A Dynamic Load Sharing Mechanism in Multihomed Mobile Networks

Seongho Cho, Jongkeun Na and Chongkwon Kim
School of Electrical Engineering and Computer Science, Seoul National University
San 56-1, Shilim-dong, Kwanak-ku, Seoul, 151-742, Korea
Email: {shcho, jkna, ckim}@popeye.snu.ac.kr

Abstract—An entire network can be managed as a single mobility entity when it moves as a unit. To support Network Mobility (NEMO), a mobile router has been introduced to manage the mobility of whole nodes inside the network. In this mobile network, multiple Mobile Router (MR)s and Home Agent (HA)s scenarios are considered to provide reliability and load sharing. In this paper, we present a neighbor MR authentication and registration mechanism in multihomed mobile networks. Also, using registered MRs, we propose a HA-based dynamic load sharing mechanism. Using measured latency from periodic Binding Update (BU) messages, the HA shares traffic load with an alternative tunnel. Our proposed mechanism requires no additional signaling messages except some options in the BU message.

I. INTRODUCTION

Mobile data communication is increasingly prevalent with local area wireless networks based on the IEEE 802.11 standard. Also, Personal Area Network (PAN), Car Area Network (CAN), and transportation systems (e.g. bus, train, and airplane) will have permanent connectivity to the Internet even during movement. From these mobile data services, various types of IP-based services, such as seamless data service, real-time health care, and remote car repair, are possible.

For these mobile communication environments, the new mobility management problem has been considered to treat a network itself as a single moving entity. However, the existing node mobility management protocols, like Mobile IP (MIP) protocols [1], [2], cannot support the network mobility because the mobility service should be transparently provided to every node inside the network. To support this kind of network mobility, a Network Mobility (NEMO) Basic Support protocol [3] has been proposed. The NEMO Basic Support protocol is the protocol extension of Mobile IPv6 (MIPv6) [2].

A mobile network consists of one or more Mobile Router (MRs) and local or visiting nodes. The MR operates both as the Mobile Node (MN) of MIPv6 and as the location updater of the NEMO protocol. Using the Prefix Scope Binding Update (PSBU) of the NEMO protocol, the MR registers the attachment point of the network. Besides, the MR operates bi-directional tunneling with the Home Agent (HA), encapsulation and decapsulation of IP-in-IP packets, and ingress filtering. Therefore, the MR is the essential service node in the mobile network.

Considering the importance of the MR, multihomed mobile networks [4], [5] are discussed in the IETF NEMO Working Group [6]. Various types of multihoming scenarios are considered. The MR, an interface of the MR, Mobile Network Prefix (MNP), and the HA are components of multihoming. From this multihoming, ubiquitous access, fault recovery, load sharing, and bi-casting can be obtained [5]. For fault tolerance, MRs or HAs are duplicated to recover the link failure or the node failure. To provide the load balancing among MRs or HAs, traffics can be shared through several MR-HA tunnels of the same mobile network. Also, simultaneous transmission through different tunnels can minimize loss or delay for real-time communication.

In this paper, we propose a HA-based dynamic load sharing mechanism in multihomed mobile networks. To provide this HA-based solution, registered neighbor MR-HA tunnels and measured MR-HA tunnel latency are required. First, we present a dynamic neighbor MR authentication and registration mechanism. We analyze security problems of multihomed mobile networks and propose an authentication and registration mechanism simply using the Return Routability procedure [2] of MIPv6. It is highly desirable for MRs to be equipped with the automatic neighbor MR discovery and dynamic neighbor MR registration method for more flexibility even though MRs can be manually configured by the network administrator.

Also, we propose a dynamic load sharing mechanism using registered neighbor MRs. As a load sharing metric, our proposed mechanism measures tunnel latency using periodic Binding Update (BU)/Binding Acknowledgement (BACK) messages and the HAHA protocol [7]. From measured tunnel latency, the HA can share traffic load with the neighbor MR-HA tunnel.

