Experiences with IPFIX-based Traffic Measurement for IPv6 Networks

Nakjung Choi[1], Hyeongu Son[2], Youngseok Lee[2] and Yanghee Choi[1]

[1] Seoul National University, Seoul, Korea
{fomula, yhchoi}@mmlab.snu.ac.kr

[2] Chungnam National University, Daejon, Korea
{hgson, lee}@cnu.ac.kr

ABSTRACT

Though the popular Cisco NetFlow is widely used for flow-level traffic measurement in IPv4 networks, it is not suitable for IPv6 networks because of the fixed flow structure that cannot carry IPv6-related information. Therefore, the IETF IP Flow Information eXport (IPFIX) standard that employs the flexible flow template structure has been recently proposed to support various flow-level traffic monitoring applications for next-generation Internet such as QoS monitoring, anomaly detection, and IPv6 traffic measurement. Yet, realistic traffic measurement methods with IPFIX have not been much studied. IPv6 traffic analysis has been possible with IPFIX, but it has to be investigated in detail. Especially, traffic measurement in IPv6 networks meets new challenges because ICMPv6 messages, IPv6 extension headers, and mobile IPv6 packets are commonly used for many IPv6-specific features. Hence, this paper presents traffic monitoring experiences in IPv6/mobile IPv6 (MIPV6) networks with IPFIX by proposing new flow templates that have been extended to observe various kinds of IPv6 traffic. From our experiments, it was shown that IPFIX-based IPv6 traffic measurement scheme is useful for anomaly IPv6 traffic detection and MIPv6 handover analysis. For instance, IPv6 anomaly traffic exploiting ICMPv6 messages and covert channels could be easily detcted with our templates. In addition, the MIPv6 traffic measurement methodology with IPFIX has been verified to estimate the user-experienced handover latency.

Categories and Subject Descriptors

C.2.3 [**Network Operations**]: Network Management, Network Monitoring; C.2.1 [**Network Architecture and Design**]: Network Communications, Wireless Communication; C.2.5 [**Local and Wide-Area Networks**]: Internet

IPv6'07, August 31, 2007, Kyoto, Japan.

General Terms

Management, Measurement, Design, Experimentation, Verification

Keywords

IPv6, traffic measurement, IPFIX, mobile IPv6, anomaly traffic

1. INTRODUCTION

Internet traffic measurement is essential for monitoring trends, accounting, network planning and anomaly traffic detection. In general, simple packet- or byte-counting methods with SNMP have been widely used for easy and useful network administration. In addition, the passive traffic measurement approach that collects and analyzes packets at routers or dedicated machines is also popular in IPv4 networks. However, traffic measurement will be more difficult in the next-generation Internet with the features of high-speed links or new protocols such as IPv6 or mobile IPv6.

Traffic measurement at high-speed links is challenging because of fast packet-processing requirement. Though packet-level measurement can describe the detailed traffic characteristics, it is not easy to support high-speed line rates of multi-gigabit per second. Moreover, standalone systems for packet-level traffic monitoring will be expensive for wide deployment and easy management in a large-scale network. Hence, Internet Service Providers (ISPs) will generally prefer the flow-level traffic measurement approach that could be easily embedded into routers or switches to dedicated packet-level traffic monitoring systems. Currently, flow-level measurement modules at routers such as Cisco NetFlow [1] have become popular, because flow-level measurement could generate useful traffic statistics with a significantly small amount of measured data. Recently, the standard for traffic monitoring of routers has been proposed by IETF IPFIX WG [2], which defined the flexible and extensible template architecture that can be useful for various traffic monitoring applications. For example, IPv6 traffic monitoring, intrusion detection, and QoS measurement have been possible at routers due to the flexible template structure of IPFIX. Thus, it is expected that IPFIX will be useful for various traffic monitoring methods in next-generation Internet such as IPv6/MIPv6 networks. However, only a few studies regarding IPv6 traffic measurement [3-7] are reported, and furthermore, real experiences of traffic monitoring in IPv6

networks with IPFIX have hardly been studied. For detailed traffic measurement in IPv6 networks, it is important to systematically monitor ICMPv6 and IPv6 packets with extension headers as well as plain IPv6 traffic, which will be useful for understanding the diverse IPv6 traffic characteristics more correctly.

