

Security Considerations for Intrinsic Monitoring within IPv6 Networks: Work in Progress

Alan Davy and Lei Shi

Telecommunication Software&Systems Group,
Waterford Institute of Technology, Ireland
adavy,lshi@tssg.org

Abstract. Intrinsic Monitoring is a method of collecting and disseminating node specific monitoring data throughout an IPv6 network by using the IPv6 extension headers as a carrier medium. The advantages of such a monitoring mechanism can be invaluable to a network operator, offering a wide range of performance and accuracy enhancements over traditional SNMP based or active probing based approaches. This paper discusses previous proposals related to Intrinsic Monitoring and highlights a number of security considerations that must first be resolved for such an approach to be deployable within an operational IP network. The paper offers initial contributions towards addressing these challenges.

1 Introduction

Nowadays network monitoring systems are crucial to communication networks. They periodically collect network performance metric values, identify performance anomalies, and determine root causes for the problems. Their effectiveness and efficiency determine the quality of network services. The most important performance metrics include connectivity, delay, packet loss rate, location of congested network nodes, and bandwidth information.

There are typically three ways to do the monitoring: active, passive and intrinsic. The intrinsic monitoring technique is viewed as a hybrid of active and passive monitoring approaches. In the intrinsic monitoring method, any added measurement data is piggybacked onto real user packets. It will receive the same treatment and follow the same path as original user traffic. Thus an accurate reflection of the characteristics of the real user traffic flows can be provided. On the other hand, the overhead is the additional systematic processing delay.

The basic idea is that the performance of a data flow can be monitored between a source-destination pair by inserting specific information in an extension header of select IPv6 packets in the data flow. By initiating an extension header at a source, and updating the extension header at any intermediate nodes along the source-destination path, a destination node can have a performance evaluation of select nodes in a network based upon the reported data in the IPv6 extension header.

The Internet is operated by thousands of interconnected ISPs, each ISP would like to keep their operational information as secret, such as IP address allocation,

packet loss rate, etc. Moreover, monitored information is vulnerable to malicious attacks and data corruption due to the complexity of networks. It is, therefore, important to ensure security properties, such as data confidentiality, integration of the monitored data in the IPv6 extension header and authentication of origin. In this paper, we present a secure method for obtaining and reporting monitored information based on a proposed IPv6 hop-by-hop options header.

The rest of the paper is organized as follows. Section 2 summarizes related work. In Section 3, we define the requirements for the secure intrinsic monitoring. In Section 4, we first presents the design of *hop-by-hop monitoring option header*, then we discuss system assumptions and propose our method to protect the monitored data. Finally Section 5 concludes the paper and discusses future work.

2 Related Work

The utilization of IPv6 hop-by-hop options header has been studied in [1, 6, 7]. A method is proposed in [7] to accurately and efficiently determine the network bandwidth in IPv6 networks through the use of a proposed IPv6 timestamp hop-by-hop options header. In RFC draft [1], another new IPv6 hop-by-hop option, RR6 option, extension is defined. Based on that, a "Record Route for IPv6" mechanism is described. In RFC draft [6], IPv6 hop-by-hop options header is used to record information along a communication path. The collected information includes interface attributes and statistics such as IP address, speed, number of transmitted packets and so on. These RFC drafts were rejected mainly because of the lack of security consideration.

All the above work does not consider the implications of the security, which makes the deployment far from the reality. IPv6 has its own IP Security (IPsec) [5] protocol suite to provide security services at the IP layer. It enables communication nodes to establish mutual authentication, negotiate cryptographic keys, select required security protocols and determine the algorithms to use. Two fundamental elements of IPsec are Encapsulated Security Payload (ESP) [4] and Authentication Header (AH) [3]. However, neither ESP nor AH could encrypt and authenticate the augmentable IPv6 hop-by-hop options header.

3 Security Considerations for Intrinsic Monitoring

Information security is critical for the monitored information dissemination. In this section, we focus our security considerations on the monitored data confidentiality, integrity and authentication of origin. Confidentiality means stored or transmitted monitored information cannot be read or altered by an unauthorized party. The monitored performance information is proprietary for ISPs and they would not be willing to disclose their internal network structure and performance information details. Integrity means any alteration of transmitted or stored monitored information can be detected. The receiver should be able to detect altered information to prevent misinterpreting the meaning of the original

data or even malicious attacks. Authentication of origin ensures the monitored data from trusted sources.

