

Experiences with IPFIX-based Traffic Measurement for IPv6 Networks

Nakjung Choi, Hyeongu Son*, Youngseok Lee* and Yanghee Choi

Seoul National Univ
*Chungnam National Univ

2007. 8. 31 (Fri)



SIGCOMM 2007 IPv6 Workshop

1

Introduction

- Internet traffic measurement
 - Monitoring trends, accounting, network planning, and anomaly traffic detection
 - General Internet traffic monitoring methods
 - Simple packet- or byte-counting: SNMP
 - Passive traffic measurement: e.g., tcpdump
- Flow-level traffic measurement approach
 - E.g., Cisco NetFlow
 - Less overhead
 - Easy deployment
 - IETF IP Flow Information eXport (IPFIX) standard



SIGCOMM 2007 IPv6 Workshop

2

Motivation

- Examine the feasibility of IPFIX-based traffic measurement methods
 - IPFIX enables various traffic monitoring applications suitable for IPv6 flows, QoS, and intrusion detection
- Few studies on IPv6 traffic measurement with IPFIX
 - Cisco NetFlow v9: only covers IPv6 basic flows
 - However, ICMPv6 as well as IPv6 extension headers are important for traffic monitoring
 - E.g., IPv6 anomaly traffic and mobile IPv6 traffic

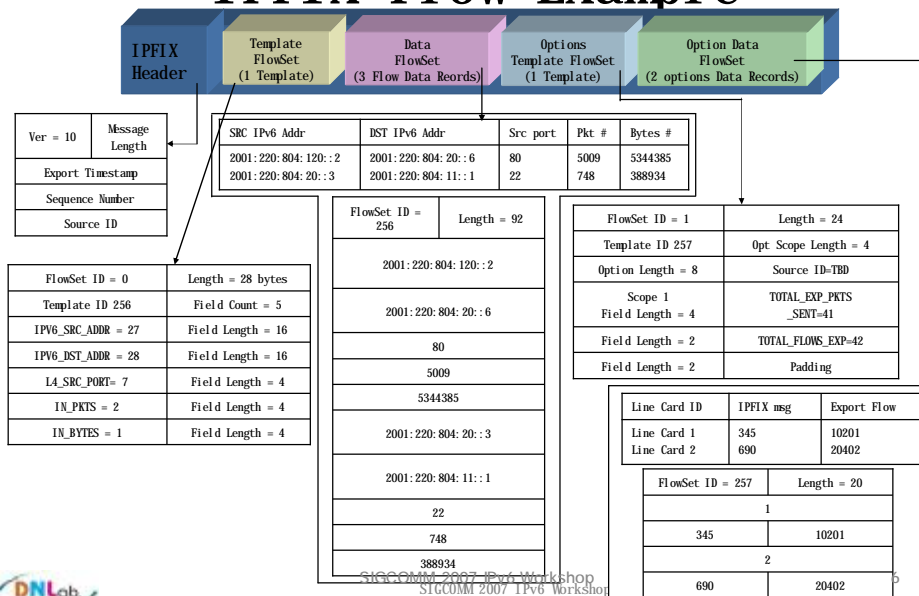
Contribution

- Propose IPFIX templates for monitoring
 1. anomaly IPv6 traffic that are exploiting ICMPv6 and IPv6 extension headers
 2. mobile IPv6 traffic with mobility headers
- Experiences with IPFIX-based IPv6 traffic monitoring

IP Flow Information eXport (IPFIX)

- Popular flow-level traffic measurement
 - Cisco NetFlow v5 in IPv4 networks
- IETF IPFIX standard
 - Based on Cisco NetFlow v9
 - Flexible and extensible template
 - Supports IPv6, MPLS and multicast
 - Reliable transport protocols
 - SCTP, TCP

IPFIX Flow Example



Measurement of Basic IPv6 Flows

- An (basic) IPv6 flow
 - A set of IPv6 packets sharing 5-tuples of (src IP addr, src port, dst IP addr, dst port, next header) within a timeout
- Generally, IPv6 flow-level measurement is similar with IPv4
 - Cisco NetFlow v9
- However, IPv6 extension header and ICMPv6 information are ignored