Hence, in this paper, we describe IPv6 traffic measurement experiences with our proposed IPFIX templates for monitoring anomaly IPv6 traffic and MIPv6 traffic. Our major contribution is that the in-depth analysis of IPv6 anomaly traffic and MIPv6 traffic has been possible with the proposed IPFIX template. Particularly, we have verified that the IPv6 anomaly traffic with ICMPv6 and IPv6 extension headers could be correctly classified with our monitoring method. In addition, it was shown from the experiments that the user-perceived handover latency in MIPv6 networks could be easily derived by our IPFIX MIPv6 traffic monitoring approach.

The remainder of this paper is organized as follows. We begin in Section 2 by introducing NetFlow/IPFIX and explain the basic IPv6 traffic monitoring method with IPFIX in Section 3. In Section 4, we propose new IPFIX templates that could carry the information on anomaly IPv6 traffic and MIPv6 traffic. Section 5 describes how to build our IPFIX-based traffic monitoring system and its experimental results, especially MIPv6 handover delay analysis. Lastly, we concludes this paper in Section 6.

2. BACKGROUND

Cisco NetFlow v5 is commonly used for flow-level monitoring in current IPv4 networks. However, NetFlow v5, that has a fixed key structure, is not capable of monitoring various kinds of protocols such as IPv6, MPLS and multicast. Moreover, the per-flow statistics analyzed at observation points are transmitted over unreliable UDP, which could induce the loss of measured data. To tackle the drawbacks of NetFlow v5, IPFIX is equipped with the flexible and extensible template architecture, and it uses reliable SCTP/TCP as a default transport protocol.

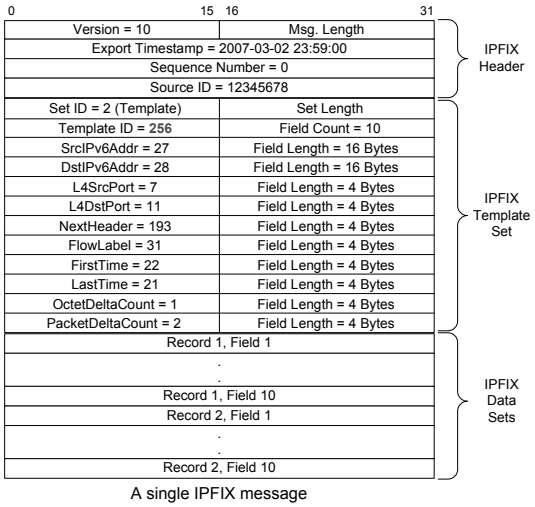


Figure 1: An example of IPFIX message.

IPFIX regards a flow as a sequence of packet arrivals observed in a specific timeslot that share common properties such as IP addresses and port numbers. An IPFIX exporter that usually resides within routers will periodically send IPFIX flows to the IPFIX collector. IPFIX defines the makeup of these flow message through a special type of a message called the "template". Various templates could be specified for each traffic monitoring application, which makes IPFIX adaptive to different measurement scenarios. A simple example of a IPFIX message that carries IPv6 flow statistics is illustrated in Fig. 1. The message contains an IPFIX header and two different IPFIX sets: one is the template set that introduces the build-up of the data set and the other is the flow data set which shows two flow entries. The template set should be sent to the IPFIX collector before the data set in advance. Often it will be periodically delivered to the IPFIX collectors.

3. MEASUREMENT OF BASIC IPV6 FLOWS

A basic IPv6 flow is defined by a set of IPv6 packets that share five-tuples of the same basic IPv6 header fields and the upper-layer header fields that are typically composed of (src IPv6 addr, dst IPv6 addr, src port, dst port, next header). Thus, IPv6 extension headers are not considered for basic IPv6 flow measurement. The flow classifier processes incoming IPv6 packets with 5-tuples of IPv6 header fields and upper-layer protocol header fields to find the corresponding flow entries stored at the flow binding table. If any flow entry matching to the incoming packet does not exist, a new flow will be created. Otherwise, attributes of the flow entry such as the number of packets, the number of bytes and the first/last flow time will be updated. In order to maintain the flow binding table, a flow expiration timer is set to terminate a flow if a packet belonging to the same flow specification does not arrive within the given timeout. Then, the expired flow entries will be exported to the flow collector. In basic IPv6 flow measurement, each flow entry includes data records according to the defined flow template as shown in Fig. 1 where fields related with the plain IPv6 basic header are only given.

