Secure Dynamic Gateway to Internet Connectivity for Ad-hoc Network

Jinhua Zhao[1], Ling Wang[1], Yoohwan Kim[2], Yingtao Jiang[3], Xiaozong Yang[1]

[1] Department of Computer Science and Technology, Harbin Institute of Technology, Harbin, China, 150001.
[2]Department of Computer Science, Univ. of Nevada, Las Vegas, USA.
[3]Department of Electrical & Computer Engineering, Univ. of Nevada, Las Vegas, USA.

{zjh, lwang}@ftcl.hit.edu.cn, yxz@hit.edu.cn,
yoohwan@cs.unlv.edu, yingtao@egr.unlv.edu

Abstract

Mobile ad hoc networks (MANETs) are autonomous, infrastructureless networks that support multi-hop communication through IP routing. MANET and the Internet have many differences, which are not only the structure and topology of the networks, but also communication patterns of nodes in both of the networks. It is challenging for MANET to access the Internet due to these differences. There are two different kinds of accessing modes, i.e., single fixed gateway and multi-gateway where the load-balancing overhead may reduce the network performance. In this paper, we make three contributions: 1) The concept of dynamic gateway, which acts as an interface between MANET and the Internet, is proposed. 2) The load-balancing problem is considered on the dynamic gateway for ad-hoc Internet connectivity. 3) secDSDV protocol is proposed to enhance security performance for the networks. Our simulation results show that the performance of networks with dynamic gateways is superior to that of fixed gateway architecture. Compared with DSDV, secDSDV does not affect the performance of the networks.

Keyword: Dynamic Gateway, Internet, Load-balancing, Ad Hoc Network, Security.

I. Introduction

An ad-hoc network is a network where a group of mobile computers want to establish network communication with each other using compatible wireless communication devices. Mobile Ad hoc network (MANET) is an infrastructureless network without any fixed routers. A MANET can be defined as a set of mobile nodes that agree upon forming a spontaneous, temporary network without any infrastructure or any form of centralized administration [1]. Mobile nodes, which want to communicate with each other over a wireless communication medium, act as both routers and hosts to forward packets to everyone.

At present, most work concerning ad-hoc networking has been concentrated on stand-alone ad-hoc networks. Not much work has been done concerning the integration of ad-hoc networks and Internet. This integration of MANET and the Internet allows MANET nodes, which may not be able to access the Internet directly, to share the Internet connection.

However, MANET and Internet have many incompatible features. These differences are not only the structure and topology of networks, but also communication protocol of nodes in both networks. In this paper, we propose *the dynamic gateway* concept that acts as an interface between MANET and the Internet. These dynamic gateways can use Mobile IP [13] for communicating with the Internet and DSDV (Destination Sequenced Distance Vector) [14] for interacting with MANET. The load-balancing problem is considered for the *dynamic gateway* architecture. Furthermore, this paper investigates the security issues in the dynamic gateway architecture proposed in our earlier paper [26]. To resolve the security challenges, DSDV authenticated secure routing protocol (secDSDV) is proposed in MANET. This secure dynamic gateway solution should not only improve the performance of network but also increase the security of the routing on the networks.

This paper is organized as follows. Section II presents the dynamic gateway concept, optimize policy, and how to overcome the problem of load-balancing. Section III describes an authenticated routing protocol for ad-hoc Internet connectivity. Section IV describes simulations and performance evaluated. Section V offers concluding remarks.

II. The Dynamic Gateway Strategy

A. The Dynamic Gateway

The existing approaches for integrating MANET and Internet are summarized in this section.

In [9], Lei and Perkins have proposed a method to construct ad-hoc networks and provide Internet access for MANET nodes. A routing protocol is used within MANET, a modified Routing Information Protocol (RIP), to interconnect the ad-hoc network with the Internet.

Sun *et al.* [19] have proposed an approach, which enables the cooperation of AODV and Mobile IP to guarantee ad-hoc Internet connectivity. While AODV is used to discover and maintain the routes within MANET, Mobile IP provides the mobile nodes with the *care-of addresses*. However, handoff occurs only if either a mobile node has not heard from its foreign agent for more than one beacon interval, i.e., the time between two successive agent advertisements, or when its route to a foreign agent has become invalid.

In [3], Broch *et al.* proposed a mechanism for the integration of MANET and Internet with Mobile IP. They introduce the concept of border router (or gateway), which has two interfaces.

The one connected to the Internet uses normal IP routing to send packets in and/or out MANET, while the interface connected to MANET uses the dynamic source routing (DSR) protocol to route packets within MANET.

Ratanchandani and Kravets [17] proposed a hybrid approach, which makes use of Mobile IP to provide global Internet connectivity. Certain techniques such as TTL scoping of agent advertisements, eavesdropping and caching agent advertisements were used. The Time-To-Live (TTL) field is used to reduce the flooding of agent advertisements in MANET.

