Toward Bandwidth-efficient Data Distribution in Satellite Networks

Jianfeng Xu[1, a], Liming Wang[2, b], Chen Song[2, c], Ding Tang[2, d] and Zhen Xu[2, e]

[1]School of Cyber Security, University of Chinese Academy of Sciences, Beijing 100049, China;

[2]Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China.

[a]xujianfeng@iie.ac.cn, [b]wangliming@iie.ac.cn, [c]songchen@iie.ac.cn, [d]tangding@iie.ac.cn, [e]xuzhen@iie.ac.cn

Abstract. In the satellite communication system, the satellite-ground link acts as an intermediary connecting the space network with the terrestrial network. Unfortunately, this link has become a bottleneck due to bandwidth fatigue, which seriously threatens the availability of network services. Besides, as a typical open channel, the satellite-ground link faces numerous security threats, such as signal interception and interference. In response, solutions have been developed to mitigate such a bottleneck. However, the existing schemes cannot achieve the security and efficiency of transmission concurrently. In this paper, we propose a lightweight data distribution mechanism, which economizes the satellite-ground link bandwidth through request aggregation and service subscription. Meanwhile, it enables the secure transmission by employing digital signature technology. Further, to reduce the service delay, we design a caching mechanism based on resource popularity prediction. Simulation experiments validate the higher bandwidth efficiency of our solution, and thus greatly improving the availability of satellite services.

Keywords: Satellite network; satellite-ground link; data distribution.

1. Introduction

With the continuous advancement of terrestrial networks and mobile communication networks represented by 5G, users have proposed specific requirements for the next generation network infrastructure, such as ultra-high-speed transmission, ultra-bandwidth, ultra-high reliability, seamless coverage and ready access [1]. Satellite network [2], due to its vast coverage, has received widespread attention in next generation network research. Nowadays, the applications of satellite communication network, such as offshore fishing, energy exploration and disaster prevention, gradually involve all aspects of human life.

In recent years, network researchers have carried out extensive efforts on satellite network architecture, network management, routing, mobility management, etc. This paper, as a supplement, delivers a lightweight solution regarding secure data distribution against the problems exposed by the satellite-ground link. Serving the intermediary connecting the space network with the terrestrial network, the satellite-ground link with limited bandwidth resources introduces a high overhead to communication. Additionally, such a link faces numerous security threats such as signal interception and interference, due to its openness. Therefore, how to effectively utilize the satellite-ground link bandwidth while ensuring the transmission security is a practical challenge to be solved urgently.

The satellite-ground link is more sensitive to computational overhead and transmission overhead in data transmission protection schemes. Currently, the traditional communication protocols and security schemes have certain limitations, which cannot satisfactorily meet the stringent requirements of the data transmission between satellites and ground. The researchers are mitigating these problems in the satellite environment primarily by improving traditional solutions. [3] applies IPSec in the performance-enhanced gateway PEP of the satellite IP network, which improves the performance of TCP/IP on the satellite IP network, and enhances the security of the satellite network. [4] Introduces a layered architecture extension in IPSec, called CL-IPSec, to provide authentication and integrity services. Based on the original IPSec-PEP, [5] proposes a certificate-based multiple key exchange protocol to avoid the key distribution problem. Insufficiently, the existing solutions cannot guarantee the transmission efficiency and security concurrently over the resource-limited satellite-ground link.

Specifically, the IPSec protocol is widely used to protect unicast traffic, that is, the satellite needs to respond to each user request, so that the repeated responses are transmitted. Moreover, the IPsec and its enhanced protocols bring complexity design cost and distribution overhead for overweight keys.

In this paper, we design a lightweight data distribution and protection mechanism based on request aggregation and service subscription, considering the limited bandwidth resources of satellite-ground link. Further, we propose a caching mechanism that employs popularity-based replacement strategy to reduce the service response latency.

The remainder of this paper is organized as follows. We state the research background and motivation in Section 2. The design of our mechanism is detailed in Section 3. Section 4 reports the evaluation results. At last, we conclude our work in Section 5.

