Getting underlying information using cross-layer mechanism in transport study

Katsushi Kobayashi, ikob@ni.aist.go.jp
National Institute of Advanced Industrial Science and Technology (AIST) *

Abstract

Transparency inside a network must be required for the diversified internet. The previous works for the transparency have been focused on the network operator. Further, the disclosure policy is controlled by the operator. In this paper, we introduce a concept to provide the transparency from an end-system using in-band cross-layer approach in past transport studies. We also present privacy preserving mechanism which respects the policies, not only operators but also the end-system. This position paper shed a light to in-band cross-layer mechanism in Internet transport study viewpoint from operation, administration and maintenance.

1 Introduction

With diversification of network technologies, we have encountered many difficulties due to the lack of transparency inside a network deriving from the end-to-end principle as the followings.

Without any transparency inside these upcoming architectures, an end system cannot understand what was, is, or will be, happen on the network because the network is working under intelligent manners compared to a dumb network.

In studies on congestion control, the several approaches that an end system utilizes inside network information for TCP congestion control have been presented as PTP, ETEN, SIRENS [5, 2, 3, 4]. Hereafter, the above approaches are collectively called, "Explicit Network information Collection Along Path (ENCAP)" In ENCAP approaches, an end-system acquires inside information using an in-band cross-layer approach. ENCAP can handle any type of information on a network, although it was originally designed for congestion control. In this study, we utilize ENCAP as a generic information collection tool: this improves the transparency inside a network when the network is viewed from an end system. However, the current ENCAP approach discloses all the information along the path. In order to deploy ENCAP as a generic network transparency framework, we have to also provide a privacy-preserving function together. On the other hand, most of previous approach to improve the transparency is required a server to collect information from network device. In general, an end-system cannot access the collected information because the transparency is not for an end-system but for a network operator. Even in few approaches for an end-system, the server is also required, and the disclosure policy is managed by the operator.

In this paper, we introduce a concept to provide transparency inside a network path that presented in transport studies. We also present a privacy preserving mechanism with respecting disclosure policies among the end-systems and networks. In Section 2, we firstly discuss how the transparency inside a network contributes to the enhancement of a network system. We present related works in Section 3. In Section 4, we present the ENCAP approach, and discuss the issue of privacy. In Section 5, we present our concept of privacy-preserving mechanisms. Finally, we conclude this paper in the last section.

*This position paper is a modified version of author's earlier article entitled as "Better end-to-end visibility leads better networks" appeared in 3rd International Conference on Future Internet Technologies, Seoul, 2008

2 Transparency inside a network

A network router maintains information that is required for routing, such as routing tables, access control lists, and link utilization. In addition, a router stores information required for the network operation, e.g., a calendar clock, time zone, temperature, location, operator's contact detail, and charging information of a circuit. Such information can be accessed only by the network operators. However, if the information is disclosed to an end-system, the network provides improved end-to-end transparency inside a network.

More types of information can be provided by a router by using auxiliary devices or its interfaces, such as environmental sensors and GPS. The cost of the auxiliary system is negligible as compared with an expensive ISP router. Further, since the router, as part of an ISP infrastructure, is maintained with a higher quality operation as compared to almost all end systems, the information obtained from the network is expected to be of a better quality.

Although SNMP has been well deployed on network devices, a network infrastructure device usually rejects SNMP queries from an unknown end system. Because frequent SNMP queries degrades the device performance since the SNMP service is implemented on the management plane. A network device status and configuration can be changed with an SNMP operation. The system must take care of the action to change something on the device with the management plane.

However, the function to change a device status and configuration is beyond our scope, since our goal is just to collect information. Thus, a new information collection mechanism can be implemented with a different design not to involve the management plane.