However, all the above existing approaches consider only fixed gateways, but not dynamic multi-gateway. The dynamic gateway is one type of the multi-gateway, which it uses MANET node as gateway and optimizes the gateway according to distance, number of nodes registered, and quantity of communication. The concept of the dynamic gateway is proposed, that is the gateways are mobile and the number of gateways is variable. The gateway nodes act as gateways in one time period, but they do not be gateways in another time period according to the criterion of the gateway selection.

As shown in Fig .1, ad–hoc mobile nodes (MN) access Internet source through dynamic gateway, foreign agent (FA) supply Internet connectivity to dynamic gateway. Any interaction between MANET nodes and Internet has to be provided by only dynamic gateways (GW).

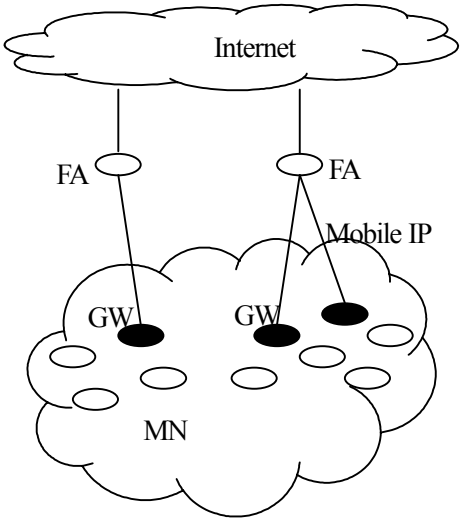

Fig.1 MANET with Internet Connectivity

A dynamic gateway is a MANET node with an extended capability, which is one hop away from foreign agent. Thus, dynamic gateway motion is limited to the coverage area of foreign agents. When a dynamic gateway moves out of one hop away from foreign agent, it becomes a normal MANET node, but not a dynamic gateway. These dynamic gateways can use Mobile IP when they communicate with the Internet, and use DSDV when they interact with MANET.

The dynamic gateway provides transparent service for MANET nodes. Although many foreign agents helping dynamic gateway supply Internet connectivity for MANET nodes, no MANET nodes are aware of the details, which is so-called transparency. We discuss two types of transparency, connection transparency and handoff transparency. With connection transparency, the MANET nodes do not realize which foreign agent is indirectly supplying the Internet connectivity. Selecting an optimal foreign agent and supplying transparent service for MANET nodes are the main tasks of dynamic gateway. With, handoff transparency, a dynamic gateway should switch foreign agent from one to another not affect the interaction of MANET nodes. MANET nodes do not consider that which dynamic gateway is connected to.

Hence we define this architecture as dynamic gateway. The dynamic gateway has several advantages:

- First, it eliminates the need for additional fixed gateways, reduces the system complexity, improves reliability, and lowers the cost.
- Second, because dynamic gateway movement causes the routes to be updated frequently, it is beneficial for the network to exchange data and improve performance.
- Third, dynamic change of gateway magnitude, which is determined by network environment such as MANET nodes locations and magnitude, and gateway load etc., eliminates the network congestion.
- Fourth, dynamic handoff is available. That is, with change of network environment, MANET nodes automatically switch to the optimal gateway, and the dynamic gateway can also switch to the optimal foreign agent.
- Fifth, the problem of load-balancing for multi-gateway can be overcome.
- Sixth, being peer-to-peer architecture, it has neither a centralized gateway nor centralized algorithm. Therefore, dynamic gateways are able to adapt to variety of MANET nodes.

B. Operation of the Dynamic Gateway

Assume that every MANET node, including dynamic gateways, holds a routable IP home address, and a MANET node, called S, wants to access a global Internet node, known as correspondent node, say D. This access is processed as follow:

A dynamic gateway registers with a foreign agent in the following sequences. As foreign agents broadcast *agent advertisements* (FAAdv) (TTL=1 hop [17]) periodically, a dynamic gateway can make a choice among many agent advertisements according to an optimize policy. Then, the dynamic gateway unicasts the registration request. A foreign agent accepts the registration of a dynamic gateway if it does not register with this foreign agent or previous registration has expired.

A MANET node "S" selects an optimized dynamic gateway. Node S initiates a *gateway solicitation* (GWSol) and broadcasts GWSol through MANET. After dynamic gateways, which are currently present in MANET, received the GWSol, they should unicast a *gateway advertisement* (GWAdv) to node S. Only dynamic gateways registered with a foreign agent could send back a GWAdv packet. Thus, dynamic gateways not yet registered with foreign agents ignore this request packet.

Figure 2 shows GWAdv message formats. GWAdv has some fields, such as gateway's IP address, GWAdv's lifetime, which node S would be able to register with dynamic gateway deadline, the number of MANET nodes (NN) registered with this dynamic gateway, the length of the queue for waiting to deliver data packets (QL), the distance (DS) between this dynamic gateway and the MANET node, i.e. hops, and a sequence number to uniquely identify GWAdv.