An IPFIX Template for Basic IPv6 Flows

Version=10		Length = Total Length
Export Time		
Sequence Number		
Source ID		
Set ID		Length
Template ID = 256		Field Count = 10
0	Src IPv6 addr = 27	Field Length = 16
0	dst IPv6 addr = 28	Field Length = 16
0	L4SrcPort = 7	Field Length = 4
0	L4Dstport = 11	Field Length = 4
0	Next Header = 193	Field Length = 4
0	FlowLabel = 31	Field Length = 4
0	First time = 22	Field Length = 4
0	Last time = 21	Field Length = 4
0	OctetDeltaCount = 1	Field Length = 4
0	packetDeltaCount = 2	Field Length = 4

Measurement of Extended IPv6 Flows with New IPFIX Templates

- Extended IPv6 flows
 - IPv6 extension headers (EH) or ICMPv6
- Why important ?
 - Various normal usages of IPv6 EH and ICMPv6
 - IPv6-specific features such as address auto-configuration, router advertisement, MIPv6
 - IPv6 anomaly traffic exploiting
 - IPv6 EH
 - ICMPv6

IPv6 EH-related Anomaly Traffic

- Attack hosts under address auto-configuration
 - ICMPv6 NS/NA messages are exploited
 - The Hackers' Choice Attack Tool (<http://thc.segfault.net>) in 2006
 - Known vulnerability in IPv6
 - IETF Secure Neighbor Discovery (SEND) is not fully deployed
- IPv6 routing header vulnerability
 - DoS attack at Cisco IOS reported in 2007

IPv6 EH-related Anomaly Traffic (cont' d)

- Covert channels
 - Secret communication path
 - Popular in IPv4
- IPv6 covert channels with IPv6 EH
 - T. Graf, Messaging over IPv6 Destination Options, 2003
 - N. B. Lucena et al., Covert Channels in IPv6, 2005

How Can We Monitor Extended IPv6 Traffic ?

- Define new IPFIX templates with the following information elements
 - ICMPv6 NS/NA-related information
 - (src MAC addr, dst MAC addr, target IPv6 addr)
 - IPv6 extension header information
 - (IPv6 extension header flag)
 - Mobile IPv6 information
 - (Mobile IPv6 BU/BA)
 - (Tunneled IPv6 flows)

IPFIX Template for ICMPv6 NS/NA

Set ID	Length
Template ID = 301	Field Count = 12
0 Src IPv6 addr = 27	Field Length = 16
0 dst IPv6 addr = 28	Field Length = 16
0 Next Header = 193	Field Length = 4
0 First time = 22	Field Length = 4
0 Last time = 21	Field Length = 4
0 OctetDeltaCount = 1	Field Length = 4
0 packetDeltaCount = 2	Field Length = 4
0 icmpTypeIPv6 = 178	Field Length = 4
0 icmpCodeIPv6 = 179	Field Length = 4
0 srcMacAddr = 56	Field Length = 6
0 dstMacAddr = 80	Field Length = 6
0 TargetIPv6addr = 200	Field Length = 16

- ICMPv6 NS/NA
 - (icmp code, icmp type, src MAC addr, dst MAC addr, target IPv6 addr)
- Usage
 - DAD in IPv6 auto configuration
 - Attack known as “new-dos-IPv6”

IPFIX Template for IPv6 EH

Set ID	Length
Template ID = 303	Field Count = 12
0 Src IPv6 addr = 27	Field Length = 16
0 dst IPv6 addr = 28	Field Length = 16
0 L4SrcPort = 7	Field Length = 4
0 L4DstPort = 11	Field Length = 4
0 Next Header = 193	Field Length = 4
0 TrafficClass = 5	Field Length = 4
0 FirstTime = 22	Field Length = 4
0 LastTime = 21	Field Length = 4
0 IPv6ExtensionHeaders = 64	Field Length = 4