3 Related Work

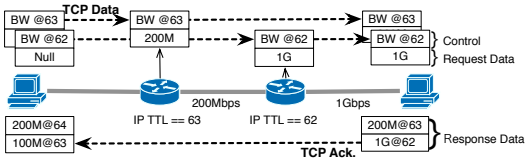
Most of tools and studies to provide transparency inside a network have been focused on operation, administration, and maintenance. Our goal of transparency is also to enhance functionalities of an end-system with enriching network information.

`traceroute` is mostly used diagnostic tools for obtaining end-to-end IP reachability information inside a network. Network management and monitoring system, such as HP OpenView and MRTG, collects the information of devices with polling and receiving trap mainly using SNMP. Only limited information and access are enabled on the system from an end-system. Since the system usually serves single administrative domain only, it is far to enable end-to-end transparency.

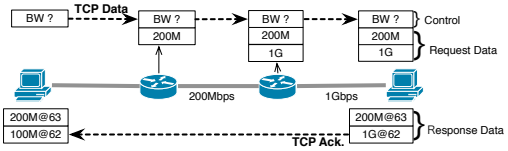
4 ENCAP and its privacy issue

ENCAP is an in-band feedback approach that involves routers, and it is designed as a thin layer between the network layer and the transport layer. In the ENCAP protocols (Fig. 1), a sender host sends an information request encapsulating into a usual packet, such as TCP data. When a router receives an ENCAP request packet, the router inserts or overwrites appropriate information into the ENCAP header, if required. A receiver sends back the collected information onto the feedback packet as TCP Ack. In the case of PTP, with increase in the packet size, all the router data along the path are stacked into a single packet. In SIRENS, since the data of only a specific hop router is collected by one packet, N packets are required to collect all the information along the path: N corresponds to the number of router hops between the sender and the receiver. Thus, ENCAP cannot provide any information without cooperation between the sender and the receiver. Moreover, ENCAP only provides information on restricted routers that are located on the packet path between the sender and the receiver.

ENCAP provides a scalable network information collection infrastructure. Because, ENCAP just requires small storage both only on sender and receiver, and ENCAP does not include any risk of state explosion on router. This scalability enables that an end-system continuously records the information even at "normal" condition. In some cases of network trouble, it is difficult to identify what is different, because of lacking the information of "normal" condition. It is a significant helpful to identify a trouble, if an end user can report the trouble with the information both at "normal" and "trouble".



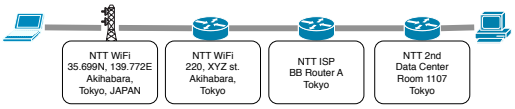
(a) SIRENS: a packet collects only one hop's information.



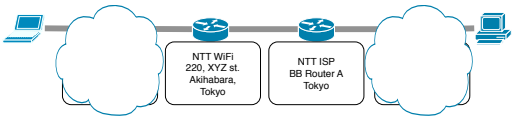
(b) PTP: only one packet collects information along the entire path.

Figure 1: Overview of ENCAP protocols, (a) SIRENS, (b) PTP.

(a) Network hiding inside.



(b) Path information of entire network disclosed.



(c) Network path is disclosed while privacy of both ends is preserved.

Figure 2: Privacy preserving model with ENCAP

In the ENCAP studies conducted to enhance TCP performance, an end-system collects the network path conditions, such as bottleneck bandwidth, queue capacity of an interface, and corruption loss. The TCP behavior is optimized by adjusting the congestion window size or redundancy level of FEC according to the conditions.

As mentioned above, the original ENCAP proposals focused on congestion control only. Information relevant to congestion was regarded as not containing any privacy-sensitive information. However, if we apply ENCAP to all types of data, we have to consider the issue of privacy.

Let us assume that a TCP connection in which ENCAP is available is established between Alice and Bob. However, Alice and Bob prefer not to reveal their respective locations to others, before they both agree to disclose their locations to each other. If Alice would like to know the geographical location of the WiFi router on her own uplink, Alice sends ENCAP location requests by using the TCP connection. Bob gathers the location information of all the routers along the connection path. Bob sends back the location data to Alice. Thus, Alice knows the location of her uplink router. However, if all the ENCAP data are encapsulated with plain text, Bob can determine Alice's location immediately, when the ENCAP packet is received by Bob. If all the ENCAP data are encrypted in order to prevent Bob from accessing the data, Bob cannot determine the type of information that is being retrieved by Alice.

