Deliberation and Implementation of Adaptive Fuzzy Logic Based Security Level Routing Protocol for Mobile Ad Hoc Network

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

Hong Zhou
Faculty of Engineering and Surveying
University of Southern Queensland
Email: 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 deliberate and implement one secure routing protocol FLSL (Adaptive Fuzzy Logic Based Security Level Routing Protocol) and study its performance under different scenarios. The implementation of FLSL protocol has been carried out by use of NS-2. Various experiments results from simulation verify the protocols, also demonstrate the feasibility of the protocol. A set of experiments under different scenarios have been presented and results of these experiments have been analyzed.

I. INTRODUCTION

In early time, researchers in ad hoc networking have generally studied the routing problems in a non-adversarial network setting, assuming a trusted environment. Consequently, current mobile ad hoc networks have no efficient security mechanism, this could possibly lead active attackers to easily exploit or possibly disable the mobile ad hoc network. 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 II, an adaptive Security-Level algorithm for mobile hosts which is based on fuzzy logic is deliberated. Section II-B describes a new distributed multicast FLSL routing protocol based on the mobile host's Security Level. Section III focus on the implementation of main route selection mechanism and dynamic adjusting of FLSL. Section IV introduces the developing platform, experiment results, analyses the results of FLSL protocol and makes comparison with existing protocols. Conclusions are drawn in Section V.

II. A SECURITY CONSCIOUS ROUTING PROTOCOL FOR MANETS

A. Message Packet Format

FLSL has three kinds of message: Route Request (RREQ), Route Reply (RREP) and Route Error (RERR).

The format of the Route Request/Reply message is illustrated in Figure 1 and 2. The Security Level field is a new inserted field compared with RREQ/RREP messages in AODV protocol[6] and SAODV protocol[2], which indicates the lowest security level of passed-by nodes.

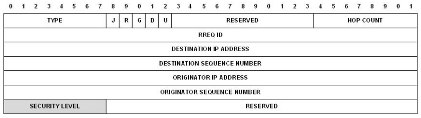


Fig. 1. RREQ packet format in FLSL protocol

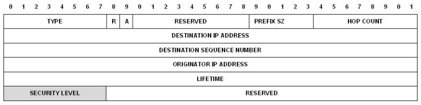


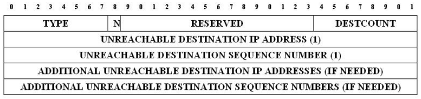
Fig. 2. RREP packet format in FLSL protocol

The format of the Route Error message is illustrated Figure 3. The RERR message is sent whenever a link break causes one or more destinations to become unreachable from some of the node's neighbors.

B. Security-Level of Mobile Host

In MANET environment, the security level of individual mobile host is related closely with the multiple variables. So far, we have investigated three factors which are irrespective and independent with each other though, as follows:

1-4244-0667-6/07/$25.00 ©2007 IEEE
This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2007 proceedings.



TYPE | N | RESERVED | DESTCOUNT

UNREACHABLE DESTINATION IP ADDRESS (1)

UNREACHABLE DESTINATION SEQUENCE NUMBER (1)

ADDITIONAL UNREACHABLE DESTINATION IP ADDRESSES (IF NEEDED)

ADDITIONAL UNREACHABLE DESTINATION SEQUENCE NUMBERS (IF NEEDED)

Fig. 3. RERR packet format in FLSL protocol

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:

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

C. Security-Level Based Routing

As we know, the key component of FLSL protocol is the source-initiated route discovery procedure [10].

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, i.e.:

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

III. Implementation

A. Adaptive Security Level of Mobile Host

According to the Equation (1), We have tried to take advantage of fuzzy logic theory in the modeling of security level of a mobile host in MANETs. The fuzzy membership functions for both of antecedent sets and consequent are set as below [5]:

1) Fuzzy membership function of secret key length (l). Two fuzzy sets, *short* and *long*, are defined in Equation 4.

$$l = \begin{cases} short & \text{the secret key is 40 bits long or less} \\ long & \text{the secret key is 128 bits long or more} \end{cases} \tag{4}$$

2) Fuzzy membership function of changing frequency of secret key (f). Two fuzzy sets, *slow* and *fast*, are defined in Equation 5.

$$f = \begin{cases} slow & \text{the secret key is constant} \\ fast & \text{the secret key is changeable} \end{cases} \tag{5}$$

3) Fuzzy membership function of amount of active neighbor hosts (n). Three fuzzy sets, *few*, *normal* and *many* are defined in Equation 6.

$$n = \begin{cases} few & \text{less than 2} \\ normal & \text{between 2 and 6} \\ many & \text{more than 6} \end{cases} \tag{6}$$

4) Fuzzy membership function of security level of single given mobile host (S). Five fuzzy sets, *lowest*, *low*, *normal*, *high*, and *highest* are defined in Equation 7.