The rest of the paper is organized as follows. Section 2 introduces multihomed mobile network scenarios with multiple MRs and HAs. Also, we describe main characteristics of these scenarios. Section 3 analyzes security problems of above multihomed mobile network and proposes the neighbor MR authentication and registration mechanism. Section 4 classifies load sharing mechanisms in multihomed fixed networks. In Section 5, we propose the HA-based dynamic load sharing mechanism using MR-HA tunnel latency. Section 6 shows simulation results of the proposed mechanism. In Section 7, we conclude our results and present some future research issues.
III. THE NEIGHBOR MR AUTHENTICATION AND REGISTRATION MECHANISM

In this section, we introduce possible attack cases in multihomed mobile networks. And we also present the new procedure of the neighbor MR discovery, authentication and registration.

A. Possible Attack Scenarios

Typically, Denial-of-Service (DoS) attacks, redirection attacks and replay attacks are possible. First, the MR can be exposed to various DoS attacks. Because the MR has mobility, the access link is usually the wireless channel. Therefore, simple channel jamming can make a network service unavailable. And, the DoS attack for the service availability of the MR can be a severe attack because the MR is the main service component of mobile networks.

Second, several types of redirection attacks can be possible in multihomed mobile networks. In the situation of the MR failure, the MR-HA tunnel can be broken. To preserve a previous active session, tunneling through the neighbor MR or nested tunneling through neighbor MR-HA tunnel is required. If there exists no authentication between MRs, the fake MR acts as a neighbor MR and redirects packets maliciously. In this case, various attacks, like privacy violation, redirection for cryptographic analysis, redirection for DoS attack stream, and stream redirection are possible.

Also, the sub-network with the MR has mobility. Therefore, the neighbor MR information can be stale after the sub-network moves away. A malicious MR can reuse previous binding information for attacking the previous mobile networks. This kind of replay attack can cause privacy violation, redirection attacks, and DoS attacks.

B. The Neighbor MR Authentication and Registration Mechanism

Considering above security problems, we present our neighbor MR authentication and registration mechanism. Our mechanism consists of neighbor MRs discovery, neighbor MR authentication and neighbor MRs registration.

Neighbor MRs discovery is based on the Router Advertisement (RA) message [8]. Each MR should broadcast the RA message periodically at the foreign network. By listening Router Advertisement (RA) messages on the ingress interface, the MR can get information of neighbor MRs. This RA message can be initiated from the explicit Router Solicitation (RS) message. The root MR which is at the visiting network should respond to this RS message from the ingress interface. And, the RA message should contain its own Home Address (HoA) and Mobile Network Prefix (MNP) as an option. From this neighbor discovery process, the MR can acquire neighbor MR’s information, like the HoA, CoA, and MNP.

The MR authenticates the neighbor MR after discovering a neighbor MR. Because the MR operates both as the MN of MIPv6 and the MR of NEMO Basic Support protocol, the MR can initiate the Return Routability procedure with the neighbor MR as the MN of MIPv6. Using the Home Test and Care-of

II. RELATED MULTIHOMING SCENARIOS OF MOBILE NETWORKS

The multihoming analysis draft [4] classifies multihomed mobile networks using \((x, y, z)\) notation. Variables \(x, y,\) and \(z\) respectively mean the number of MRs connected to the Internet (so called root MRs), the number of HAs, and the number of Mobile Network Prefix (MNP)s. In case of 1, each variable implies that there exists a single node or prefix. If the variable is N, then it means that one or more agents or prefixes exist in a single mobile network. From different combinations of the 3-tuple \((x, y, z)\), various types of multihoming scenarios are possible. For example, the \((N, 1, 1)\) scenario means there are multiple MRs at the mobile network, but all of MRs are managed by single HA and use same MNP.

In this paper, we focus on multiple MRs and HAs scenarios, like \((N, N, 1)\) or \((N, N, N)\) cases. Figure 1 shows a typical example of multihomed MRs and HAs scenario. If the mobile network visits the foreign network, each MR obtains Care-of-Address (CoA) from the Access Router (AR), and registers its own CoA and MNP to its own HA using periodic PSBU messages. The MNP can be either single or multiple. From this process, each MR makes the bi-directional tunnel with its own HA. This tunnel is called as the MR-HA tunnel.