2. Background

2.1 Satellite Network.

As the core infrastructure of informationized warfare, the satellite and its terrestrial infrastructure together constitute a satellite network which plays an extremely important role in earth observation, navigation and positioning. For the convenience of description, we abstract the entire satellite network into three layers: the spatial layer, the ground layer and the user layer, as shown as Figure 1. The spatial layer is composed of communication satellites of different orbits, whose networking mode is not the focus of this paper, and thus we omit it here. The ground layer includes various ground stations and control centers to manage and monitor the satellites. The user layer contains a variety of fixed or mobile devices that are connected to the ground layer via wired or wireless networks.

Fig. 1 Global architecture of satellite networks

2.2 Satellite-ground Link.

The satellite-ground link serves the communication between the ground layer and the space layer. However, with the increase of devices in the network, the limited bandwidth resources make satellite-ground link a bottleneck, seriously affecting the availability of satellite services. For instance, microwave communication between satellite and ground station typically has a transmission rate of only a few Kbps to tens of Mbps. Meanwhile, an adversary can easily offend the satellite-ground link to eavesdrop or tamper with sensitive information transmitted, due to its openness.

2.3 Motivation.

At present, several mechanisms have been developed, mainly focusing on the improvement of transmission performance or security, such as [3, 4, 5]. However, these schemes lack system city and versatility, and the computational overhead and communication overhead are relatively high. This

paper aims at proposing a lightweight data distribution and protection mechanism, comprehensively considering transmission security and efficiency.

3. Architecture

3.1 Overview.

Our mechanism includes seven functional modules: access management, identity management, key management, service subscription, message distribution, cache management and state audit, as displayed in Figure 2.
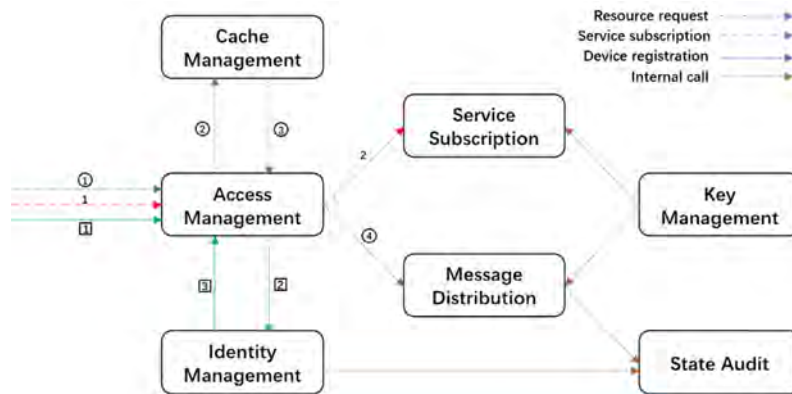

Fig. 2 Architecture overview

Access management module is to realize the communication with multiple devices, and completes the functions, such as identity generation, device registration, identity verification and authority. There are three types of messages received by this module: registration request, resource request and service subscription request. After receiving the registration request, the module first checks the legality of the device, and then returns an identity generated to device. Upon receiving the resource request and the service subscription request, the module checks the authenticity of the device and determines whether the device is permitted to access the resource or subscribe to the service. The function of identity management module is to store information of all registered devices to achieve data persistence, and provide corresponding operation interfaces to other modules. Similarly, key management module saves information such as the identity and public key of the managed satellite. Through these keys, we employ digital signature technology to achieve transmission security. State audit module is responsible for monitoring the running status of other modules and detecting abnormal events in time. Regarding the remaining three modules, we elaborate on their design below, due to their criticality.

3.2 Service Subscription.

Service subscription module focuses on services that actively push information. The most basic feature of these services is timeliness, such as flood monitoring applications. Once a disaster occurs, the place information is pushed from the satellite to devices immediately. This module maintains a hash table to store the device's service subscription information. The format of the entry is as follows:

$$entry = <Resource_i, [Dev_1, Dev_2, Dev_n]>$$

The above entry indicates that $Resource_i$ is subscribed by Dev_1, Dev_2 and Dev_n. With the service subscription module, the satellite only needs to send the same information to the ground station once, without having to transmit information to each device using unicast, thereby greatly reducing the bandwidth consumption of the satellite-ground link.