$$S = \begin{cases} lowest & \text{less than 20} \\ low & \text{from 20 to 40} \\ normal & \text{from 40 to 60} \\ high & \text{from 60 to 80} \\ highest & \text{greater than 80} \end{cases} \tag{7}$$

After an investigation and deliberation, we identified the relation between SL and factors that can be described using fuzzy rules and illustrated in Table I:

TABLE I
FUZZY LOGIC SYSTEM RULES

No.	Input			Output
i	l	f	n	S
1	short	slow	few	low
2	short	slow	normal	lowest
3	short	slow	many	lowest
4	short	fast	few	normal
5	short	fast	normal	low
6	short	fast	many	low
7	long	slow	few	high
8	long	slow	normal	normal
9	long	slow	many	low
10	long	fast	few	highest
11	long	fast	normal	high
12	long	fast	many	high

B. Fuzzy Logic Based Security Level Determination

For given input variables l, f, n, there must be a unique membership function associated with each input parameter. Based on the membership function, the membership degree values $F(l)$, $F(f)$, $F(n)$ can be determined [8]. In our implementation of security level rules, the membership degree values should be:

1) for member function l

$$F_i(l) = F_{L-rule_i}(l), i \in \{1, 2, \ldots, 12\} \tag{8}$$

2) for member function f

$$F_i(f) = F_{F-rule_i}(f), i \in \{1, 2, \ldots, 12\} \tag{9}$$

3) for member function n

$$F_i(n) = F_{N-rule_i}(n), i \in \{1, 2, \ldots, 12\} \tag{10}$$

Moreover, the weighting factor , W_i, for each entry of current rules should be:

$$W_i = \min\{F_i(l), F_i(f), F_i(n)\}, i \in \{1, 2, \ldots, 12\} \quad (11)$$

By computing the logical product of the membership weights for each active rule, a set of fuzzy output, S_i, response magnitudes are produced by using Equation 12.

$$S_i = F_{S-rule_i}(W_i), i \in \{1, 2, \ldots, 12\} \quad (12)$$

Finally, all that remains is to combine and defuzzify these output responses [10]. The single mobile host's security level can be computed by:

$$SL = \frac{\sum_{i=1}^{12} W_i S_i}{\sum_{i=1}^{12} W_i} = \frac{W_1 S_1 + W_2 S_2 + \ldots + W_{12} S_{12}}{W_1 + W_2 + \ldots + W_{12}} \quad (13)$$

C. Route discovery in FLSL

The route discovery processing in FLSL protocol consists of 4 steps.

a) stage 1: Route discovery process to locate the peer node. The source node (SN) disseminates a route request (RREQ) to broadcast address. The Security-Level of RREQ is equal to the originator node's Security-Level. The Hop Count field is set to zero. Then the RREQ packet will be broadcasted to originator node's neighbors.

b) stage 2: When an intermediate node receives the RREQ from its neighbor, the intermediate node firstly authenticates RREQ. And then compare its current Security-Level value with the one contained in RREQ, and updates the Security-Level of RREQ with the minimum value, which is the latest Security-Level of route. Meanwhile, a route entry which points to the originator node of RREQ packet is created in the intermediate node's routing table.

c) stage 3: Once the RREQ has arrived the destination node (DN), the node (DN) generates route reply (RREP) packet for the RREQ packet which indicates new originator or has higher security level than current route, and unicasts RREP back to the neighbor from which it received the RREQ. Like RREQ, the RREP packet also includes Security Level field, as introduced in Figure 2.

d) stage 4: When an intermediate node receives the RREP from its neighbors, it first increases the hop count value in the RREP by one. If the Destination Sequence Number contained in the RREP is less than the existing Destination Sequence Number in the node's routing table, the RREP will be dropped silently.

IV. Simulation and Experiment

A. Experiment Platform Setup

NS-2 is used for the simulation experiments[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 UDP packet size is 512 bytes. The simulation time for each session is 10 minutes and the transmission range of each node is 100m.

B. Feasibility of FLSL

Nodes located in random initial topologies.

Figure 4 and 5 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 6 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.

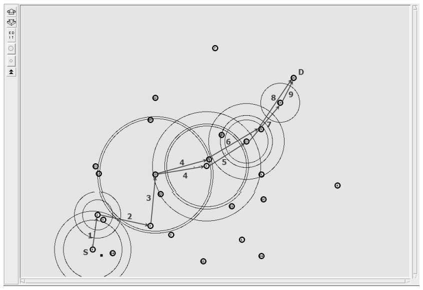


Fig. 4. FLSL RREQ packets transmission (27 random nodes)

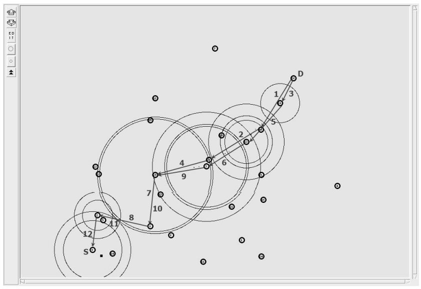


Fig. 5. FLSL RREP packets transmission (27 random nodes)

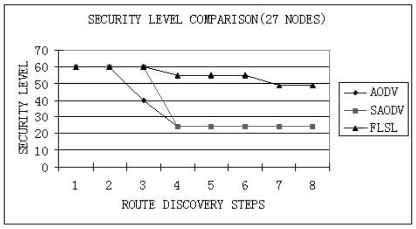


Fig. 6. Security level comparison (27 random nodes)

Figure 7 and 8 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 9 shows the security level comparison of discovered 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.