- IPv6 EH
 - (flag)
- Usage
 - Various in normal
 - E.g., MPv6
 - Anomaly
 - E.g., covert channel

IPFIX Template for MIPv6

Set ID	Length	
Template ID = 257	Field Count = 12	
Fields for basic IPv6		
0	MIPv6MsgType = 200	Field Length = 4
0	MIPv6CoA = 201	Field Length = 16
0	MIPv6HAAAddr = 202	Field Length = 16
0	MIPv6HomeAddr = 203	Field Length = 16
0	MIPv6MsgSeqNum = 204	Field Length = 4

- BU/BA in MIPv6
 - Handover signal
 - (BU/BA, CoA, HAA, HoA, SEQ)
- Usages
 - Tracking handover events in MIPv6
 - Computing handover latency

IPFIX Template for MIPv6 (cont' d)

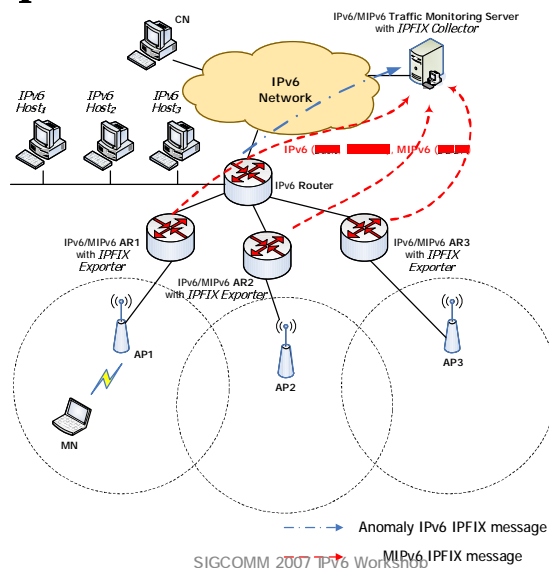
Set ID	Length	
Template ID = 258	Field Count = 12	
Fields for basic IPv6		
0	IPv6TunnelSrcAddr = 300	Field Length = 16
0	IPv6TunnelDstAddr = 301	Field Length = 16
0	TunnelProto = 302	Field Length = 4

- Tunnelled IPv6 flow
 - in MIPv6 without R0
 - (tunnel src addr, tunnel dst addr, proto)
- Usage
 - Computing user-perceived handover latency in MIPv6

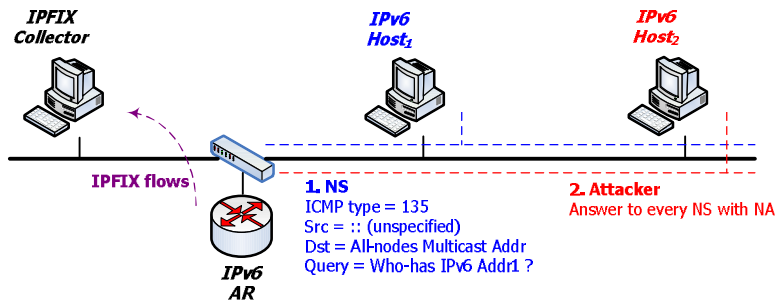
Experiments

- IPv6/MIPv6 network testbed
 - Linux PC routers/hosts with 802.11g cards
 - Software
 - MIPv6: MPL v2.0
 - IPFIX probe: modified nProbe
 - IPFIX flow collector/analyzer: our implementation and modification
 - WinIPFIX for detecting anomaly IPv6 traffic
 - Nfsen, RRD for MIPv6 flow
- Test traffic
 - iPerf, DVTS for video streaming
 - Anomaly traffic
 - THC: new-dos-attack
 - IPv6 covert channel