3.3 Message Distribution.

The message distribution module is responsive to the request-response service. This module converts multiple requests of multiple devices to the same resource into a request to satellite by aggregating the device's resource requests. To efficiently achieve request aggregation, the message distribution module maintains a forwarding status table, and the format of the saved entry is:

$$entry = <Resource_i, [Dev_1, Dev_2, Dev_n], time>$$

This entry indicates that, in the current state, Dev_1, Dev_2 and Dev_n initiate the same access request to $Resource_i$. Besides, time represents the moment when the first device requests $Resource_i$, providing richer information for state audit module. The message distribution module realizes the transition of multiple requests and responses to one request and one response by request aggregation, which quite improves the bandwidth utilization of the satellite-ground link.

3.4 Cache Management.

Currently, there are many services that are highly sensitive to network latency, such as games, on-line video live, and real-time communication. For these applications, even a small increase in response time degrades the user experience. Consequently, economic benefits are significantly reduced. To reduce the delay for devices to obtain resources, we introduce a cache management module. Notably, we design a replacement mechanism based on resource popularity prediction to improve the cache hit rate. To quickly achieve popularity prediction and minimize the consumption of computing resources, we design a prediction algorithm based on Taylor series.

We define resource popularity as the frequency of accesses to a resource within a statistical period and calculate it as follows:

$$Pop_i = \frac{\mathrm{Re}\,q_i}{N} \tag{1}$$

Where Pop_i indicates the popularity of $Resource_i$; Req_i indicates the number of accesses to $Resource_i$ in a statistical period and N indicates the total number of resource accesses. Besides, we set a global item, called *Counter*, to count the number of resource accesses in each period. When *Counter* reaches N which administrator predefines, it indicates the end of the current period. The cache management module maintains a table to record the historical popularity of each resource, as shown in Table 1.

Table 1. Historical Popularity of Each Resource

Resource	Period 1	Period 2	...	Period t
1	$Pop_1(1)$	$Pop_1(2)$	...	$Pop_1(p_t)$
2	$Pop_2(1)$	$Pop_2(2)$	...	$Pop_2(p_t)$
...	...	...	...	...
i	$Pop_i(1)$	$Pop_i(2)$	...	$Pop_i(p_t)$

Note that, in Table 1, $Pop_i(p_t)$ indicates the popularity of $Resource_i$ in period t. Based on the historical popularity, we predict the popularity of each resource in the next period. For $Resource_i$, we calculate the first and n_{th} derivative of resource popularity as follows:

$$Pop_i^{'}(p_t) = \frac{Pop_i(p_t) - Pop_i(p_{t-1})}{p_t - p_{t-1}} \tag{2}$$

$$Pop_i^{n}(p_t) = \frac{Pop_i^{n-1}(p_t) - Pop_i^{n-1}(p_{t-1})}{p_t - p_{t-1}} \tag{3}$$

Our module can predict the popularity of *Resource_i* in the period *t+1* based on the previous *k* (we set *k* as 3) predicted value and observed value according to the following formula.

$$P_i(p_{t+1}) = Pop_i(p_t) + ... + \frac{Pop_i^n(p_t)(p_t - p_{t-1})}{n!} + item \qquad (4)$$

Where *item* is defined as:

$$item = \frac{1}{k}\sum_{j=0}^{k-1} Pop_i(p_{t-j}) - P_i(p_{t-j}) \qquad (5)$$

Due to network instability, we attempt to assign coefficients for the derivative terms to make the Taylor series formula more general, and therefore, we obtain the resource popularity prediction formula as follows:

$$P_i(p_{t+1}) = Pop_i(p_t) + ... + a_n \times \frac{Pop_i^n(p_t)(p_t - p_{t-1})}{n!} + item \qquad (6)$$

a_n is the coefficient determined by the different network conditions, and the simulation results show that the ability to predict is greatly improved with coefficients.

Through the prediction algorithm, the cache management module can obtain the popularity of each resource in the next period. Accordingly, after receiving the response information from the satellite, our module will delete the content in the cache whose popularity is lower than the received information, so as to free up enough space for the highly popular resources.