5 Preserving privacy with ENCAP

Although we have considered many risks and threat models related to ENCAP, we cannot present all of them here due to limited space. Further, we cannot enumerate the requirements for privacy preservation. Therefore, we present our concept for managing ENCAP information while respecting the privacy policy of the sender, receiver, and network. Further, we discuss a threat model for ENCAP protocols.

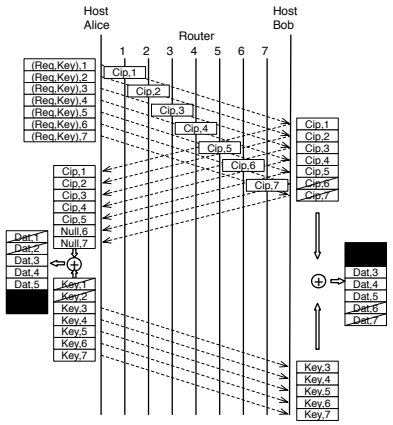
In order to implement the disclosure policy of the network, the network operator just applies the policy, such as whether the information on the router can be disclosed to everybody by an ENCAP request, or not. Different policies depending on the network operator are acceptable, though the information of the path is not a complete.

ENCAP requires three fields *control, request data,* and response data. The *control* field is used to specify the requested data for the use of a receiver and routers. The *request data* is updated by a router, which delivers the requisite information to a receiver. The *response data* carries back the collected data from a receiver to a sender. The *control* field should not be encrypted because every ENCAP router has to refer to it. Further, the

control field should not be modified by an intermediate router. This is because Bob should be able to determine the type of information that is being retrieved by Alice just by observing the control field. Bob stops sending the corresponding *request data*, when he decides not to disclose it. Therefore, the *control* field requires an end-to-end integrity protection mechanism, such as HMAC. The *response data* field does not require any new security mechanism because the *response data* does not involve any router action. It is sufficient for the *response data* to apply a deployed end-to-end security scheme, such as TLS.

In contrast to the abovementioned security scheme, which is aimed at sharing information between end-to-end systems, some contents of the *request data* field should be kept confidential from a receiver.

Our concept for preserving privacy is a simple: router information is selectively disclosed by designating whether or not a specific hop-count router information is disclosed. A selective disclosure mechanism can be realized as follows (Fig. 3): Alice generates a one-time encryption keys, and encapsulates the encryption keys into the ENCAP request packet. The number of keys corresponds to the *request data* field number. The router updates the *request data* field with the encrypted data and removes the used one-time key from the packet. If Bob can disclose the information type specified with the *control* field, he sends back the received *request data* encrypted by Alice's key. Even if the privacy policy of Bob does not allow disclosure of specific information type, he can decide that the information on the router far from his system is of less concern regard to his privacy. In this case, Bob selectively sends back the encrypted request data following his policy. Alice confirms the location with the ENCAP responses sent back by Bob. If Alice decides to disclose the location to Bob, Alice transmits the corresponding encryption keys to Bob. In the above scheme, we quietly use a symmetric encryption algorithm for the request data field. It assumes that Bob cannot capture ENCAP request packets before the key being removed by a router. If Bob can get an encryption key used by the router along the path, he can obtain the information before Alice. If the risk cannot be acceptable, we have to use asymmetric encryption with higher processing cost.