4. MEASUREMENT OF EXTENDED IPV6 FLOWS WITH NEW IPFIX TEMPLATES

4.1 Extended IPv6 Traffic

Although plain IPv6 traffic is monitored with basic IPv6 headers and UDP/TCP header fields, it is necessary to additionally observe IPv6 extension headers (EH) and ICMPv6 fields for more correct traffic classification. For example, Hop-by-Hop EH is used for Jumbo-grams or Router Alert option, and Routing EH is employed in IPv6 mobility and source routing. Fragmentation EH is for support of fragmented IPv6 packets, and Authentication/Encapsulating Security Payload EHs are for IP security. Mobility EH is also essential in MIPv6. Hence, without IPv6 extension headers, correct IPv6 traffic analysis cannot be achieved. Besides, it was observed from experimental results that a lot of ICMPv6 flows for administrative usages are generated. For example, ICMPv6 is widely used for IPv6-specific features such as auto-configuration or router advertisement. On the other hand, since ICMPv6 traffic might be used for anomaly traffic, various types of ICMPv6 packets should be judiciously tracked.

Recent reports on IPv6 anomaly traffic show that IPv6

EHs have been already maliciously utilized. For example, a covert channel, that is a communication path which allows to transfer information in a way that violates a security policy, could be exploited by using the IPv6 protocol for exchanging anomaly traffic. In [8] the destination option and ICMPv6 echo reply were abused for transporting text chatting messages unnoticeably, which could avoid the typical IPv6 firewall. It was shown that other fields of IPv6 protocol messages could be vulnerably used for covert channels [9]. Moreover, an ICMPv6-based attack tool that could generate various types of IPv6 anomaly traffic such as DoS using IPv6 Duplicate Address Detection (DAD), fake IPv6 routers, and IPv6 smurf attack was announced in [10]. Among several IPv6 features, it is well known that auto-configuration without authentication is prone to attacks such as new-dos-IPv6. Recently, SEcure Neighbor Discovery (SEND) [11] has been standardized to protect attacks with ICMPv6 neighbor solicitation/acknowledgement messages. However, it is not fully implemented and deployed throughout the whole IPv6 network.

On the other hand, IPv6 extension messages and ICMPv6 are important in MIPv6, where binding update (BU)/binding acknowledgement (BA) messages with mobility headers are using a destination EH and a routing option EH. In MIPv6, traffic of a mobile node is moved to the visiting network when the handover is completed. Therefore, MIPv6 handover signaling as well as IPv6 traffic should be monitored for analyzing MIPv6 host behaviors and handover performance. For this purpose, BU/BA messages and tunneled IPv6 traffic should be collected. Especially, for the IPFIX application of MIPv6 traffic monitoring, we propose a simple methodology that can estimate the user-experienced handover latency with IPv6 data flows and MIPv6 handover flows.

4.2 How to Monitor Extended IPv6 Traffic

Although basic IPv6 traffic could be monitored with predefined IPFIX templates, we need to extend IPFIX templates to monitor IPv6 traffic with EHs and ICMPv6 fields. For this purpose, we combines effective information fields defined in IPFIX, which are related with IPv6 EHs and ICMPv6 in order to capture anomaly IPv6 and MIPv6 traffic. Hence, our new IPFIX templates can carry ICMPv6 information, EH fields, and IPv6-in-IPv6 tunnel traffic.

4.2.1 Monitoring ICMPv6 traffic

0 … 15	16 … 31
Set ID	Set Length
Template ID = 301	Field Count = 12
SrcIPv6Addr = 27	Field Length = 16 Bytes
DstIPv6Addr = 28	Field Length = 16 Bytes
NextHeader = 193	Field Length = 4 Bytes
FirstTime = 22	Field Length = 4 Bytes
LastTime = 21	Field Length = 4 Bytes
OctetDeltaCount = 1	Field Length = 4 Bytes
PacketDeltaCount = 2	Field Length = 4 Bytes
IcmpTypeIPv6 = 178	Field Length = 1 Bytes
IcmpCodeIPv6 = 179	Field Length = 1 Bytes
SrcMacAddr = 56	Field Length = 6 Bytes
DstMacAddr = 80	Field Length = 6 Bytes
TargetIPv6Addr = 200	Field Length = 16 Bytes

Figure 2: An IPFIX template for monitoring ICMPv6 NS/NA traffic.

