International Journal of Control and Automation
Vol. 9, No. 6 (2016), pp.359-364
http//dx.doi.org/10.14257/ijca.2016.9.6.34

Adaptive Transmission Control based Secured Multimedia Data Traffic Distribution Scheme over Integrated Wireless Networks

Ronnie D. Caytiles, and Byungjoo Park*

Department of Multimedia Engineering, Hannam University
133 Ojeong-dong, Daeduk-gu, Daejeon, Korea
*rdcaytiles@gmail.com, bjpark@hnu.kr**
**Correspondent Author: Byungjoo Park* (bjpark@hnu.kr)*

Abstract

Flow mobility distribution for mobile devices is essentially important for IP-based environments in order to efficiently manage the load of data traffic. For Heterogeneous hierarchical mobility management protocol, the load of traffic is concentrated on the mobility anchor point (MAP) for it acts as the central controller for all connecting mobile devices. Whenever, the MAP handoff is breached, the entire operation that goes through the MAP is compromised. This paper deals with the analysis of a secured distribution of traffic load within the MAP domain over hierarchical mobility management environments. The overview of hierarchical mobility management will be discussed as well as securing the flow control signaling scheme will be introduced in order to determine and ensure the optimized flow of traffic, considering the amount of traffic that every MAP handles.

Keywords*: Hierarchical mobility management, flow mobility distribution, secured flow control signaling*

1. Introduction

As mobile devices are allowed to move from one network domain to another, it is provided with a fixed IP address (home address or HoA) in the standard Mobile IPv6 (MIPv6) protocol [1, 2]. Whenever the mobile device moves, it configures another temporal IP address based on the router prefix of the visited network that is being used to route data traffic intended to its home address (HoA). This temporal IP address refers to as the Care-of Address (CoA) can be used by the mobile device after the default router is discovered; a stateless autoconfiguration and duplicate address detection (DAD) are performed.

Multimedia data traffic distribution using the standard mobile IPv6 (MIPv6) could be time consuming and will be unreliable as the number of mobile devices that connects and disconnects to the Internet is continuously increasing. The distribution of multimedia data traffic of mobile devices across the Internet can be greatly affected by the longer latency of MIPv6 handovers to which is contributed by the signaling overhead. That is, the standard MIPv6 allows more exchange of signaling messages whenever the mobile device is moving across different network environments. The routability issues can also cause packet losses that make the mobility far more complex and inefficient.

The increasingly connecting bulk of mobile devices cause the demand for a robust and balanced load distribution of data traffic which is essentially important in order for an efficient and manageable flow mobility. Thus, in order to address these issues, an optimization of the standard MIPv6 is implemented to limit the number of signaling between the mobile devices, its home agent and correspondent nodes. This optimization protocol refers to as the hierarchical mobile IPv6 (HMIPv6) [3] which

ISSN: 2005-4297 IJCA

include a central controller to manage and control the available access routers for mobile devices. The use of the central controller called the mobility anchor point (MAP) optimizes the exchange of signaling for mobile devices and thus provides a faster delivery of multimedia data traffic.

The optimized flow can be determined through the identification of the different factors that are essential for the computation of the handoff latencies for every access router (AR) that is available to the MAP. Such factors include bandwidth, traffic conditions, routing issues, the number of connected mobile devices, etc. In addition, the assurance of integrity for the delivered multimedia data traffic could be a turning factor for unreliable routing. Thus, routability optimization for IP packets distribution among mobile devices can be achieved through taking advantage of the multi-connectivity feature of HMIPv6 as well as securing its handoff signaling.

This paper aims to provide an analysis of a secured flow mobility distribution of multimedia data traffic over HMIPv6 environments. The mobile devices are allowed for multi-connectivity among available access routers (ARs) within the HMIPv6 domain. The MAP is given the control to determine the optimized route based on the identified traffic conditions and its exchange of signaling is secured with the utilization of the Authentication Header (AH) and Encapsulating Security payload (ESP) combination in the IPSec protocol [4, 5].

