Automated Selection of Security Protocols in SINET

Xiaojie Wang[1,a], Ping Dong[1,b] and Fei Song[1,c]

[1] School of Electronic Information and Engineering, Beijing Jiao Tong University, P. R. China

{[a]15120147, [b]pdong, [c]fsong}@bjtu.edu.cn

Keywords: security protocols, security, quality of service, energy of consumption, automated selection, smart identification network

Abstract. Existing security protocols are only promoted or evaluated in one of the aspects of security or performance, but network users' demand for network security is diverse and varied. Providing one security protocol does not meet users' demand. Meanwhile, there is a severe phenomenon of wasting network resource. Thus, we propose a method of automated selection of security protocols (*assp*) in smart identifier network. This method helps to adjust the security configuration dynamically, and provides different security services for different service groups. Theoretical analysis shows that the method has advantages in performance, and has high practicability.

Introduction

With the development of science and technology, information science has become a great impetus to the progress of society nowadays. The application of network has penetrated into all aspects of human society such as politics, economy, culture and education. However, the openness of network makes the users and data face a lot of threat, so the network needs a robust security mechanism. In order to achieve network security protection at different layers of tcp / ip network architecture, various security protocols are prepared, such as *ipsec* protocol at network layer, transport layer security (*tls*) and secure sockets layer (*ssl*) at transport layer, and so on [1,2]. Ipsec provides end-to-end security services using encryption-based service protection and dynamic key management. Ssl/tls implements secure communication using authentication, signature, and encryption at transport layer.

However, most of the existing security protocols [3,4,5] are designed only taking one aspect of security and performance into account from the point of the designers, but different users need different network security mechanism. Some users need a higher security mechanism, but other users are more concerned about the efficiency of the mechanism's performance. Even to a same user, the demand of network security changes dynamically. For example, some users only browse news, web and video, etc., so they are not concerned much about the security of the protocol, but more concerned about the efficiency of the protocol and the impact on the latency. However, some others use online banking for online payment, etc., thus, they have a higher demand on the security of the protocol. Therefore, it is not appropriate for the network components to provide the same security mechanism for all services. Designers and developers should consider, for instance, latency, throughput, overhead data communication properties and hardware power consumption when designing services for pervasive environments. Providing a unified security mechanism for all users and all communications cannot satisfy customized services, moreover, it is a waste of network resources.

Smart identification network (*sinet*) [6] uses a new network architecture including three vertical layers and two horizontal domains. Sinet can identify and describe service intelligently, perceive service requirements and network state, and cluster the network components. Sinet is aimed at perceiving changes in service demand intelligently and scheduling network resources for adaptation dynamically. In this paper, we design a dynamic and adaptive security protocol selection method based on *sinet*. The method can select security protocols according to the changes of service demand. On the basis of satisfying security and efficiency requirements of the different network users, this method can improve utilization of network resources.

Smart Identifier Network

Sinet is vertically divided into three layers and horizontally divided into two domains. The three vertical layers include the smart pervasive service layer (*l-sps*), the dynamic resource adaption layer (*l-dra*), and the collaborative network component layer (*l-cnc*). The two horizontal domains include the entity domain (*d-en*) and the behavior domain (*d-be*). In *l-sps*, *sid* (service identifier) and *sbd* (service behavior description) are used to uniquely identify an intelligent service. In *l-dra*, *fid* (family identifier) and *fbd* (family behavior description) are used to identify a network function group. In *l-cnc*, *nid* (node identifier) and *nbd* (node behavior description) are used to uniquely identify a network node or component.

As shown in Fig.1, the architecture of *aasp* can divided into three parts. First, we use *sid* and *sbd* to describe the requirement of a service, including security requirement, *qos* (quality of service) requirement and energy consumption requirement. Second, the mechanism maps the service to the appropriate group. Finally, the group are mapped to the corresponding component for transmission.