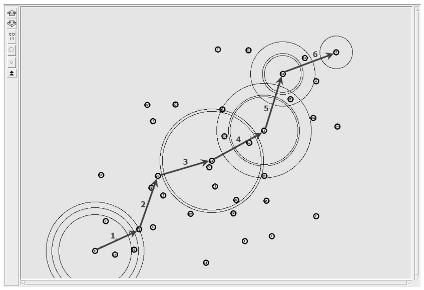


Fig. 7. FLSL RREQ packets transmission (38 random nodes)

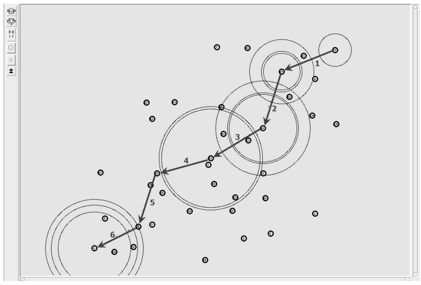


Fig. 8. FLSL RREP packets transmission (38 random nodes)

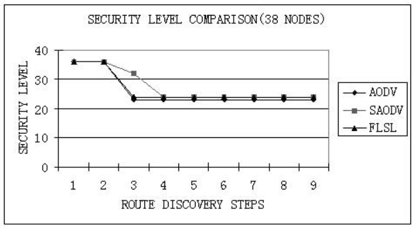


Fig. 9. Security level comparison (38 random nodes)

Figure 10 and 11 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 ($N_0 \rightarrow N_5 \rightarrow N_{35} \rightarrow N_{25} \rightarrow N_3 \rightarrow N_{19} \rightarrow N_{18} \rightarrow N_{12} \rightarrow N_{37} \rightarrow N_{50}$). Figure 12 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.

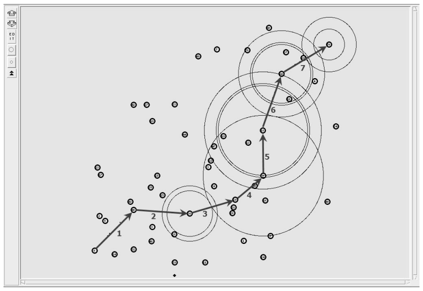


Fig. 10. FLSL RREQ packets transmission (51 random nodes)

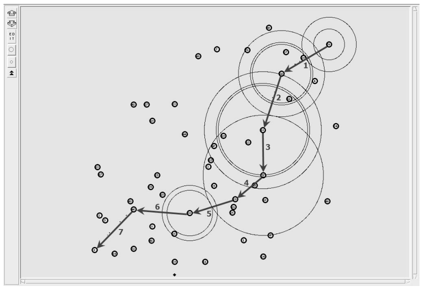


Fig. 11. FLSL RREP packets transmission (51 random nodes)

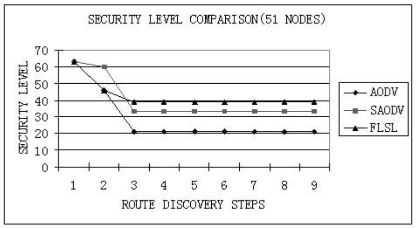


Fig. 12. Security level comparison (51 random nodes)

C. The Performance of FLSL

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.

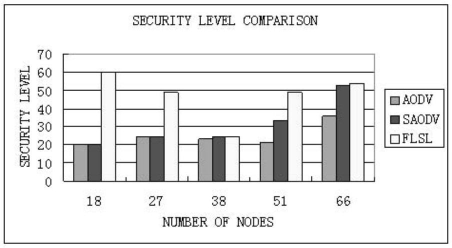


Fig. 13. Security level comparison

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 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.

V. Conclusion

In this paper, 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. 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 by using Artificial Intelligent techniques.

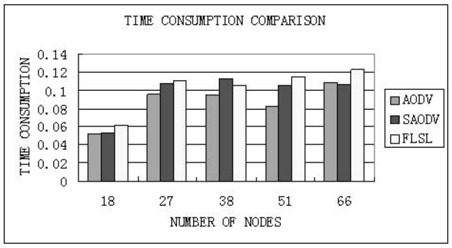


Fig. 14. Route discovery time comparison

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.

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, and Hong Zhou. ”Implementing and Evaluating An Adaptive Secure Routing Protocol for Mobile Ad Hoc Network”. Wireless Telecommunications Symposium, Pomona, California, April 27-29, 2006.