When node S receives all GWAdv packets, which are sent back by all dynamic gateways, it selects an optimized gateway according to the formula in section C, denotes as GW. Then it

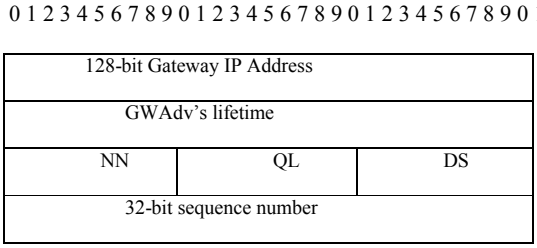

Fig.2 GWAdv message format

registers with "GW" by sending back a *gateway registration request* (GWReq) packet to "GW", and receiving a *gateway registration reply* (GWRep). The GWRep includes GW's IP address, which will be node S's *care-of address*. GWRep has a registration lifetime, the period of time where node S may access the Internet through the "GW". When a registration lifetime has expired, the corresponding MANET node needs to update its registration. Many MANET nodes may register with the same gateway if only its registration is valid .

After node S registers with the "GW", any interaction with the Internet goes through this "GW". When node S sends data packets to node D, the data packets will have to reach "GW" using DSDV routing protocol. Then the foreign agent, "GW" has registered with, delivers these data packets to final correspondent node D using Mobile IP protocol.

C. Selection Formula of the Dynamic Gateway

Dynamic gateway, providing Internet connection with MANET nodes, must register with a foreign agent and in the same manner, the MANET nodes accessing Internet must register with dynamic gateways. Several definitions are given in selecting the best dynamic gateway.

Definition 1 Node number (NN): An effective number of MANET nodes registered with a dynamic gateway or an effective number of dynamic gateways registered with a foreign agent is defined as their load NN.

Definition 2 Queue length (QL): The waiting queue length of data packets on dynamic gateway and foreign agent is defined as load QL.

Definition 3 Distance (DS): The Euclidean distance between two nodes is also defined as load DS.

A dynamic gateway would select a the least loaded foreign agent. Similarly, a MANET node would select a the least load dynamic gateway. To accommodate the different weights of each factor on network communication, three factors are considered, i.e., the Distance (DS), the registered number of nodes (MN) and the queue length (QL) of data packet delivered. Depending on the actual conditions of the network environment, the weight values can be adjusted.

The formula of the MANET nodes and dynamic gateway is given as,

$$GWExp = DS \times n + NN \times m + QL \times k \tag{1}$$

$$GW = Min\{GWExp_1, GWExp_2, ..., GWExp_j\} = Min\{GWExp_i\}_{i=1}^{j} \tag{2}$$

$$n + m + k = 1 \tag{3}$$

Where *n, m, k* are weighted factors, *GWExp* represents the weighted value of gateway, and *i* refers to the number of gateway advertisement (GWAdv) that a MANET node receives. Likewise, the formula for the dynamic gateways and foreign agent is given as,

$$FAExp = DS \times n + NN \times m + QL \times k \tag{4}$$

$$FA = Min\{FAExp_1, FAExp_2, ..., FAExp_j\} = Min\{FAExp_i\}_{i=1}^{j} \tag{5}$$

$$n + m + k = 1 \tag{6}$$

Where *FAExp* represent the weighted value of foreign agent and *i* indicates the number of foreign agent advertisement (FAAdv) that a dynamic gateway receives.

In both cases, the weights *n*, *m*, *k* can be adjusted depending on the network conditions, i.e. MANET network scale, geographic environment, foreign agent quantity and channel conditions, etc. Here, *n*, *m*, *k* are set as 0.74, 0.2, and 0.06, respectively.

D. Load-balancing of the Dynamic Gateway

Load-balancing is a critical problem when MANET nodes access the Internet using multi-gateway. The network performance can be improved if the gateways are well load- balanced.

Traditionally this problem has been solved by "Cluster Control" technique (as seen in Fig. 3), which works as followings. When there are information exchange between MANET nodes and the Internet, three steps are performed.

- First step, a gateway with fewer loads is chosen to complete information exchange by the mission deployment controller.
- Second step, the gateway chosen broadcasts gateway advertisements.
- Third step, the MANET node, which wants to interact with Internet, gets to gateway advertisements and then registers with the gateway chosen.

In this "cluster control technique", the route is established in a top-down manner. Mission is deployed on the gateway by the mission deployment controller, then the gateway controls MANET node. Therefore, the gateway and MANET node can complete the mission passively. The whole system is controlled by the mission deployment controller, which increases the complexity of the system and slows down the system capability. The mission deployment controller can become a bottleneck of the system and worsen the performance of the network.