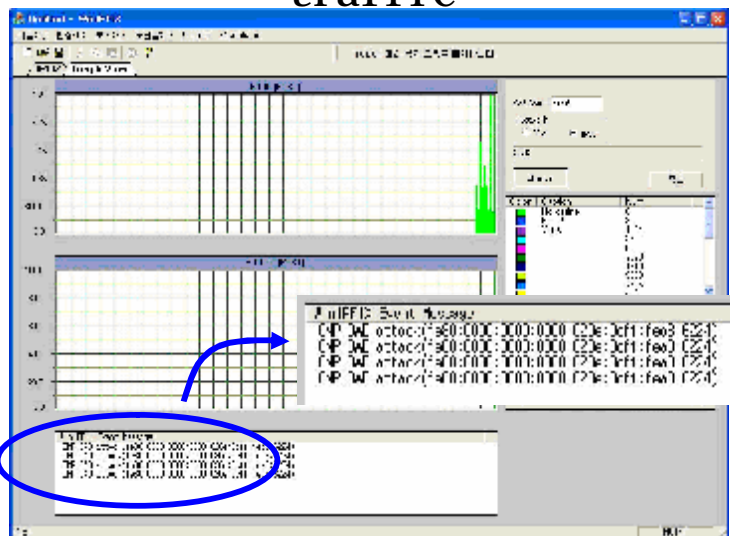
Experimental Environment



IPv6 Anomaly Traffic: new-dos-IPv6



Results - detecting new-dos-IPv6 traffic



The terminal window shows a chat session:

```

root@yale:/home/gale/tastry/fig ./fig.sh -n bob
MultiCast Mode: 1902::1
alice hello
bob hello
alice hello
bob hello
alice- hello bob
bob- can you hear me ?
yes
bob- yes
alice- this is really cool
great
bob- great
alice- chatting over ip6?
right right, nobody can hear
bob- right right, nobody c
alice- nev, let's start st
sure go ahead
bob- sure go ahead
neev
bob- neev
alice- what
  
```

The Wireshark window shows a packet capture of an IPv6 Echo Reply message:

No.	Time	Source	Destination	Protocol	Info
1	0.000000	fe80::20c:5bff:fe5:bae1	fe80::1	SIPv6	SIPv6 Echo Reply
2	0.000000	fe80::20c:5bff:fe5:bae1	fe80::1	SIPv6	SIPv6 Echo Reply
3	0.000000	fe80::20c:5bff:fe5:bae1	fe80::1	SIPv6	SIPv6 Echo Reply
4	0.000000	fe80::20c:5bff:fe5:bae1	fe80::1	SIPv6	SIPv6 Echo Reply
5	0.000000	fe80::20c:5bff:fe5:bae1	fe80::1	SIPv6	SIPv6 Echo Reply

Detailed packet details for packet 2:

- Ethernet II, Src: Netgear_c81be44 (00:09:5b:c5:be44), Dst: IPv6-neighbor-discovery_00:00:00:00:00:00 (03:00:00:00:00:00)
- Destination: IPv6-neighbor-discovery_00:00:00:00:00:00 (03:00:00:00:00:00)
- Source: Netgear_c81be44 (00:09:5b:c5:be44)
- Type: IPv6 (0x0006)
- Internet Protocol Version 6
 - Version: 6
 - Traffic class: 0x00
 - Flow label: 0x000000
 - Payload length: 74
 - Next header: IPv6 destination option (0x03)
 - Hop limit: 64
 - Source address: fe80::20c:5bff:fe5:bae1
 - Destination address: ff02::1
- Next header: ICMPv6 (0x03a)
 - Length: 2 (24 bytes)
 - Internet Control Message Protocol v6
 - Type: 129 (Echo Reply)
 - Code: 0
 - Checksum: 0x6516 (correct)
 - TTL: 0x0000
 - Sequence: 0x0000
 - Data (42 bytes)