Each MR has the Secure Association (SA) with its own HA by sharing the secret key. From this SA, packets are protected through the MR-HA tunnel. However, each MR may not share the pre-defined SA because the composition of mobile network can be dynamically changed. For example, a European inter-city train is composed of several wagons with different destinations. And, each wagon can be divided or reunited at the intermediate station by its destination. If the wagon has its own MR, sub-mobile networks join or leave dynamically.

Fig. 1. An Example of the Multiple MRs and HAs Scenario
The MR can authenticate its own HoA and CoA to the neighbor MR. After the mutual Return Routability procedure, each MR can authenticate neighbor MRs. This procedure is proven to be secure in the MIPv6 draft [2].

The MR registers neighbor MRs with the BU message after the above authentication procedure. With an option noted as the Neighbor MR Registration Option [9], the MR registers acquired (HoA, CoA, MNP) pairs of neighbor MRs to its own HA. This registration is periodically repeated by the BU message. From this periodic registration, the HA can keep the current neighbor MRs list. Because the HA can obtain authenticated neighbor MRs information, the fake MR cannot redirect packets. Also, periodic BU messages protect the false binding request from the MR conducting a replay attack.

Figure 2 shows the whole procedure of our neighbor MR authentication and registration mechanism in the configuration like Figure 1. $MR_1$ discovers the presence of $MR_2$ from the neighbor discovery procedure with the RS and RA message. $MR_1$ initiates the Home Test Init and Care-of Test Init message of the Return Routability procedure. After the mutual Return Routability Procedure, $MR_2$ authenticates all the discovered neighbor MRs. And $MR_2$ sends the BU messages to $HA_2$ with the Neighbor MR Registration Option. Likewise, $MR_1$ can register $MR_2$ to $HA_1$.

IV. RELATED WORK

In multihomed fixed networks, several solutions for load sharing have been proposed. Typically, there exist Border Gateway Protocol (BGP)-based solutions [11], [12] and Network Address Translation (NAT)-based solutions [13], [14] at a network layer. For an application level solution, the Domain Name Service (DNS)-based mechanism [15] also exists.

BGP-based solutions provide multiple links between enterprise networks. Each BGP peer allocates multiple IP address prefixes for the other enterprises. Load sharing can be obtained from the different routing for different IP address prefixes. This BGP-based routing can be either static or dynamic. In case of static routing [11], aggregated traffics are mapped to a predefined prefix and routed by the IP address prefix. The dynamic mechanism [12] measures latency, loss rate, throughput, or link utilization and distributes traffics by the link condition. To distribute traffic load, dynamic solutions require the BGP routing update. Therefore, dynamic BGP-based solutions can experience heavy routing overhead.

NAT-based solutions distribute traffic load through multiple links. Each link has own public IP address. The IP address of a connection is translated from a private address to a public address. If the outbound connection is allocated to one link, the inbound traffic of this connection returns back through the same link. Also, NAT-based solutions can be static or dynamic. Static load sharing [13] can be done by selecting the public IP address of a connection from the hash result of the private IP address. For dynamic load sharing [14], the least loaded link is selected by translating the corresponding IP address. However, NAT-based solutions have a scalability problem to keep the IP address translation mapping. And some applications cannot be served from the NAT solution.

For the application level load sharing, DNS-based redirection [15] can be used in server selection. This mechanism can select the least loaded or closest server to the client and decide the TTL value by the load or latency. However, there also exists the scalability problem and the DNS server can be the bottleneck of load sharing.

Above solutions are too heavy to apply to mobile networks. Because the attachment point of a mobile network changes frequently, a dynamic and scalable load sharing solution for multihomed mobile networks is required.

V. A DYNAMIC LOAD SHARING MECHANISM

In this section, we present the HA-based Dynamic Load Sharing Mechanism using registered neighbor MRs. We use latency as a metric to share traffic load dynamically. It is known that the latency-based load sharing is more effective than the throughput-based load sharing [14]. Compared to latency, the measured throughput is inaccurate because of the severe fluctuation of measured throughput. Especially, the HA can easily measure the MR-HA tunnel latency using the BU message. Also, it can obtain neighbor tunnel latency and measure latency between the HA and neighbor HA by the HAHA protocol [7]. We introduce a latency measurement method by the HA and a load sharing algorithm based on measured tunnel latency.