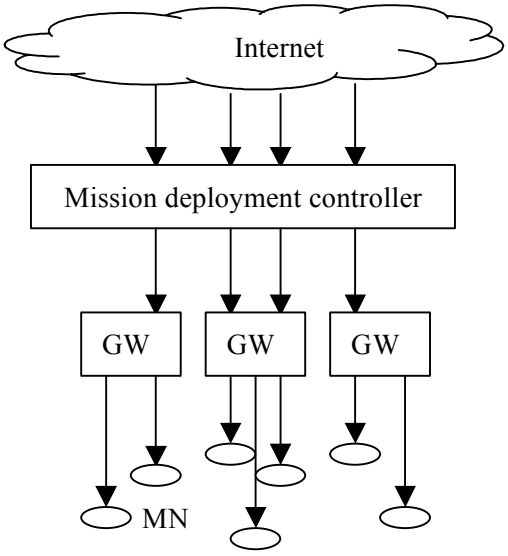

Fig.3 Top-down Mission deployment

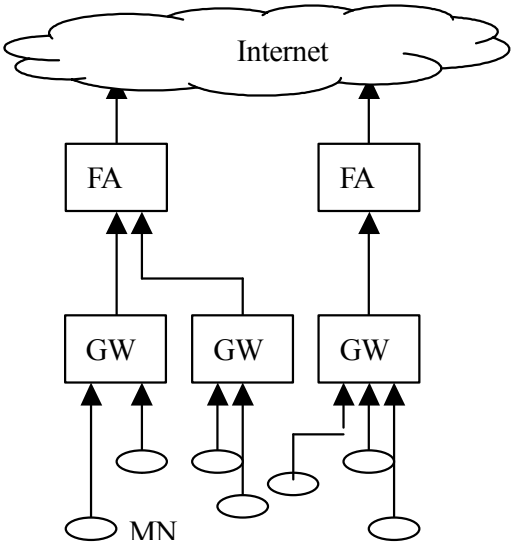

Fig.4 Bottom-up free choice

Compared to the conventional method, our proposed dynamic gateway architecture can achieve load-balancing automatically. The dynamic gateway strategy solves the bottleneck of "Cluster Control" technique. It works in a bottom-up manner (See Fig. 4), which is opposite to the traditionally way. Different to the gateway chosen by controller in the cluster control technique, MANET nodes freely choose the gateway with fewer load and shorter distance, and the gateways freely choose foreign agent with less load and distance. In this way, the gateway with the least load gets the new mission and the gateway's load is well balanced. Each choice made

by the MANET node or the gateway is optimal at the moment. After operating for some time, all foreign agents and gateways are well load-balanced automatically, and the whole system enters into an optimal stage. In dynamic gateway architecture, route is created in a bottom-up way, and the mission is deployed automatically, therefore it's easier and more efficient to control and implement the load-balancing of gateways.

From above analysis, we can observe that MANET nodes choose the gateway with the least load, and gateways choose the foreign agent with the least load. The system will adjust the load-balancing of each gateway and foreign agent automatically.

III. Secure Routing Protocol on Dynamic Gateway

A. Secure Ad-Hoc Routing

Wireless ad hoc networks are used to support dynamic scenarios where no wired infrastructure exists. Most ad-hoc routing protocols are cooperative by nature [18], and rely on implicit trust-your-neighbor relationships to route packets among participating nodes. This naïve trust model allows malicious nodes to paralyze an ad-hoc network by inserting erroneous routing updates, replaying old routing information, changing routing updates, or advertising incorrect routing information [12]. While these attacks are possible in fixed networks as well, the nature of the ad-hoc environment magnifies their effects, and makes their detection difficult [25].

In a MANET, two security issues need to be addressed: one is to protect transmitted data which can be done through end-to-end protection. The other is to make the routing protocol secure. This is particularly challenging for MANETs with dynamically changing topologies.

As noted earlier, a majority of the proposed routing protocols assume non-hostile environments, where nodes faithfully forward packets, and malicious nodes are absent. Thus, MANETs are extremely vulnerable to attacks due to their dynamically changing topology and open medium of communication. To address these concerns, several secure routing protocols have been proposed: SAODV [25], SRP[16], SAR[22], CSER[11], SEAD[7].

The SAODV (Secure Ad hoc On-demand Distance Vector Routing) protocol [25] is an extension of AODV [14]. The SRP (Secure Routing Protocol) [16] guarantees that fabricated, compromised, or relayed route replies would either be rejected or never reach back the querying source. The SAR (Security-Aware Routing) protocol [22] incorporates security attributes as parameters in route discovery. The CSER (Cooperative Security Enforcement Routing) protocol [11] allows a path consisting of multiple segments, each starting and ending by nodes from the same security domain as the source node. The middle of each segment can

contain untrusted nodes. A secure proactive routing protocol based on DSDV called SEAD [7], which is also based on public-key signed hash chains.

B. Authenticated Routing Protocol

Authenticated routing for ad-hoc networks (ARAN) is a routing protocol proposed by Kimaya Sanzgiri et al. [20]. ARAN protocol uses "public-key cryptographic mechanisms" to defeat all identified attacks. Inspired by this approach, secDSDV protocol is proposed to secure ad-hoc Internet connectivity as our dynamic gateway is based on DSDV protocol. In the secDSDV, "cryptographic certificates mechanisms" is used to authenticate DSDV route protocol.

Table 1 Variables and Notations

K_{M+}	Public key of node M.
K_{M-}	Private key of node M.
C_M	Certificate of node M.
IP_M	IP address of node M.
REQ_id	Route Request Packet identifier.
REP_id	Reply packet identifier.
RUP_id	Route Update packet identifier.