Fig. 2 shows a new IPFIX template that can carry ICMPv6 neighbor solicitation (NS) or neighbor advertisement (NA) message fields. The NS/NA messages are normally used for a part of DAD in an auto-configuration procedure. Hence, when a new IPv6 host is attached to a LAN, it sends an NS message to check that its address is not owned by others. If a new host hears any response message, it could not be connected to the LAN; this is called the new-dos-IPv6 attack [10]. Therefore, we have to investigate ICMP packets in order to detect the new-dos-IPv6 attack or similar attack called parasite6 that is also exploiting ICMPv6 NS/NA messages. The IPFIX template shown in Fig. 2 carries ICMPv6 type and code fields, which could be used for ICMPv6 traffic classification. In addition, MAC addresses and target IPv6 address will be useful for traffic classification of auto-configuration and DAD.

4.2.2 Monitoring IPv6 EHs

0 … 15	16 … 31
Set ID	Set Length
Template ID = 303	Field Count = 9
SrcIPv6Addr = 27	Field Length = 16 Bytes
DstIPv6Addr = 28	Field Length = 16 Bytes
L4SrcPort = 7	Field Length = 4 Bytes
L4DstPort = 11	Field Length = 4 Bytes
NextHeader = 193	Field Length = 4 Bytes
TrafficClass = 5	Field Length = 4 Bytes
FirstTime = 22	Field Length = 4 Bytes
LastTime = 21	Field Length = 4 Bytes
IPv6ExtensionHeaders = 64	Field Length = 4 Bytes

Figure 3: An IPFIX template for IPv6 flows with extension headers.

Since IPv6 EHs have variable sizes and different fields, they could not be carried in a single fixed IPFIX flow format. As defined in [12], we used the flag information field that can mark the existence of IPv6 EHs. Due to the IPFIX template in Fig. 3, we can infer from the EH flag information field which EHs are used. Generally, the usage of IPv6 traffic consisting of EHs could be well described in advance. Thus, classification of IPv6 traffic patterns using EHs will not be difficult. In addition, since IPv6 anomaly traffic could use EHs for malicious purposes, it has to be carefully examined. For example, a message-exchanging covert channel tool has been announced in [8]. In this IPv6 covert channel, the destination EH was used, because its current usage is only related with MIPv6. Therefore, IPv6 flows with the destination EH should be carefully inspected. Typically in firewalls, IP addresses and port numbers are employed for rule matching. However, IPv6 firewalls should be aware of EHs for applying security policy rules.

4.2.3 Monitoring MIPv6 traffic

In MIPv6 [13], when BU/BA IPv6 packets are exchanged between MN and HA during handover, every packet should be looked into by routers to examine the cascaded IPv6 EHs, because BU/BA messages are encapsulated with destination option/routing, ESP, and mobility headers in order in addition to the IPv6 basic header [4]. After handover is completed, the traffic from CN to MN will be sent to MN through the tunnel via HA if route optimization is not applied. Therefore, the IPv6 EHs for IPv6-in-IPv6 tunneled packets should be also identified. Since a mobile node will be associated with multiple IPv6 address, MIPv6 handover messages as well as IPv6 data flows should be carefully mon-

itored. In order to monitor MIPv6 traffic with IPFIX, we present two new MIPv6-specific IPFIX templates that can carry information regarding layer-3 (L3) handover BU/BA messages and tunneled IPv6 flows.

0 15	16 31
Set ID	Set Length
Template ID = 257	Field Count = 15
Fields for basic IPv6 flow	
MIPv6MsgType = 200	Field Length = 4 Bytes
MIPv6CoA = 201	Field Length = 16 Bytes
MIPv6HAAddr = 202	Field Length = 16 Bytes
MIPv6HomeAddr = 203	Field Length = 16 Bytes
MIPv6MsgSeqNum = 204	Field Length = 4 Bytes

(a) BU/BA messages.