A. Latency Measurement

To provide load sharing, the HA should know the latency of its own MR-HA tunnel and alternative MR-HA tunnels. Especially, to obtain latency of the alternative MR-HA tunnel, both neighbor MR-HA tunnel latency and neighbor HA-HA latency are required. We explain how to measure tunnel latency from BU/BACK messages and the Binding Information Update message of the HAHA protocol. The HAHA protocol can be used to implement the virtual home network or to share the information between HAs.

First, the HA measures own MR-HA tunnel latency from periodic BU/BACK messages. The HA can specify the lifetime of the BU message with the Lifetime field of a BACK message. This Lifetime field can be used as the offset of BU messages. The MR transmits the BU message with the timestamp option.
After receiving the BU message with the timestamp option, the HA can calculate the current MR-HA tunnel latency from the specified lifetime, previous timestamp, and current timestamp. The $i$th measured latency $C(i)$ is shown as

$$C(i) = [T_{BU}(i) - T_{BU}(i-1)] - O(i)$$  \hspace{1cm} (1)

where $T_{BU}(i)$ is the $i$th timestamp of the BU message and $O(i)$ is the offset between the $i$th BU message and the $(i-1)$th BU message.

To obtain fine-grained latency, we can send BU messages with shorter lifetime value. However, this BU message exchange experiences severe overhead because the BU message should be encrypted. To measure the tunnel latency more frequently, the "tunnel heartbeat" message [4] can be used. If there exists no data packets between the HA and the MR, small probe packets are exchanged. By transmitting probe packets with a fixed interval, the latency measurement is easier than by the BU message. Using this heartbeat message, the HA can also measure the fine-grained tunnel latency with the fixed offset using Eq. (1).

From the measured latency $C(i)$, the HA calculates the exponential moving average using Eq. (2), where $L(i)$ is the $i$th moving average and $\alpha$ is the weight for current latency.

$$L(i) = (1 - \alpha)L(i-1) + \alpha C(i)$$  \hspace{1cm} (2)

Second, the HA can measure the latency $L_k(i)$ with the $k$th neighbor HA from the $i$th HAHA protocol. Like the BU message, the timestamp option of the HAHA protocol can be used to measure latency. After receiving the BU message with the Neighbor MR Registration Option from the MR, the HA sends the Binding Information Request message with the timestamp option to the HA of the neighbor MR. The neighbor HA replies with the Binding Information Update message with the timestamp option. The HA can measure the latency with the $k$th neighbor HA from the difference of timestamps of the Request and Update message. Using Eq. (2), the average latency $M_k(i)$ and $N_k(i)$ of the $k$th HA at the $i$th time can be obtained. And the neighbor MR includes the measured average latency $N_k(i)$ of the $k$th neighbor MR-HA tunnel in the $i$th Binding Information Update message. Then, the HA measures the average latency $M_k(i) + N_k(i)$ through the alternative MR-HA tunnel.

### B. Load Sharing Algorithm

For whole $N$ neighbor, $k$th MR-HA tunnel which satisfies $\min_{k \in N}(M_k(i) + N_k(i))$ is selected. We define the load sharing benefit ratio $R_k(i)$ of the current tunnel and the $k$th tunnel at the $i$th time. The ratio $R_k(i)$ is shown as

$$R_k(i) = \frac{L(i)}{p_c L(i) + p_k (M_k(i) + N_k(i))}$$  \hspace{1cm} (3)

where $p_c$ is the weight for the current tunnel and $p_k = 1 - p_c$ is the weight for the $k$th tunnel. From Eq. (3), if the ratio $R_k(i)$ is greater than $\beta$, then the HA shares the traffic with the $k$th neighbor MR-HA tunnel as much as $p_k$ times.

From this algorithm, the HA can dynamically share the traffic load through the neighbor MR-HA tunnel. Because the HA can share the traffic load without updating the routing table, our proposed load sharing mechanism can adapt to the network mobility faster than BGP-based solutions. Also, our proposed mechanism requires no additional operation entity and no additional signaling messages. Therefore, our mechanism is more adequate and scalable to the multihomed mobile network compared to NAT-based solutions.