SecDSDV contains three operations: authenticated route discovery, authenticated route setup, and authenticated route maintenance. Fig. 6 shows an example of the whole process. Variables and notations are shown in Table 1. Steps from ? to ? indicate the process of authenticated route discovery, and steps from ? to ? indicate the process of authenticated route setup. The last step, ? , indicates route maintenance. In fig.6, larger circles represent mobile nodes with the inner character indicates the node id. Line between two nodes indicates that these two

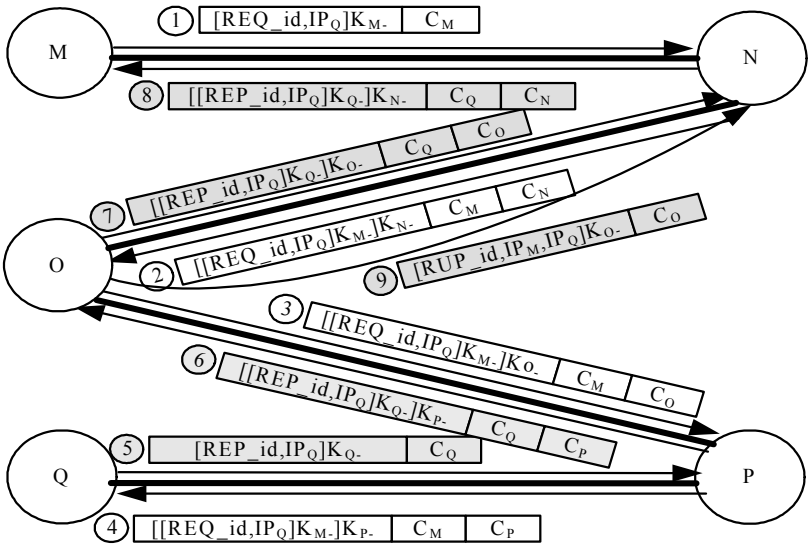

Fig. 6 Process of authenticated routing

nodes can communicate with each other directly. Single-headed arrow between two nodes indicates a packet transmission with the node pointed by the arrow as the receiver. The table adjacent to a single-head arrow represents the content of the transmitted packet. Packets indicated by white tables are transmitted in broadcast mode, while those indicated by gray tables are transmitted in unicast mode. For example, the white table with content "[[REQ_id, IP_Q]K_{M-}]K_{N-}, C_M, C_N" indicates that node M is broadcasting a route request packet, which contains three fields. The first field contains packet type identifier ("REQ_id") and the IP address of the destination (IP_Q), all signed with node M's private key. The second field contains the certificate of the source that initiates the route discovery process. The last field contains the sender's certificate. Numbers before the tables indicates the order of the corresponding packet transmissions.

1) Authenticated Route Discovery

Step1 When a path to node Q is required, the source node *M* starts a route discovery process by broadcasting a route request packet (REQ) to its neighbors. Since the packet is only signed by node M and not encrypted, the content of the packet is readable publicly.

Step2 When node N receives the REQ packet sent by node M, node O validates the signature for node M and sets up a reverse path back to node M by recording the neighbor M from which it received the REP. Then, node N signs the first field of the received REQ, appends its own certificate, and broadcasts the modified REQ packet to all its neighbors.

Step3 When receiving the forwarded REQ packet from node N, node O validates the signatures for both node M and node N using the certificates in the REQ packet. Node O then removes node N's certificate and signature, signs the contents of the message originally broadcasted by node M and appends its own certificate, and then broadcast the new REQ packet.

Step4 Similarly, node P forwards the REQ packet further.

2) Authenticated Route Setup

Step5 When receiving the REQ packet sent by node P, the destination, node Q, unicasts a reply (REP) packet to node *P*.

Step6 Node P signs the REP packet, appends its own certificate, and then unicast the packet to the next hop towards the source node.

Step7 Similarly, Node O forwards the REP packet further.

Step8 Node N forwards the REP packet to the source node *M*.

Till now, a secure path to destination Q is found. With authenticated route discovery and authenticated route setup, a source believes that the node that initiates the corresponding authenticated route setup process is indeed the intended destination.

3) Authenticated Route Maintenance

To maintain routing tables, each node will transmit a routing update packet to each of its neighbor routers periodically. Routing update packets contain the information from the sender's own routing table. For example, node O will transmit its routing update packet, shown step ? in Fig.6. This packet is forwarded along the path toward the source with modification.

IV. Performance Evaluation

A. Simulation Environment and Scenarios

There are the following four performance measures studied [8]:

- *Packet* delivery *fraction is the ratio of the amount of data packets delivered to the destination* and *total number of data packets sent by source.*
- *Average end-to-end delay (ms) measures the average time between the sending of the data packet and its receipt at its final destination.*
- Aggregate *throughput (bits/s) is the fraction of the amount of data received by the destinations and the interval of time between the first and last data packets sent.*
- Overhead *(packets) is the amount of control packets in the network for the operation of secDSDV or DSDV and Mobile IP.*

As shown in the Figure 7, simulation environment is set as 20 nodes distributed over a