0 15	16 31
Set ID	Set Length
Template ID = 258	Field Count = 13
Fields for basic IPv6 flow	
IPv6TunnelSrcAddr = 300	Field Length = 16 Bytes
IPv6TunnelDstAddr = 301	Field Length = 16 Bytes
TunnelProto = 302	Field Length = 4 Bytes

(b) IPv6 tunneling flows.

Figure 4: New IPFIX templates for MIPv6.

Fig. 4 shows the MIPv6-specific IPFIX templates employed by IPFIX flow generators at ARs. Fig. 4(a) illustrates the IPFIX template format that could carry BU/BA messages. A BU/BA flow template consists of MIPv6messageType (= BU or BA), MIPv6CareOfAddress, MIPv6HomeAgentAddress, MIPv6HomeAddress and MIPv6MessageSequenceNumber besides the basic IPv6 template. This BU/BA flow is created when a BU or a BA packet has been monitored at each AR. In Fig. 4(b), the IPFIX template of IPv6-in-IPv6 tunneled flows is shown, where the source and destination addresses of the tunnel have been added to the basic IPv6 template. After receiving IPFIX flows exported by ARs, the IPFIX flow collector can detect the L3 handover events based on BU/BA flows and can track which flow as well as which MN have moved to which cell.

In our IPv6/MIPv6 network testbed, when the handover is completed, the traffic between the MN and the CN will be forwarded through the tunnel between the MN and its HA[1]. Thus, the IPFIX collector can extract MIPv6 traffic information from plain or tunneled IPv6 data flows exported by each AR as well as L3 handover flows of BU/BA messages. In order to infer user-perceived handover latency, we calculate the time difference between the last time of basic or tunneled IPv6 data flow at the previous AR and the first time of a flow at the new AR. This time difference is called *data-driven handover latency*, which estimates the user-experienced handover delay. Its primary advantage is that we can consider the data-driven handover latency as a barometer of user-experienced performance degradation induced by handover in IPv6/MIPv6 network since it measures the interrupted time interval of continuous data transfer with the only L3 information. Though handover analysis with the measured data at end hosts is more correct, our approach will be suitable for measurement in a large-scale network by ISPs when it is not possible to collect the data at mobile nodes.

[1]In this paper, we assume only the bidirectional tunneling MIPv6 communication mode without route optimization. However, route optimization and other handover mechanisms such as fast handover could be easily supported.

5. EXPERIMENTS

5.1 IPv6/MIPv6 Network Testbed

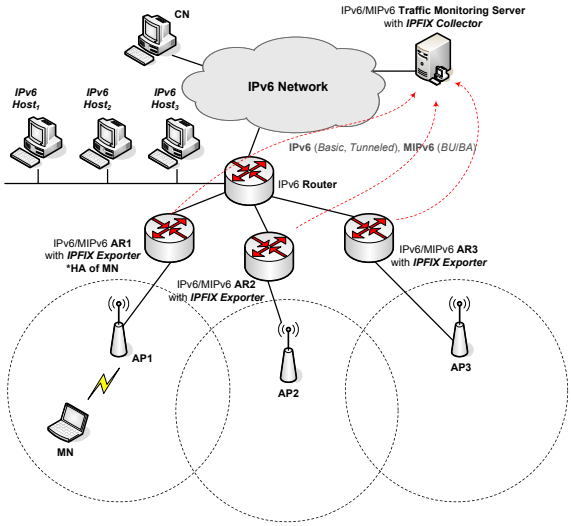


Figure 5: The experimental environment for measurement of extended IPv6 traffic.

An IPv6/MIPv6 network testbed for the experiments is depicted in Fig. 5. We used the IPFIX flow generator at IPv6 PC routers by modifying *nProbe* [14] to carry the proposed multiple IPFIX templates. We have also implemented a flow collector by using a open-source library, *libipfix* [15]. From the collected IPFIX data, the flow analyzer periodically extracts diverse useful information such as total IPv6 traffic, the number of MIPv6 nodes and binding update latency, and it updates Round Robin Databases (RRDs) related to the IPv6 statistics. For our IPv6/MIPv6 traffic visualizer, we have extended an open-source tool called *nfsen* [16] for a web-based graphical interface which displays the analysis results of the measured data stored at RRDs. In addition, we have implemented the MIPv6 traffic analysis functions to observe mobile traffic such as mobility pattern, MIPv6 traffic usage, and BU/BA flows. Our MIPv6 testbed was based on MIPLv2 [17].