The rest of this paper is organized as follows: Section 2 discusses the HMIPv6 overview and its operations; the analysis for a secured flow mobility distribution over HMIPv6 environments is outlined in Section 3; and the concluding remarks in Section 4.

2. HMIPv6 Overview

The mobility anchor point (MAP) in HMIPv6 is the pivotal point for delivering a seamless mobility for mobile devices within the HMIPv6 environment. Figure 1 depicts the network architecture for the MAP utilization in a HMIPv6 domain. The mobile device in Figure 1 is allowed to move between Access Routers (ARs) that are directly controlled by a central controller referred to as the MAP while it is communicating with its correspondent node.

As soon as the mobile device moves to another area within the HMIPv6 domain, it discovers the MAP's global address that is included in the received Router Advertisements (RAs). While moving around, the mobile device can continuously receive RAs containing the MAP's global address. This is essentially important to determine whether the mobile device is still located within the same MAP domain or it has moved to another MAP (i.e., with a different global address).

The mobile device within the HMIPv6 domain is provided with two addresses: a regional Care-of Address (RCoA), which is based on the interface identifier of the mobile device and the subnet prefix of the MAP; and an on-link Care of Address, which is based on the mobile device's interface identifier and the subnet prefix of the default router to which it is connected.

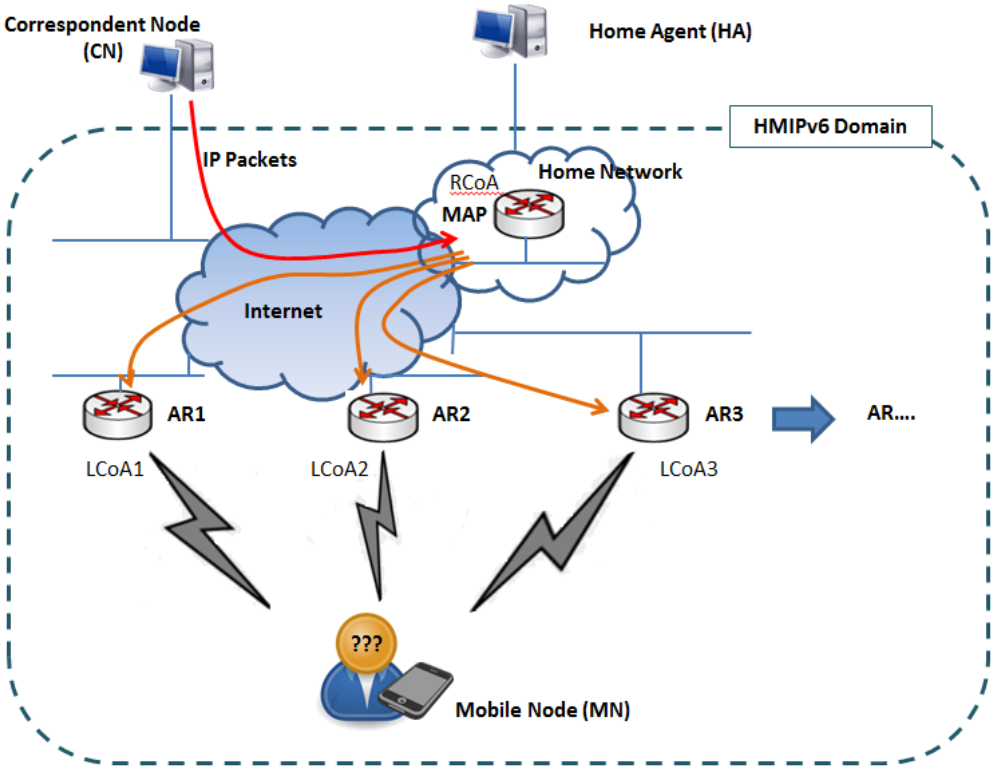

Figure 2. HMIPv6 Network Entities and Scenario

As soon as the mobile device acquires both the RCoA and LCoA, that is, for example it is connected to AR1, a local binding update (BU) is sent by the mobile device to the MAP that includes its RCoA in the Home Address option and uses its LCoA as the source address. Through this BU, the mobile device binds its LCoA (indicates its current location) with RCoA (indicates the MAP to which the access router is connected). With the successful binding (that is, a binding acknowledgement is received from the MAP), a bi-directional tunnel will be created between the mobile device and the MAP. The multimedia data traffic intended to the mobile device will then be forwarded by the MAP through tunneling. That is, the MAP will encapsulate the packets and directly forward it to the LCoA of the mobile device. Hence, the MAP acts as the home agent (HA) for the mobile device as well as the central controller for the access routers within its domain.