Results – detecting IPv6 EH traffic including covert

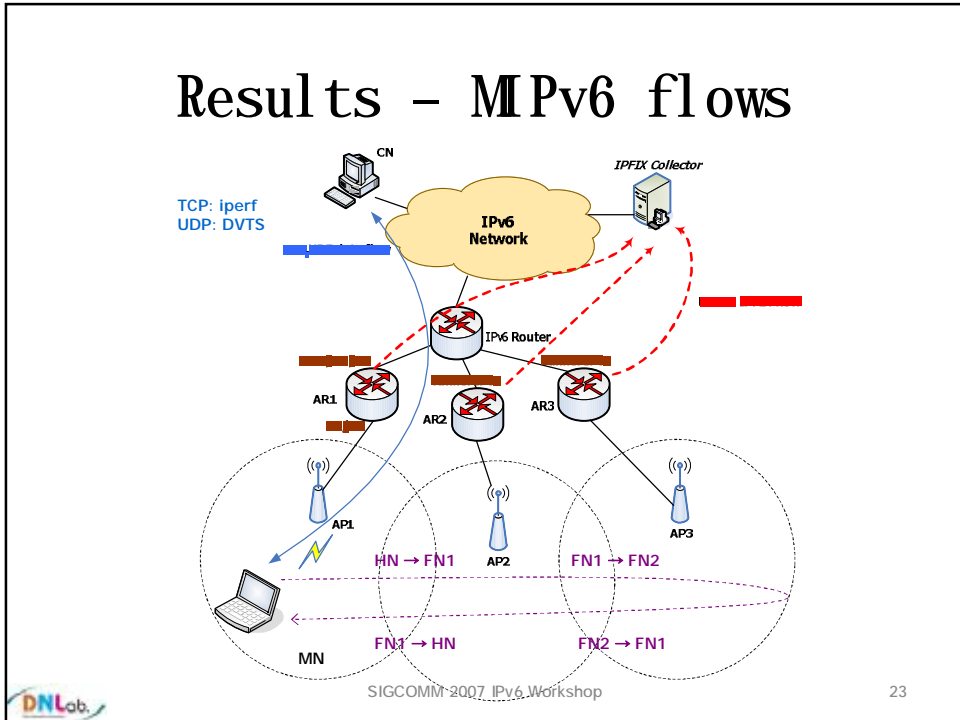
The NetworkMiner tool interface displays a traffic graph and a list of detected messages:

Messages:

- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1
- IPv6 Echo Reply: covert Conn: fe80::20c:5bff:fe5:bae1 -> fe80::1

The interface also shows a traffic graph with a blue arrow pointing to a specific data point.

Results - MPv6 flows



Results - handover delays

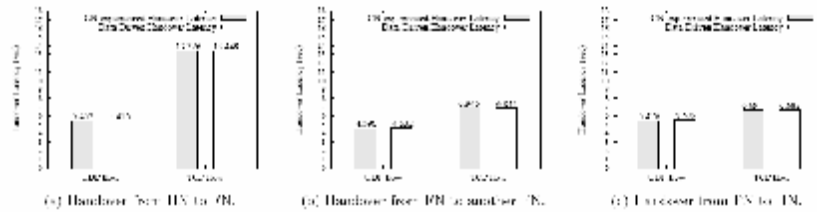


Figure 8: Upload IPv6 flow with handover in MIPv6 networks.

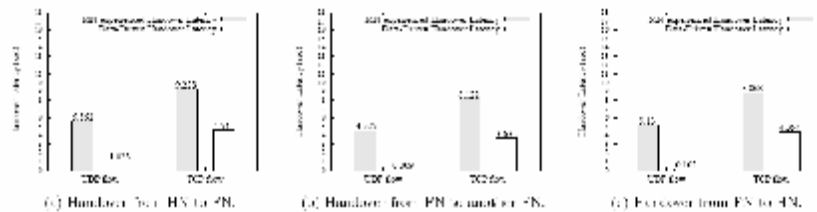


Figure 9: Download IPv6 flow with handover in MIPv6 networks.

Conclusion

- Propose new IPFIX templates for detailed IPv6 traffic analysis
 - Detect anomaly IPv6 traffic
 - E. g. , ICMPv6 or IPv6 EH
 - Capture handover events and compute user-perceived handover performance in mobile IPv6 networks
- Issues
 - Computation overhead with various templates at routers
 - Packet sampling