There are few requirements for doing the authentication and encryption to achieve the information security purpose. First, the amount of encrypted data should be reduced to minimum because encryption is computationally expensive. Each network node should only encrypt the data it inserts to reduce the encryption overhead. The second is to limit the authentication overhead to minimum. The network node should only authenticate the data it inserts to reduce the authentication overhead. Both the encryption and authentication is computationally expensive, so it is important to use suitable encryption and authentication algorithms to reduce the requirements for computing resource.

4 Protecting the Hop-by-Hop Options Header

A *hop-by-hop monitoring option header* is composed of a header and multiple performance metric records as shown in Table 1. This design aligns all the information into a 32-bit word boundary.

Table 1. IPv6 Hop-by-hop Monitoring Option Header Format

Next Hdr	Hdr Ext Len	Option type	Option Type
Sequence Number			
Record Count	Num of Metrics	Flags	Record Hdr Length
Identifier 0	Identifier 1	...	Padding
IPv6 address(optional)			
SPI			
Node Position 0	Num of supported Metrics	Authentication data length	Record Length
Identifier 0	Identifier 1	...	Padding
Identifier0 Data			
Identifier1 Data			
...			
IdentifierN Data			
Padding and padding length			
Authentication Data			
...			
SPI			
Node Position N	Num of supported Metrics	Authentication data length	Record Length
Identifier 0	Identifier 1	...	Padding
Identifier0 Data			
Identifier1 Data			
...			
IdentifierN Data			
Padding and padding length			
Authentication Data			

It is flexible to use the IPv6 Hop-by-hop options to collect monitoring information. Firstly, the *hop-by-hop monitoring option header* can indicate all performance metrics it interests. Example identifier values are listed in Table 2. Second, it can also specify the nodes it is interested to monitor. Routing header

options could be used together to monitor designated intermediate nodes. Third, an IPv6 address could also be include in the *hop-by-hop monitoring option header* to indicate a specific node and only the information from this node be collected. Fourth, it is also possible to collect all the intermediate nodes information because IPv6 hop-by-hop option will be processed by every router along the path.

Table 2. Identifier values for monitoring metrics

Value	Identifier
1	Num of packets forwarded
2	Num of packets discarded
3	Num of packets received
4	Portion of packets with ECN bit marked
5	Number of packets with ECN bit marked
6	Available bandwidth
7	Congestion Points
8	TimeStamp

Now we present our method of protecting the *hop-by-hop monitoring option*. As Internet Key Exchange version 2 protocol (IKEv2) [2] is integrated as a core component of IPv6 protocol stacks, we assume that it is supported by every network node. A protocol, for example an extended ICMPv6 protocol, initiates IKEv2 protocol for all nodes along the path in order to create IPsec Security Associations (SAs) with the destination node. SA includes keys, key lifetime, encryption and authentication algorithm, and related parameters.

IKEv2 offers a reliable and efficient key exchange scheme to provide a secure data transport. It also defines procedures to establish, negotiate, modify, and delete SAs. The advantage of IKEv2 is that it enables on-demand creation of keys for SAs and facilitates the use of keys in a large distributed system.

Our method is a combined encryption and authentication method. After the SAs are created, each node along the path shares a secret key with the destination node. Even each node has pair of private and public key, asymmetric algorithms use significant computational resources in comparison with their symmetric counterparts and therefore are not chosen to encrypt monitored data.

The symmetric encryption algorithms use a single key to encrypt and decrypt the data. The advantage is that symmetric algorithms use significantly less computational resources than their asymmetric counterparts. This single key is exchanged securely before the secure communication using key management protocols in IPsec framework. Typical key sizes are 64, 128, or 192 bits. Fig 1(a) shows how a shared secret key is used for protecting confidentiality of each record. The data portion starting from *node position* until *padding length* field (inclusive) is encrypted.