Whenever the mobile device moves to another access router (AR) within the MAP domain, there is no need for the mobile device to register again its RCoA to the correspondent node (CN) as well as to its home agent (HA). It only needs to send a local binding update indicating its new LCoA based on another access router (AR). The LCoA need not to be registered to the CN and HA. This allows a mobile device to have a multi-connection capability within the MAP domain in HMIPv6 environment.

However, if the mobile device moves to another MAP domain, the same process can be performed, that is, the mobile device configures a new RCoA and LCoA. A local BU will be sent to the new MAP that include the LCoA of the mobile device, and a home BU will be sent to the home agent (HA) to register its RCoA. All packets intended to the mobile device can then be intercepted by the new MAP and tunneled to the new LCoA of the mobile device.

3. Securing the Flow Mobility Distribution over HMIPv6 Environments

This section presents a discussion of the analysis on how to secure the binding updates and acknowledgements that are exchanged between the mobile device and its mobility anchor point (MAP). The combination of the Authentication Header (AH) and Encapsulating Security Payload (ESP) of the IPSec protocol is essentially important to utilize whenever registration signaling is exchanged by the mobile device and it's MAP. If binding updates and acknowledgements are breached by attackers, all packet exchange within the HMIPv6 domain will be compromised. Figure 2 depicts the multi-connectivity feature of mobile devices within a MAP domain in HMIPv6 environments. The mobile device needs to register its RCoA only once to its home agent as well as to its corresponding nodes. A secured flow control signaling is sent by the MAP to all available ARs in order to determine to which path is optimal such that the delivery of multimedia data traffic will distributed among the access routers. Information such as bandwidth, number of connected nodes, and handoff latency are determined through this flow control signaling. The path with the shortest handoff latency will be identified and a bi-directional tunnel will then be established. In this case, AR1 has the optimal path and all packets from the correspondent node will be intercepted by the MAP and tunneled to LCoA1 to where the mobile device needs to receive the data packets.