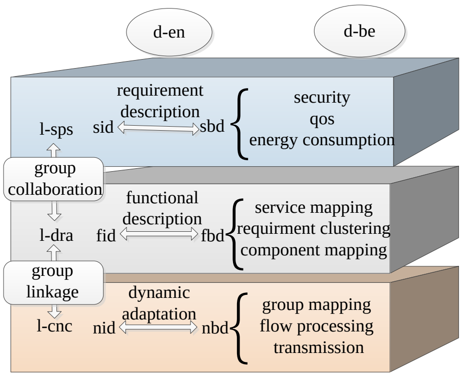


Fig.1 Architecture of aasp

Method Description

Service Description

A service can be identified using (sid, sbd) according to the service request made by the service requester. Sbd mainly describes the security demand level, qos demand and energy demand of the service. Among them, the security metric can be expressed by the following parameters: confidentiality, authentication and integrity. Qos metric can be expressed by the following parameters: latency, overhead and throughput. Energy consumption metric can be expressed by the following parameters: energy consumption of sending data, energy consumption of receiving data, energy consumption of cryptographic operations (Hash algorithm, key exchange algorithm, signature algorithm, encryption and decryption algorithm, etc.). Definition 1 provides a demand function definition for a service.

Definition 1: Let sid $\in sid$ denotes a service in the service identification set, and the demand definition for a service (*sid*) is represented by the parameters (p_j) and the weights (w_j), where 1$\leqslant$j $\leqslant$m. The function v_j is used to describe the availability of the parameter. The function v_j should be defined in advance to ensure repeatability. We use *s*, *q* and *e* to describe security needs, qos requirements, and energy consumption demand respectively. Each demand function can be expressed as follows.

$$s(sid) = \sum_{j=1}^{m_1} w_{sj} * v_{sj}(sid)\,. \tag{1}$$

$$q(sid) = \sum_{j=1}^{m_2} w_{qj} * v_{qj}(sid)\,. \tag{2}$$

$$e(sid) = \sum_{j=1}^{m3} w_{ej} * v_{ej}(sid). \quad (3)$$

Different services can be broadly divided into the following categories: voice and video streaming services, file transfers, message services and localization services. Different services have different demand, so we can use sbd to describe them. Equation (4) describes the definition of sbd.

$$sbd(sid) \triangleq (s(sid), q(sid), e(sid)). \quad (4)$$

Behavior Clustering and Component Matching

L-dra carries controlling information, and links the services in upper layer to the transmission in lower layer. It can send the service to the appropriate component to realize the intelligent service through two mappings.

The first mapping achieves the mapping from service identification to group identity. The method compares security metric, qos metric and energy consumption metric in service behavior description with every group description modules to select the best group function module for achieving the dynamic adaptation of service security mechanism and scheduling network resources collaboratively. Definition 2 provides a definition of group identity and group behavior description.

Definition 2: Let fid ∈ *fid* denotes a group in the group identity set, with a certain behavioral similarity within each group, which refers to a similar security requirement, qos requirement, and energy consumption demand. The description of their group behavior is defined as equation (5).

$$fbd(fid) \triangleq (f_s(fid), f_q(fid), f_e(fid)). \quad (5)$$

In equation (5), f_S denotes the security requirement of the group, f_q denotes the qos requirement of the group, and f_e denotes the energy consumption demand of the group. The demand of the same group are similar.

According to the above definition, each service can be mapped to the adapted group in order to provide a basis for the rational allocation of security protocols.