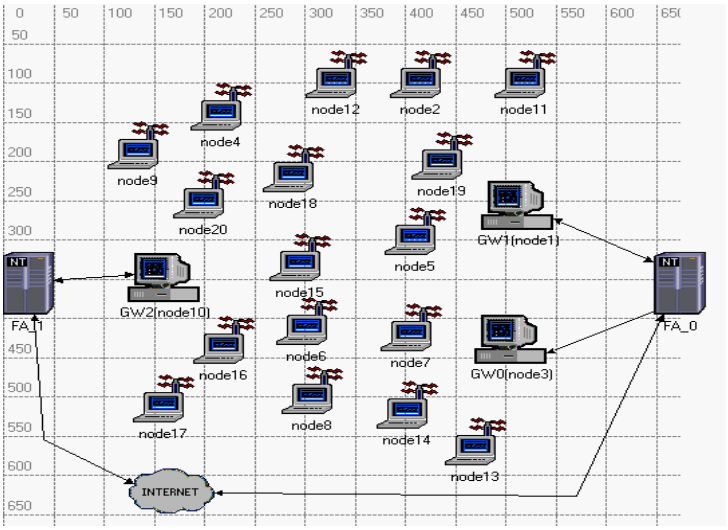

Fig. 7 Simulation Environment

$670m \times 670m$ square simulation area and a wired Internet with two foreign agents. The two foreign agents are located at the left and right borders of a simulation area. The initial positions of the nodes were random. Node mobility was simulated according to the random waypoint mobility model. The node does not discriminate one direction of motion [9], and its transmission range was 200m. We ran simulations for constant node speeds of 0,1,5,and 10 m/s, with the pause time is consistently 30 seconds. Mobile nodes communicate with correspondent nodes(CN) using constant bit rate (CBR) source traffic. The CBR data packets are 512 bytes and the sending rate is 5 packets per second. Network simulator OPNET is used.

In this experiment, there are 6 MANET nodes accessing Internet source. We consider using DSDV and secDSDV protocol in MANET. The MANET nodes move randomly over their simulation area for 900 seconds of simulated time. According to [17], a beacon interval [10, 15] would guarantee high connectivity and low overhead. There are some corresponding parameters in the following Table 2.

TABLE 2 Experiment Parameters

	GW	FA
Gateway's registration lifetime	--	20s
MANET node's registration lifetime	20s	--
Advertisement lifetime	20s	20s
Beacon times	10s	10s
Time between two solicitation	5s	5s

B. Simulation Result and Analysis

As shown in Fig. 8, the packet delivery fraction obtained using DVDS is closer to that obtained using secDSDV in all scenarios. It can be concluded that secDSDV is highly effective in discovering and maintaining routes for delivery of data packets.

When there is one dynamic gateway, packet delivery fraction obtained using DVDS and secDSDV is 82% and 84%, respectively. When the number of dynamic gateways reaches to 10, the packet delivery fraction obtained using DVDS and secDSDV is 95% and 93%, respectively. That is, with the increasing of the number of dynamic gateway, both the percentages of data delivered to destination increase for these two protocols. It proves that this mobility of dynamic gateway makes routes between MANET nodes available and avoids unnecessary wait time, when it is used to hold a data packet until a route to its destination is found. Thus, the presence of dynamic gateway prevents data packets dropping, reducing the average time for a data packet to reach its final destination.

Fig.9 shows aggregate overhead using two routing protocol in packets, the overhead of secDSDV is significantly higher than one of DSDV. And their overheads increase with the

increase of the number of dynamic gateway. When there are 5 dynamic gateways, their overhead is down 15000 packets, then when the number of dynamic gateways reaches to 10, secDVDS's overhead is 20000 packets and DSDV's overhead is 17000 packets, respectively. This indicates that control packets are increased with the increase of the number dynamic gateway. In addition, secDSDV has higher overhead due to the increased exchange of Mobile IP and secDSDV control messages.

Fig. 10 shows that the average end-to-end delay for secDSDV is higher than that for DSDV. The reason is that each node has to verify the digital signature of the previous node, and then replace this with its own digital signature, and perform cryptographic operations when processing secDSDV control packets

The average end-to-end delay using secDSDV and DSDV is nearly 50ms and 30ms at one dynamic gateway, respectively. When the number of dynamic gateways reaches to 5, the average end-to-end delay using secDSDV and DSDV decreases to 38ms and 19ms, respectively. Then average delay keeps stable after the number of dynamic gateway is greater than 5. Although more control packets lead to the increase of the delay, the transmission of data packet through multi-gateway causes the decrease of the delay. Therefore, the total delay for the multi-gateway does still not change.

The aggregated throughput graphs are approximately close for the two protocols, as shown in Fig. 11. When the number of dynamic gateways is 1, the throughout using secDSDV and DSDV is 26500 bits/s and 29000 bits/s, respectively. When the number of dynamic gateways reaches to 10, the throughout using secDSDV and DSDV increases to 30000 bits/s and 32000 bits/s, respectively. This indicates that the increase of the number of dynamic gateway has little effect on the throughput as the throughput is determined by the average delay, which does not change greatly.