5.2 Experimental Results

First, the DoS-new attack using ICMPv6 DAD messages is shown in Fig. 6. While a new host, *IPv6 host*$_1$, is booting up and begins the auto-configuration procedure, it sends an ICMPv6 NS message to the multicast address. This NS message has the ICMP type of 135 and the code of 0, and its target IPv6 address. When the attacker, *IPv6 host*$_2$, answers this NS message with the NA message of ICMPv6 type of 136 and code of 0, the new host cannot be connected. On this situation, our flow measurement tool running on

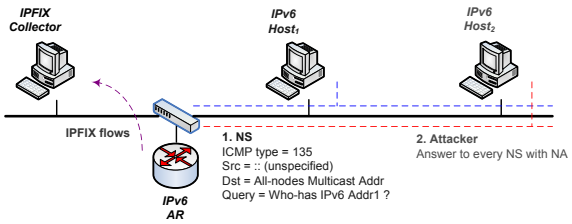


Figure 6: A DoS-new-IPv6 attack.

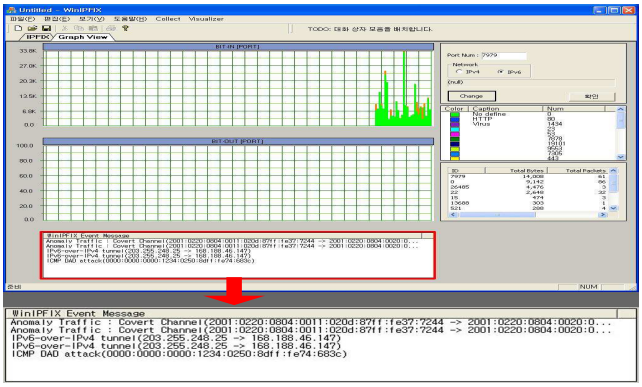


Figure 7: WinIPFIX: an IPFIX collector/visualizer that captures DoS-new-IPv6 attack flows.

the IPv6 tunneling router, captures this ICMPv6 type/code and target address in the template defined in Fig. 2. When these ICMPv6 NS/NA messages are exported to the flow analyzer [18] which we developed in Fig. 7, anomaly ICMPv6 DAD traffic is detected. Similar IPv6 anomaly traffic such as ICMPv6 could be monitored.

Second, we performed the experiment of monitoring the IPv6 EH fields. For this purpose, we used the IPFIX template defined in Fig. 3 which includes the EH flag field. A covert channel tool [10], which utilizes the IPv6 destination option and ICMPv6 echo reply, was run on *IPv6 host*$_1$ and *IPv6 host*$_3$ as shown in Fig. 6. Since the destination option is currently collocated with the mobility header in MIPv6, this flow could be classified into suspected traffic with the IPv6 destination option.

Third, we conducted massive experiments for MIPv6 handover, in which the MN whose HA is AR1 moves along ARs (AR1 → AR2 → AR3 → AR2 → AR1). In this handover scenario, the MN sends/receives UDP or TCP packets to/from the CN. UDP and TCP flows are generated by *dvts* [19] and *Iperf* [20], respectively. During the experiment, we collected BU/BA handover messages with mobility header information as well as handover IPv6 data flows exported from every AR with the IPFIX templates defined in Fig. 4. Then, we calculated data-driven handover latency by analyzing the IPFIX IPv6 data flows before/after handover and the IPFIX BU/BA flows. For the comparison, *tcpdump* [21] was used to capture all IPv6 packets at the MN and the CN from which the MIPv6 handover latency that the user really experiences will be computed.

