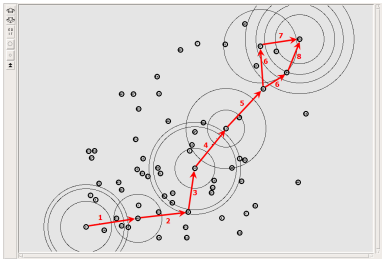

**Figure 10. FLSL RREQ packets transmission (66 random nodes)**

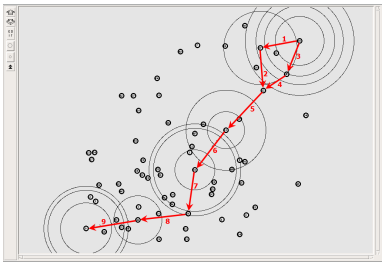

**Figure 11. FLSL RREP packets transmission (66 random nodes)**

### 4.2. The Performance Comparison

Figure 13 and 14 show the performance comparison between FLSL protocol, AODV protocol and SAODV protocol. Two comparison parameters are involved, the security level of final route and the time consumption of route discovery process.

Figure 13 shows the security level of final route for five sessions. In all five sessions, the security level values increase by 4.35%-200.00% from AODV to FLSL, and by 18.18%-200.00% from SAODV to FLSL. This indicates that the implementation of FLSL protocol enable the destination node to select a relatively securer

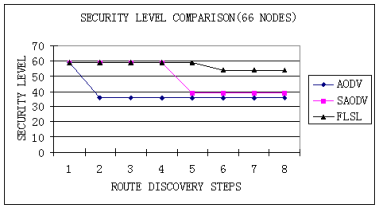


**Figure 12. Security level comparison (66 random nodes)**

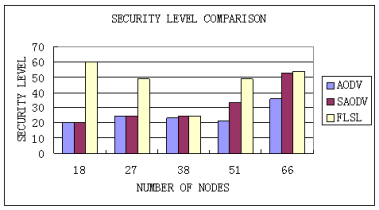


**Figure 13. Security level comparison**

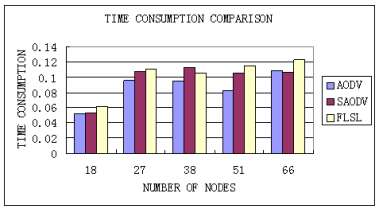


**Figure 14. Route discovery time comparison**

route for data transmission.

Figure 14 shows the time consumption comparison of route discovery processing for the five same sessions. All five sessions show the FLSL protocol consumes more time than in AODV protocol (9.92%-38.50% increases) and SAODV protocol (2.30%-16.43% increases). In the extra consumed time, the fuzzy logic algorithm calculates the security level values, and updates and switches route of the destination node. From the time consumption values of FLSL in five sessions, we may observe that there is an obvious increase with the increase of number of nodes. Each node which receives RREQ/RREP packet has to calculate security level value. More nodes will consume longer time than fewer nodes.

The experiment results showed the FLSL protocol could reliably select the data transmission route with high security level, and self-adaptively and dynamically adjust the route updating without delay. Comparing with AODV and SAODV routing protocols, FLSL spends reasonable and affordable time on security-level algorithm and route selection to improve the reliably and security of MANETs.

## 5. Conclusion

In this paper, we closely studied the current problems of routing protocols in MANET, including the reliability, feasibility, security and performance etc, and developed solutions to those problems. We deliberated and implemented a secure end-to-end protocol, Adaptive Fuzzy Logic Based Security Level Routing(FLSL), which enables the nodes to discover and determine most secure route in MANET. In comparing with AODV and SAODV, the FLSL protocol is capable of determining a more secure route among possible routes.

We also demonstrated the feasibility and the features of FLSL protocol in NS-2 platform. Simulation demonstrated the feasibility of FLSL protocol and the performance of FLSL is comparable but more secure than other secure routing protocols.

## References

[1] Levente Buttyan, Jean-Pierre Hubaux. *"Report on a Working Session on Security in Wireless Ad Hoc Networks"*. Laboratory for Computer Communications and Applications, Swiss Federal Institute of Technology, Switzerland.

[2] M. G. Zapata. *"Secure Ad hoc On-Demand Distance Vector (SAODV) Routing"*. Internet Draft: draft-guerrero-manet-saodv-04.txt 2002. Work in Progcess.

[3] P. Papadimitratos and Z. J. Haas. *"Secure Routing for Mobile Ad hoc Networks"*. Proceedings of the SCS Communication Networks adn Distributed Systems Modeling and Simulation Conference (CNDS 2002), San Antonio, TX, 2002.

[4] S.Yi, P. Naldurg, and R. Kravets. *"Security-aware ad hoc routing for wireless networks"*. ACM Int'l Symp. on Mobile ad hoc networking and computing, 2001

[5] Jing Nie, Xin He, Zheng Zhou, Chenglin Zhao, Feng Lu, Danjing Xie. *"An Adaptive Fuzzy Logic Based Secure Routing Protocol in IPv6 Ad Hoc Networks"*. Processing of Wireless Telecommunications Symposium, Pomona, California, April 28-30, 2005

[6] E.M.Royer, C.K.Toh.*"Ad-hoc On-Demand Distance Vector Routing"*. University of California, Georgia Institute of Technology Internet Draft: draft-ietf-manet-aodv-13.txt 2003. Work in Progcess.

[7] C.E.Perkins, E.M.Royer. *"Ad-hoc On-Demand Distance Vector Routing"*. Sun Microsystems Labratories, University of California, Internet Draft: draft-ietf-manet-aodv-13.txt 2003. Work in Progcess.

[8] Stephen T. Welstead. *Neural Network and Fuzzy Logic Aplications in C/C++*. John Wiley & Sons, June 1994

[9] Francisco L. Ros, Pedro M. Ruiz. *"Implementing a New Manet Unicast Routing Protocol in NS2"*. Dept. of Information and Communications Engineering University of Murcia. December, 2004

[10] Lu Jin, Zhongwei Zhang, Hong Zhou. *"Implementing and Evaluating An Adaptive Secure Routing Protocol for Mobile Ad Hoc Network"*. Wireless Telecommunications Symposium, California, April 27-29, 2006.

[11] Free Software Foundation, Inc. *"Libgcrypt-Cryptographic library"*. January 08, 2005.