### VI. Simulation Results

In this section, we describe experiments to evaluate the performance of our proposed load sharing mechanism. Based on the ns-2 network simulator [16], we implement MIPv6 and NEMO functionality of the MR, HA, and MN. The MR sends the PSBU message with timestamp option to its HA. And the HA measures the MR-HA tunnel latency using the Eq. (1) and (2). Also, the HA measures latency through the neighbor MR-HA tunnel using the HAHA protocol. The MN automatically configures its MR and it has mobility function.

Our experiments use a simulation topology shown in Figure 3. Each link has 2Mbps bandwidth and 5 ms propagation delay. We have also conducted simulations with other link bandwidth and propagation delay; the results are similar. $CN_1$, $CN_2$, and FN are fixed nodes and $MN_1$ and $MN_2$ are mobile network nodes. $HA_1$ and $HA_2$ are the HA of $MR_1$ and $MR_2$, respectively. And $HA_2$ is the HA of $MN_1$ and $MN_2$. Correspondent nodes, $CN_1$ and $CN_2$, have five FTP connections over five TCP session with mobile network nodes, $MN_1$ and $MN_2$, respectively. And FN has a CBR (Constant Bit Rate) traffic over UDP session with $MN_2$.

To compare load sharing benefit, we set an ON/OFF CBR traffic which consumes the bandwidth of the $HA_2\text{-}MR_2$ tunnel. We set the mean ON time to be 1 second, and the mean OFF time to be 2 seconds. In our experiments, we varied the sending rate of the CBR traffic from 75% to 95% during the ON time. Also, we use the static routing to exclude the routing effect to the load sharing mechanism.

The whole simulation time is 20 seconds. TCP traffics are generated just after simulation started. And the CBR traffic

![Fig. 3. Simulation Topology](image-url)
starts to generate after 3 seconds to find the load sharing effect after TCP steady-state saturation. From intensive experiments, we select the $\alpha$ and $\beta$ value of Eq. (2) and (3) as 0.05 and 0.8, respectively. Also, the load shared traffic ratio, $p_1$ and $p_k$ are selected as 0.5. Here, five TCP connections are shared through the neighbor $MR_1-HA_1$ tunnel.

Figure 4 shows the average throughput of TCP connections as the network load increased by CBR traffic. The x-axis shows the percentage of CBR traffic load during the ON time. Figure 4 shows that the network load degrades TCP throughput on the congested link. However, in case of load shared TCP connections, the average throughput of whole connections increases because both load shared TCP connections and congested TCP connections gets throughput gains. In case of 95% ON time load of the CBR traffic, the average throughput of congested TCP connections with our load sharing mechanism achieves more than 50% that of congested TCP connections without any load sharing mechanism.

Figure 5 shows average inter-packet latency as the network load increases. As the network load increases, average inter-packet delay also increases. However, load shared TCP connections experience less inter-packet delay compared to non-load shared TCP connections.

VII. CONCLUSION

In multihomed mobile networks, multiple MRs and HAs scenarios have been considered to provide fault recovery, load sharing and bi-casting. In this paper, we present a neighbor MR authentication and registration mechanism in multihomed mobile networks. We also propose the HA-based dynamic load sharing mechanism using registered MRs. The proposed mechanism is a scalable solution for mobile networks without any additional signaling message. Also, our proposed solution can provide security properties based on the proven Return Routability procedure. From the simulation, we show that our load sharing mechanism improves TCP throughput of the congested link through the neighbor MR-HA tunnel detour.

For the future work, we consider a route optimized tunneling method. Current tunneling-based load shared path can be inefficient by the triangular routing because the current NEMO basic support protocol cannot support route optimization. However, after adopting route optimization in the NEMO basic support protocol, more efficient load sharing based on our mechanism is also possible without significant modification. Evaluation for route optimized scenarios is our future work.

REFERENCES


Fig. 4. Average Throughput of TCP Connections

Fig. 5. Average Inter-packet Latency of TCP Connections