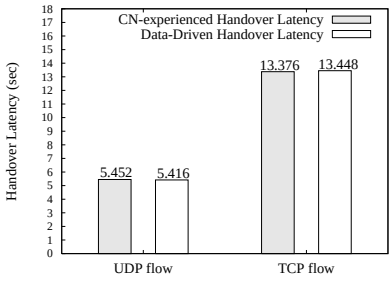
In Fig. 8 and Fig. 9, the average user-perceived service-disrupted duration is compared to the average data-driven handover latency computed from the last timestamp of the before-handover flow data and the first timestamp of the after-handover flow data with upload and download IPv6 flows, respectively. In case of upload IPv6 flows, errors between the two values are negligible irrespectively of UDP or TCP. In the downloading situation, it should be noted that data flow toward MN is still observed at the previous AR even though MN has moved to the foreign network, because it takes time for MN to register its new location at the home agent. Thus, for download IPv6 flows, we calculate the data-driven handover latency by using the first timestamp of the BU flow instead of the last timestamp of the before-handover flow. In spite of this revision, there could be still large gaps with the user-perceived handover latency as shown in Fig. 9 because the L2 handover latency and IPv6 auto-configuration latency for a CoA acquisition are omitted. As a stopgap measure, if an appropriate L2 handover and IPv6 auto-configuration latency (e.g., 4.5s in our testbed) are added, then the differences between the two values are less than 0.5s in most cases, which could be acceptable. If a technique [22] to minimize L2 handover latency is applied, we can estimate the user-experienced handover latency exactly, only with the data-driven handover latency.

5.3 Discussion

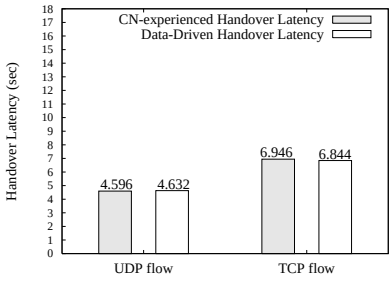
There are issues that have to be considered while measuring extended IPv6 traffic with IPFIX. Usually, *sampling* is considered in IPFIX, but it is not assumed in our work. That is, we should monitor every IPv6 packet at all observation points. However, it will not be a serious overhead for edge routers with fast packet processing capability in IPv6 access networks. The amount of traffic of the first-hop IPv6 routers will not be large in general so that it will be possible to support high-speed line cards with 1:1 non-sampling mode by using a network processor or ASIC. For the further analysis in MIPv6 networks, L2 information is necessary to monitor the end-user behaviors more precisely. Then, the handover latency of mobile users will be correctly derived with L2 and L3 information. Therefore, future work include how to measure and combine L2 traffic with MIPv6 traffic, and how to extract useful information on each end-user. Furthermore, our IPFIX-based IPv6 traffic measurement approach could be easily extended for various mobility protocols such as Fast MIPv6, HMIPv6 and mobile networks (NEMOs).

6. CONCLUSIONS

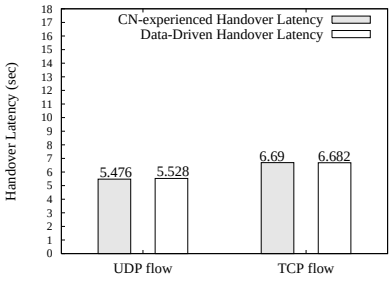
For the detailed traffic classification of IPv6 traffic, we proposed flexible IPFIX-based traffic monitoring methods that could be useful in various IPv6 traffic measurement applications. We first presented new IPFIX templates that can carry IPv6 flows with extension headers and ICMPv6 type/code, because extension headers and ICMPv6 in IPv6 networks are important for security. Then, we also proposed the method of monitoring MIPv6 data flows and handover signaling traffic by including IPv6 mobility header information fields. It is shown that our flexible IPFIX-based flow measurement method is useful for monitoring anomaly IPv6 traffic and for tracking mobile nodes and their traffic. For future work we are considering how to improve the IPFIX flow generator so that it could support multiple templates dynamically and L2 information with the minimum resources. In addition, while IPv4 networks are migrated to IPv6 networks, we have to support the integrated way of monitoring IPv4 as well as IPv6 traffic under the IPFIX architecture.



(a) Handover from HN to FN.

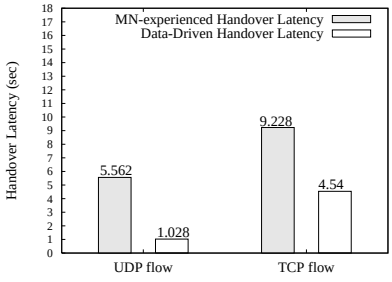


(b) Handover from FN to another FN.