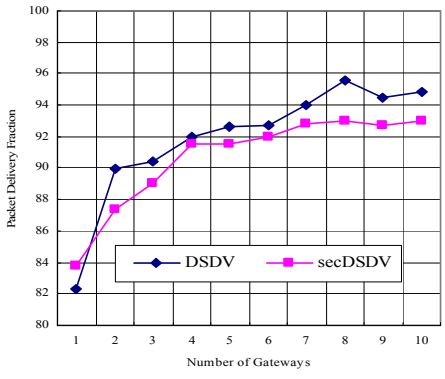

Fig. 8. Packet delivery fraction (670m×670m).

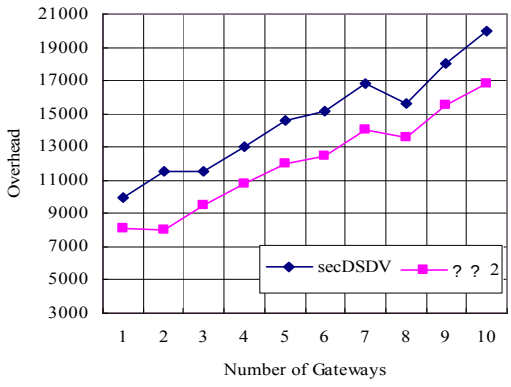

Fig.9. Average overhead (670m×670m).

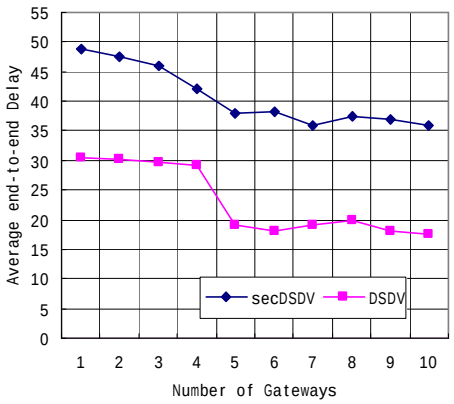

Fig. 10. Average end-to-end delay (670m×670m)

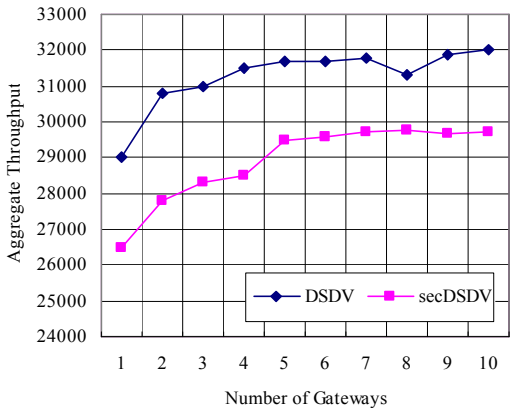

Fig. 11. Aggregated throughput (670m×670m)

V. Conclusions

This paper has presented load-balancing strategy and security routing protocol for a multi-gateway architecture called dynamic gateway. Due to the fact that the gateways are mobile and the number of gateways is variable, the gateway nodes may or may not act as gateway according to formula of the dynamic gateway. We have proposed a optimize approach to select an optimal gateway and a foreign agent. The dynamic gateway strategy could overcome the problem of load-balancing for multi-gateway. To ensure secure operation, we have proposed secDSDV authenticated routing protocol. The simulation result shows that the secure dynamic gateway architecture exhibits superior performance with higher throughput and shorter delay to fixed gateway architecture.

VI. References

[1] H. Ammari and H. E1-Rewini, Integration of Mobile Ad Hoc Networks and the Internet Using Mobile Gateways, Proceedings of the 18th International Parallel and Distributed Processing Symposium, 2004, pp.218-225.

[2] J. Broch, D. Maltz, D. Johnson, Y. Hu, and J. Jetcheva, A Performance Comparison of Multi-Hop Wireless Ad Hoc Network Routing Protocols, Proceedings of the Fourth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Dallas, Texas, USA, October 25-30, 1998, pp.85-97.

[3] J. Broch, D. A. Maltz, and D. B. Johnson, Supporting Hierarchy and Heterogeneous Interfaces in Multi-Hop Wireless Ad Hoc Networks, Proceedings of the Workshop on Mobile Computing, Perth, Australia, June 1999.

[4] M. Gasser, A. Goldstein, C. Kaufman, and B. Lampson, The digital distributed systems security architecture, In Proceedings of the 12th National Computer Security Conference,

NIST, 1989, pp.305-319.

[5] C. Kaufman. DASS: Distributed authentication security service, Request for Comments September 1993, pp.1507.

[6] Y. Hu, A. Perrig, and D. Johnson, Ariadne: A Secure On-Demand Routing Protocol for Ad-Hoc Networks, The 8th ACM International Conference on Mobile Computing and Networking, 2002.

[7] Y. Hu, D. Johnson, and A. Perrig, SEAD: Secure Efficient Distance Vector Routing In Mobile Wireless Ad-Hoc Networks, Fourth IEEE Workshop on Mobile Computing Systems and Applications (WMCSA 02), June 2002, pp. 3 – 13.