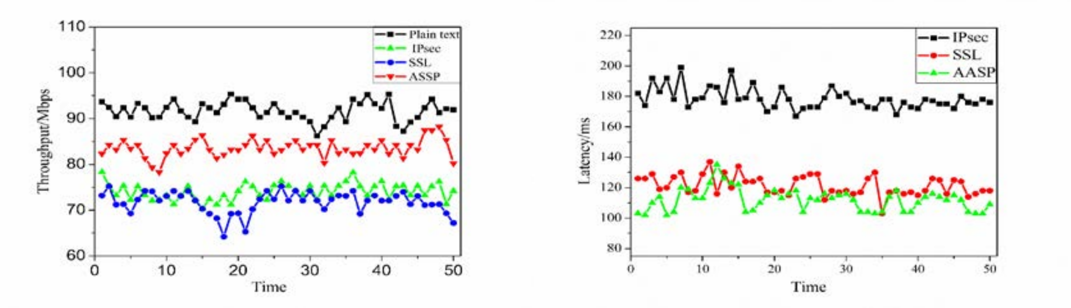
The second mapping achieves the mapping form the group to the corresponding network component. The network component will provide the security configuration required by the group. The security strength of the security protocol is mainly related to the algorithms (such as hash algorithm, key exchange algorithm, encryption algorithm, signature algorithm, etc.), but the choice of security protocol not only affects the security strength of the session, but also affects other aspects, such as qos and energy consumption. The main reason is that the cryptographic algorithms occupy the calculation resource. The cryptographic algorithm will consume additional memory and cpu resources, which will cause power consumption. In addition, the cryptographic algorithm will cause latency and latency jitter during packets processing, and will limite throughput. Therefore, in the choice of security protocols, we must consider its impact on qos and energy consumption.

Component Transmission

After the evaluation of security protocols in each network component, each group can be mapped to the corresponding network component for transmission. This process involves mapping process and service flow process. The component elects the protocol of the highest score according to the demand of the group it serves. The component who sends data will process the data by the configuration of the protocol elected and the component who receives data will process the data in reverse way.

Performance Analysis

We selected three different services (including video streaming, file transfer and online payment) for test. Then we compared *sinet*'s mechanism *assp* with traditional security protocols ipsec and ssl, tested in 100Mbps networks, comparing their throughput and the latency for 50 times for the sake of fairness, as shown in Fig.2.



(a) Throughput (b) Latency

Fig.2 Comparison of aasp with ssl and ipsec

The protocol we choose are *ipsec-esp-sha1-3des* and *ssl-3des-ede-cbc-sha*. As shown in Figure 2(a), the services processed by ipsec and ssl have lower throughput (average value 74.103Mbps and 71.780Mbps respectively), because protocol processing and encryption algorithm consume processing power of the processor. However, aasp has a higher throughput (average value 83.541Mbps) because it occupies different protocols and algorithms to the different services according to services' requirement. As shown in Figure 2(b), aasp has the minimum latency (average value 111.92ms), because the security protocol of each service is different so that the latency caused by encryption algorithm is smaller and ipsec has the maximum latency (average value 178.50ms) because the handshake time of ipsec is the longest.

The test shows that aasp has the highest throughput and the minimum latency comparing with ipsec and ssl. For networking components, using aasp can supply adaptive security protocols to different services to promote the quality of service.

Summary

This paper proposes a security protocol configuration and selection method in sinet. Based on the service security requirements, qos and energy consumption are considered. For the operation of the whole network system, the detailed method and the solution are provided in the three steps of service classification, behavior clustering and component transmission respectively. The theoretical analysis proves that the scheme has advantages in terms of performance. The network resource utilization can be promoted, thus the method can work practically.

References

[1] Schulz S, Varadharajan V, Sadeghi A R. The silence of the LANs: efficient leakage resilience for IPsec VPNs[J]. IEEE Transactions on Information Forensics and Security, 2014, 9(2): 221-232.

[2] Asadzadeh Kaljahi M, Payandeh A. TSSL: improving SSL/TLS protocol by trust model[J]. Security & Communication Networks, 2015, 8(9):1659-1671.

[3] He D, Kumar N, Lee J H, et al. Enhanced three-factor security protocol for consumer USB mass storage devices[J]. IEEE Transactions on Consumer Electronics, 2014, 60(1): 30-37.

[4] Eun H, Lee H, Oh H. Conditional privacy preserving security protocol for NFC applications[J]. IEEE Transactions on Consumer Electronics, 2013, 59(1): 153-160.

[5] Lee T F. Enhancing the security of password authenticated key agreement protocols based on chaotic maps[J]. Information Sciences, 2015, 290:63-71.

[6] Zhang H, Quan W, Chao H C, et al. Smart identifier network: A collaborative architecture for the future internet[J]. IEEE Network, 2016, 30(3):46-51.