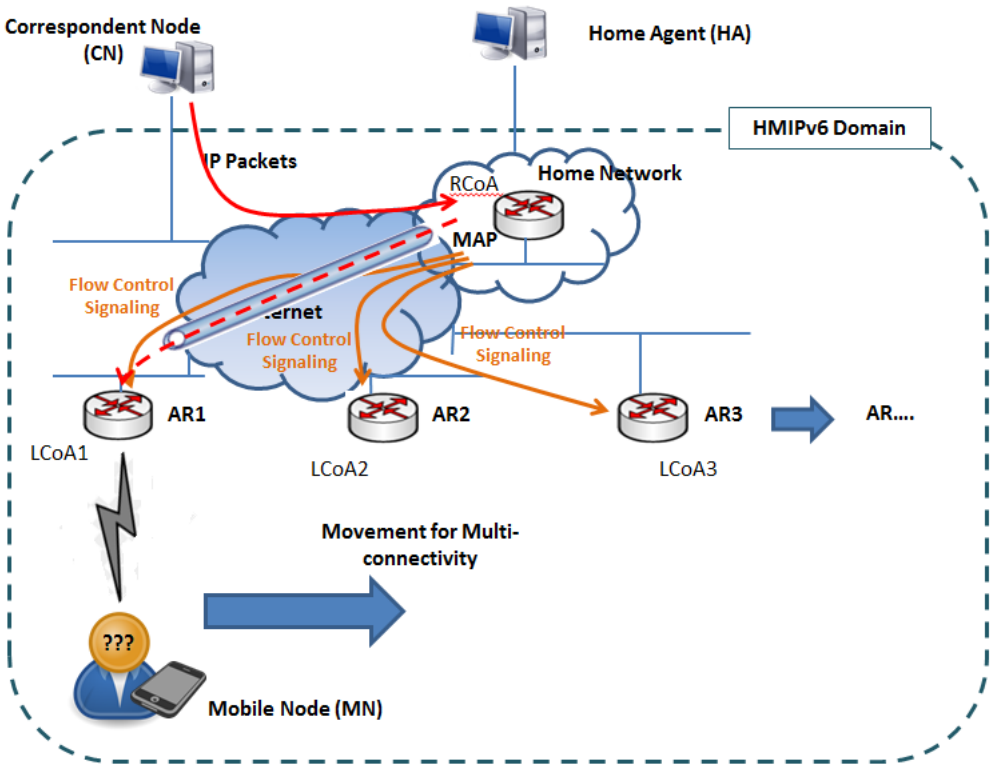

Figure 2. Multi-Connectivity Capability of a Mobile Device within a MAP Domain

If the handoff latency in AR2 is determined to be the shortest, then the bi-directional tunnel will be established between the MAP and AR2 so that the data packets can be received in LCoA2. The same scenario will be performed if the shortest handoff latency is identified to be in AR3 and so on.

Figure 2 depicts the multi-connectivity feature of mobile devices in the inter-MAP scenario. That is, the mobile device moves from one MAP to another in order to establish its optimized connectivity. The new RCoA and new LCoA need to be configured by the mobile device whenever it moves to another MAP domain. The new RCoA needs to be registered to its home agent (HA) and correspondent nodes (CNs) through sending a binding update. A local binding update will also be sent to the new MAP in order to register its new LCoA. The new MAP will then intercept the multimedia data traffic intended to the mobile device once the registrations are successful.