[8] U. Jonsson, F. Alriksson, T. Larsson, P. Johansson, and G. Q. Maguire Jr, MIPMANET - Mobile IP for Mobile Ad Hoc Networks, The First IEEE/ACM Annual Workshop on Mobile Ad Hoc Networking and Computing (MobiHOC 2000), Boston, Massachusetts, USA, August 11, 2000, pp.75—85.

[9] P. Johansson, T. Larsson, N. Hedman, B. Mielczarek, and M. Degermark, Scenario-based Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks, Proceedings of the 5th Annual ACM/IEEE International Conference on Mobile Computing and Networking (MobiCom'99), Seattle, Washington, USA, August 15-19, 1999, pp.195-206.

[10] H. Lei and C. Perkins, Ad Hoc Networking with Mobile IP, Proceedings of the Second European Personal Mobile Communications Conference (EPMCC'97), Bonn, Germany, September 30-October 2, 1997.

[11] B. Lu and U. pooch, Cooperative Security-Enforcement Routing in Mobile Ad-Hoc Networks, The 4th International Workshop on Mobile and Wireless Communications Network, 2002.

[12] S. Marti, T. Giuli, K. Lai and M. Baker, Mitigating Routing Misbehavior in Mobile Ad-Hoc Networks, In The Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Boston, MA,USA, Aug. 2000.

[13] C. Perkins, Mobile IP: Design Principles and Practices, Addison-Wesley Wireless Communications Series, 1998, 12(6), pp.5-5.

[14] C. Perkins and P. Bhagwat, Highly Dynamic Destination-Sequenced Distance Vector (DSDV) Routing for Mobile Computers, ACM SIGCOMM Symposium on Communications, Architectures and Protocols, September 1994, pp. 234-375.

[15] C. E. Perkins and E. M. Royer, Ad-Hoc On-Demand Distance Vector Routing, Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, 1999.

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

[17] P. Ratanchandani and R. Kravets, A Hybrid Approach to Internet Connectivity for Mobile Ad Hoc Networks, Proceedings of IEEE Wireless Communications and Networking Conference (WCNC), New Orleans, Louisiana, USA, 16-20 March, 2003, pp.1522-1527.

[18] E. M. Royer and C-K Toh, A Review of Current Routing Protocols for Ad-Hoc Mobile Wireless Networks, IEEE Personal Communications, Apr. 1999.

[19] Y. Sun, E. Belding-Royer, and C. Perkins, Internet Connectivity for Ad hoc Mobile Networks, International Journal of Wireless Information Networks, Special Issue on Mobile Ad Hoc Networks (MANETs): Standards, Research, Applications, April 2002.

[20] K. Sanzgiri, B. Dahill, B. N. Levine, C. Shields, and E. M. Belding- Royer, A Secure Routing Protocol for Ad Hoc Networks, in Proceedings ICNP, Nov. 2002, pp. 78–87.

[21] J. J. Tardo and K. Algappan, SPX: Global Authentication Using Public Key Certificates, In Proceedings of the IEEE Symposium on Security and Privacy, IEEE Computer Society, Oakland, California, May 1991, pp.232-244.

[22] 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.

[23] L. Zhou and Z. J. Haas, Securing Ad Hoc Networks, IEEE Network Magazine, November/December 1999, vol. 13, no.6.

[24] Y. Zhang and W. Lee, Intrusion Detection in Wireless Ad-Hoc Networks, In The Sixth Annual ACM/IEEE International Conference on Mobile Computing and Networking, Boston, MA,USA, Aug. 2000. PP. 275 – 283.

[25] M. G. Zapata, Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, Internet Draft: draft-guerrero-manet-saodv-00.txt, 2002, Work in Progress.

[26] Jinhua Zhao, Xiaozong Yang, and Hongwei Liu, Load-balancing Strategy of Multi-gateway for Ad-hoc Internet Connectivity, International Conference on information Technology: Coding and Computing (ITCC'05) - Volume II, Las Vegas, Nevada, USA, 04 - 04, 2005.

Jinhua Zhao received the M.S. degree in computer science from the National University of Defence Technology, Changsha, China, in 1995. He is currently working towards the Ph.D. degree in the Department of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. His research interests include MANET, mobile computing, wireless communications.

Ling Wang is an Associate Professor at the Department of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. She received Ph.D. degree from Electrical and Computer Engineering Department at the University of Nevada, Las Vegas in 2003. Her research interests include, VLSI CAD, and Ad Hoc Network.

Yoohwan Kim is an Assistant Professor at Department of Computer Science at the University of Nevada, Las Vegas. He received Ph.D. degree from Case Western Reserve University in 2003. His research interests include switch design, network traffic measurement, and network security.

Yingtao Jiang is an Assistant Professor at Department of Electrical & Computer Engineering at the University of Nevada, Las Vegas. He received Ph.D. degree from the University of Texas, Dallas in 2001. His research interests include VLSI design and wireless communications.

Xiaozong Yang is a senior member of IEEE and a professor at the Department of Computer Science and Technology, Harbin Institute of Technology, Harbin, China. His current research area is focused on mobile computing, fault tolerant computing, and software reliability.