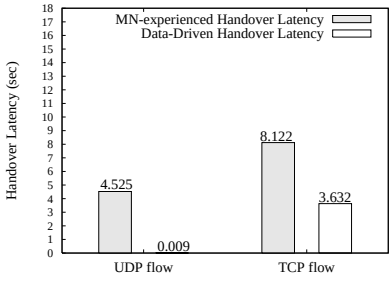


(c) Handover from FN to HN.

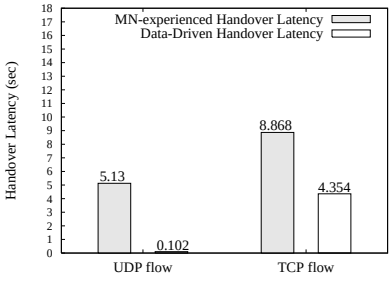
Figure 8: Upload IPv6 flow with handover in MIPv6 networks.



(a) Handover from HN to FN.



(b) Handover from FN to another FN.



(c) Handover from FN to HN.

Figure 9: Download IPv6 flow with handover in MIPv6 networks.

7. ACKNOWLEDGMENTS

This research was supported by the Brain Korea 21 project of Ministry of Education, Korea, and by the MIC (Ministry of Information and Communication), Korea, under the ITRC (Information Technology Research Center) support program supervised by the IITA (Institute of Information Technology Assessment). (IITA-2005-(C1090-0502-0020))

8. REFERENCES

[1] Cisco NetFlow, http://www.cisco.com/warp/public/732/netflow/.

[2] J. Quittek, T. Zseby, B. Claise, and S. Zander, "Requirements for IP Flow Information Export (IPFIX)," IETF RFC 3917, October 2004.

[3] P. Marques, H. Castro, and M. Ricardo, "Monitoring Emerging IPv6 Wireless Access Networks," IEEE Wireless Communication Mag. vol. 12, no. 1, pp. 47-53, Feb. 2005.

[4] Y. Lee, S. Choi, and J. Lee, "Monitoring MIPv6 Traffic with IPFIX," IEEE IPOM, Oct. 2006.

[5] W. Yi, Y. Shaozhi, and L. Xing, "Understanding Current IPv6 Performance: a Measurement Study," IEEE ISCC, 2005.

[6] P. Savola, "Observations of IPv6 Traffic on a 6to4 Relay," ACM SIGCOMM CCR vol. 35, no. 1, pp. 23-28, Jan. 2005.

[7] M. Ford, J. Stevens, and J. Ronan, "Initial Results from an IPv6 Darknet," ICISP, 2006.

[8] T. Graf, "Messaging over IPv6 Destination Options," The Swiss Unix User Group, Switzerland, http://gray-world.net/papers/messip6.txt, July 2003.

[9] N. B. Lucena, G. Lewandowski, and S. J. Chapin, "Covert Channels in IPv6," Workshop on Privacy Enhancing Technologies, May/June 2005.

[10] The Hackers' Choice Attack Tool, http://thc.segfault.net/.

[11] J. Arkko, J. Kempf, B. Zill, and P. Nikander, "SEcure Neighbor Discovery (SEND)," IETF RFC3971, March 2005.

[12] J. Quittek, B. Bryant, B. Claise, P. Aitken, and J. Meyer, "Information Model for IP Flow Information Export," IETF Draft, October 2006.

[13] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," IETF RFC3775, June 2004.

[14] L. Deri, "nProbe: an Open Source NetFlow Probe for Gigabit Networks," TERENA Networking Conference, May 2003.

[15] libIPFIX Internet Measurement Project, http://ants.fokus.fraunhofer.de/libipfix.

[16] Netflow Sensor (NfSen), http://nfsen.sourceforge.net.

[17] Mobile IPv6 for Linux (MIPLv2), http://www.mipl.mediapoli.com/.

[18] WinIPFIX, http://networks.cnu.ac.kr/ winipfix/.

[19] Digital Video Transport System (DVTS), http://www.sfc.wide.ad.jp/DVTS/.

[20] Iperf, http://dast.nlanr.net/Projects/Iperf/.

[21] TCPDUMP, http://www.tcpdump.org/.

[22] C. Vogt, R. Bless, M. Doll, and G. Daley, "Analysis of IPv6 Relocation Delays," Internet-Draft draft-vogt-dna-relocation-01.txt, July 2005.