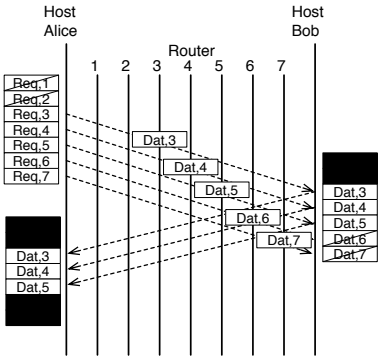


Both Alice and Bob prefer not to reveal the information up to second nearest routers from own host. Bob does not send back the ciphered text corresponding router 6 and 7 to Alice. Alice does not send Bob the decryption keys for the router 1 and 2. As the result, Alice knows the information from the router 1 to 5, and Bob knows from 3 to 7.

Figure 3: Privacy preserving on ENCAP:using encryption.

If no encryption mechanism can be used on the ENCAP router, a selective disclosure can be realized with a selective ENCAP information request. It is required in the ENCAP protocol that the ENCAP requester can designate hop count to collect information at the specific section in the path (Fig. 4). Alice requests Bob to sends ENCAP requests in order to collect the location information on the router near Alice. Bob sends ENCAP request packets by adjusting the hop count in order to designate the routers near to Alice. Alice knows the router locations around her by receiving the ENCAP request packets without revealing the location information on Bob side.

One threat model for the ENCAP system is that an end system can report a bogus network topology behind the actual end point by crafting the ENCAP response data. ENCAP essentially includes this risk by a phantom network topology, and this type of threat cannot be prevented. However, the risk is not a significant and it is a manageable. That is because, an end system cannot tamper with the real network information collected by the ENCAP packet sent from itself. In congestion control,



Both Alice and Bob prefer not to reveal the information up to second nearest routers from own host. Alice does not send the request for the router 1 and 2. Bob does not send back the data at the router 6 and 7. As the result, Alice knows the information from the router 3 to 5, and Bob knows from 3 to 7. If Alice would like to knows the router 1 and 2, Alice requests Bob to make the reverse action.

Figure 4: Privacy preserving on ENCAP:without encryption.

even if an end system pretends under better conditions than the real network, the transport stack optimizes itself considering the worst condition instead of the better one, such as bandwidth bottleneck. In content distribution with regional restriction, content leaks to outside can be detected from the router locations of the path. If a malicious user in Japan attempts to procure videos licensed in USA by forging his own location and network, the location of the user access managed by ISP is still included in the router locations on the path.

6 Conclusion

In this paper, we have provided the rough sketch of a protocol used for preserving privacy by using ENCAP. We recognize that there should be many issues in this protocol. However, we believe that better transparency inside the Internet can lead to significant advantages in network applications and end systems, and the ENCAP approach can be used to enhance the transparency.

From the view point of the knowledge plane, our transparency mechanism is a step to realize *sensor* component supporting privacy[1]. However, at the knowledge plane, network infrastructure, that is router, changes own behavior according the situation. Therefore, in order to provide complete *sensor* set for the knowledge plane, we have to develop a scalable transparency mechanism viewed from intermediate-node as well as from the end-system proposed by this paper.

7 Acknowledgement

This study is partially supported from future network research and development of NICT (National Institute of Information and Communications Technology), Japan.

References

[1] D. Clark, C. Partridge, J. Ramming, and J. Wroclawski. A knowledge plane for the internet. *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications*, pages 3–10, 2003.

[2] R. Krishnan, J. Sterbenz, W. Eddy, C. Partridge, and M. Allman. Explicit transport error notification (ETEN) for error-prone wireless and satellite networks. *Computer Networks*, 46(3):343–362, 2004.

[3] K. Nakauchi and K. Kobayashi. An explicit router feedback framework for high bandwidth-delay product networks. *Computer Networks*, 51(7):1833–1846, 2007.

[4] P. Sarolahti, S. Floyd, and M. Kojo. Transport-layer considerations for explicit cross-layer indications. *Internet Draft, draft-sarolahti-tsvwg-crosslayer-01.txt*, 2007.

[5] M. Welzl. PTP: better feedback for adaptive distributed multimedia applications on the Internet. *Performance, Computing, and Communications Conference, 2000. IPCCC'00. Conference Proceeding of the IEEE International*, pages 330–336, 2000.