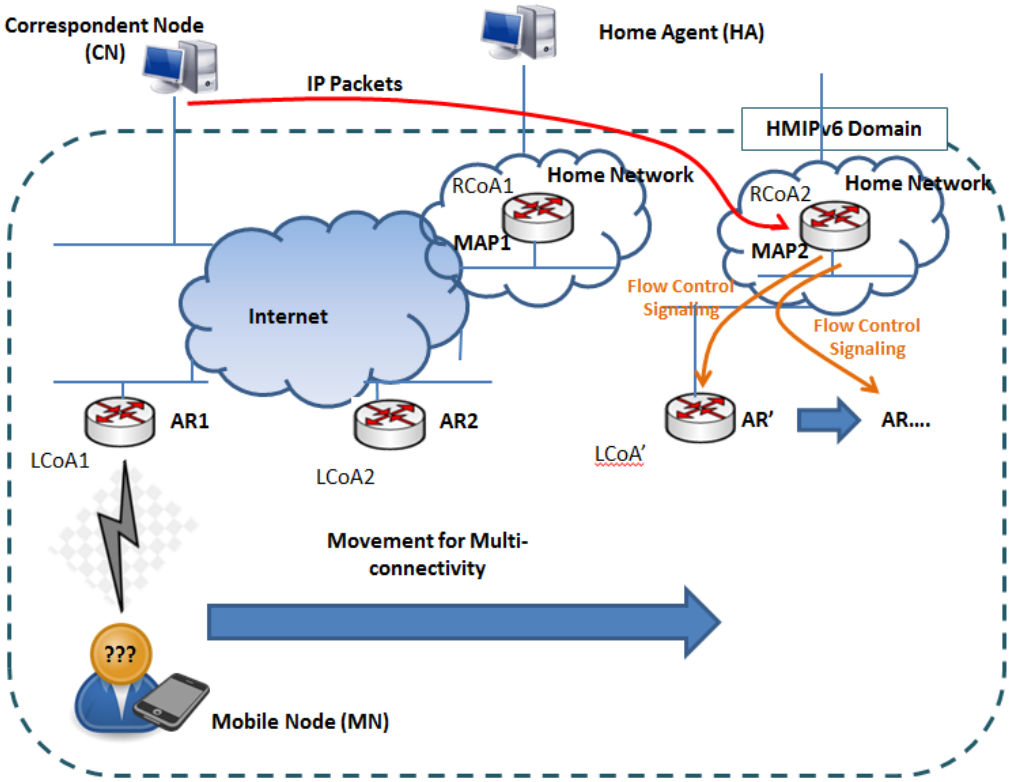

Figure 3. Multi-Connectivity Capability of a Mobile Device in the Inter-MAP Domain

The new MAP will then be acting as the central controller, and is responsible for the identification of the optimal path for forwarding the multimedia data traffic. A flow control signaling is also sent to all available access routers in order to determine which path the flow mobility needs to be delivered. That is, the same scenario of processes will be performed as in the intra-MAP domain multi-connectivity. The exchange of signaling also needs to be encapsulated with the combination of AH and ESP in the IPSec protocol.

Figure 4. Packet Format for Binding Updates

Figure 5. Packet Format for Binding Acknowledgements

Figure 4 and 5 depicts the packet formats for the binding updates (BUs) and binding acknowledgements (BAs) that are exchanged by the mobile device and the MAP and between the mobile device and its home agent (HA). The flow control signaling that is regularly sent by the MAP is also following this packet format that includes the combination of AH and ESP extension headers. Thus, the communication with the mobile device is ensured of integrity and authenticity. In addition, replay and reordering attacks can be avoided.

4. Conclusion

This paper has presented an analysis of a secured multimedia data traffic distribution management based on HMIPv6 environments. The multi-connectivity feature for mobile devices were utilized for the efficient and balanced distribution of multimedia data traffic and a centralized control over the handoffs optimization between the mobile device and the mobility anchor point (MAP) is provided. The optimum route for forwarding of multimedia data traffic can be identified in order to enhance the handover performance and efficiency for HMIPv6. The flow control signaling and exchange of binding updates and binding acknowledgements are secured with the implementation of the combination of AH header and ESP header for IPSec protocol.

Acknowledgments

This research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Science, ICT and future planning (2015R1A2A2A03002851).

References

[1] D. Johnson, C. Perkins, J. Arkko, "Mobility Support in IPv6", Internet Engineering Task Force (IETF), RFC 3775, June **(2004)**.

[2] C. Perkins, D. Johnson, J. Arkko, "Mobility Support in IPv6", Internet Engineering Task Force (IETF), RFC 6275, ISSN: 2070-1721, July **(2011)**.

[3] H. Soliman, C. Castelluccia, K. ElMalki and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", IETF, RFC No. 5380, http://www.rfc-base.org/txt/rfc-4140.txt, **(2008)** October.

[4] S. Frankel, K. Kent, R. Lewkowski, A. D. Orebaugh, R. W. Ritchey, S. R. Sharma, "Guide to IPsec VPNs: Recommendations of the National Institute of Standards and Technology", National Institute of Standards and Technology Special Publication 800-77, **(2005)** December, 126 pages, http://csrc.nist.gov/publications/nistpubs/800-77/sp800-77.pdf.

[5] http://www.unixwiz.net/techtips/iguide-ipsec.html