Message Authentication Code (MAC) algorithms are used for authentication and data integrity purpose. The MAC is the *authentication data* field of each record in the IPv6 *hop-by-hop monitoring option header* which is computed on the message using the shared key. The authenticated data starts from *SPI* until

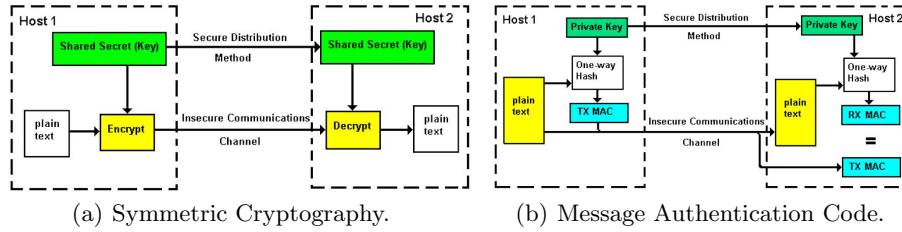


Fig. 1. Encryption and authentication.

padding length field (inclusive). After the receiver gets the message, it recomputes the *authentication data* using the authentication algorithm and shared key, then compares the result with the received *authentication data* field. If they are equal, the authentication is successful. The process is shown in Fig 1(b). The shared secure key authenticates the sender, and the hashed result ensures data integrity.

In a typical scenario, there are one sender, one receiver, and multiple intermediate nodes. The procedures can be summarized as follows: The sender initiates monitoring by creating a *hop-by-hop monitoring option* header, which indicates the interested performance metrics. Packets will be selected, e.g. from a specific application, according to the monitoring purposes.

An intermediate router receives the packet with *hop-by-hop monitoring option header*, it recognizes it is a monitoring packet. After decapsulating the packet, it collects its performance metric values according to the requirements and generate a monitoring record. It then encrypts this record using the shared key. The authentication data will be generated for the encrypted record only. Finally, the encrypted data and the authentication data will be inserted into the *hop-by-hop monitoring option header* as a record following the format defined in Table 1.

The destination node receives the monitoring packet and processes records one after another. Each record is associated with a *SPI* field, which identifies the SA to which this monitoring record belongs. The encryption and decryption is very computationally expensive, so the decryption should be done for the receiver after the successful authentication. The destination node authenticates the monitoring record using the key from corresponding SA, applies the hash algorithm to the encrypted monitoring record, and if the results match, then both the authenticity of the sender and the integrity of this monitoring record are assured. Then the decryption algorithm and key associated with the SA decrypt the monitoring record. The monitoring record will be processed by the destination node one by one until it finishes or error occurs.

This secure method has a growth in solution effort that is linear in the size of the nodes along the transportation path.

5 Conclusions and Further Work

In this paper, we have proposed a secure method for collecting monitored network information utilizing the IPv6 hop-by-hop headers. A generic IPv6 hop-by-hop option header which can be easily extended to include all the possible monitored information has been designed. We suppose that nodes are deployed with IPsec framework support, and a protocol, such as extended ICMPv6, initiates the key distribution and SA negotiation between the nodes along the flow transfer path and the destination node. Based on that, we have also discussed a light-weight information encryption and authentication scheme to securely transport collected monitoring information. To our knowledge, it is the first try to offer a generalized IPv6 hop-by-hop option header for all kinds of monitoring purpose with security consideration, which is a significant step for inline monitoring towards real deployment.

Several issues will need further investigation: 1) Due to the expensive computational cost of the IKEv2 exchange, which mainly includes the Diffie-Hellman key exchange, certificate handling and the authentication processing steps, IKEv2 requires quite some time for session establishment. The monitoring may conduct periodically to collect performance information to ensure the optimized operations of communication networks. Essential future work will seek fast reestablishment of the sessions when session expires or network problems occur. 2) An efficient and optimized compression method for monitored information in order to transport collected performance records efficiently.

References

1. L.Toutain A.Durand, *Ipv6 traceroute option*, IPv6 Working Group Internet Draft, June 1997.
2. C. Kaufman, *Internet Key Exchange (IKEv2) Protocol*, RFC 4306 (Proposed Standard), December 2005, Updated by RFC 5282.
3. S. Kent, *IP Authentication Header*, RFC 4302 (Proposed Standard), December 2005.
4. _____, *IP Encapsulating Security Payload (ESP)*, RFC 4303 (Proposed Standard), December 2005.
5. S. Kent and K. Seo, *Security Architecture for the Internet Protocol*, RFC 4301 (Proposed Standard), December 2005.
6. H. Kitamura, *Connection/link status investigation (csi) for ipv6 hop-by-hop option and icmpv6 messages extension*, Internet Draft, Work in Progress (1999).
7. Julie Baca Marshall Crocker, Georgios Lazarou and Joe Picone, *A bandwidth determination method for ipv6-based networks*, International Journal of Computers and Applications (2009).