4. Simulation

In this section, we evaluate G3S with simulation-based experiments and focus on answering the following questions: (a) How much satellite-ground link bandwidth the service subscription module and the message distribution module save for the delivery of satellite services? (b) How much cache hit rate is improved by the popularity prediction algorithm compared to Least Recent Used (LRU), First-In First-Out (FIFO) and Random replacement?

4.1 The Testbed.

Figure 3 illustrates the testbed network for our experiments. We construct a satellite network system by employing three Ubuntu virtual machines (VMs), which include VM 1 to simulate multiple devices making requests, VM 2 serving as a ground station, and VM3 providing services as satellite. Besides, we preset the link bandwidth between VM 1 and VM 2 to be 10 Gbps, while the link bandwidth between VM 2 and VM 3 is 1 Mbps.
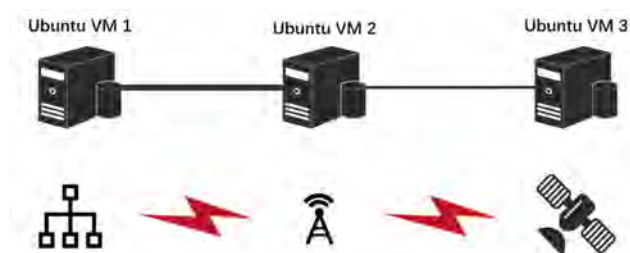

Fig. 3 The topology in our experiments

4.2 Bandwidth Efficiency.

We measure the impact of the service subscription module and the message distribution module on satellite-ground link bandwidth. VM3 returns a message with a size of 10 bytes for each received request. To evaluate the performance of the message distribution module, we employ scapy, a python library to simulate multiple devices requesting resources from the server. Figure 4 (left) shows the relation between the link bandwidth consumption and device count. We can see that, for the case of not using the message distribution module, as the number of devices in the network increases, the bandwidth consumption of the satellite-ground link increases gradually until the link is completely blocked. In another case, by using the message distribution module, many resource requests are aggregated, greatly reducing communication between the ground station and the satellite.
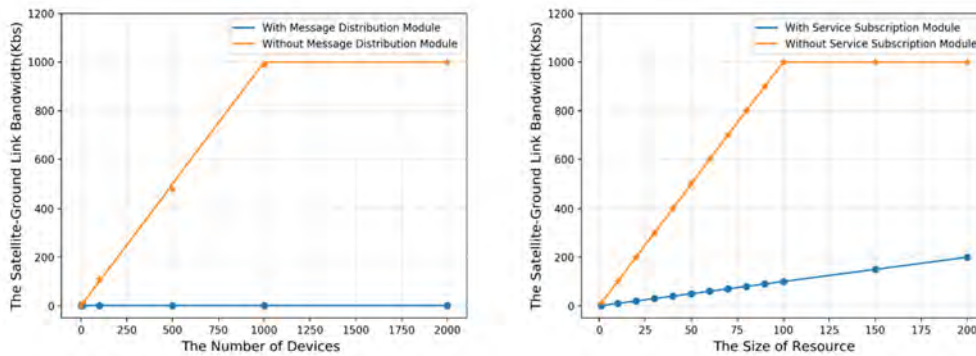

Fig. 4 Impact of message distribution module and service subscription module

As for the service subscription module, Figure 4 (right) illustrates the change of satellite-ground link bandwidth when the size of resource varies. We set up 10 devices in the network. From Figure 4, we can conclude that our mechanism can greatly save bandwidth resources by transforming the traditional unicast form into a multicast-like distribution mode, that is, for a network with n devices, we can reduce the bandwidth consumption to 1/n of the original consumption.

4.3 The Popularity Prediction.

We use a real packet traces, from a university data center used in [6], to evaluate our replacement mechanism based on resource popularity prediction. We first preprocess the data and obtain a total of 348 destination MAC addresses, and therefore, we assume there are 348 resources. The size of the cache is set to 30. We count the number of missing caches when using LRU, FIFO, Random and our replacement mechanism, respectively. Figure 5 (left) reveals that our replacement mechanism improves the cache hit rate by 30% compared to the suboptimal replacement mechanism, LRU. In addition, we measure the impact of the cache on latency, that is, the delay in which device gets the response. Figure 5 (right) shows that, in our experiment, the latency is 12.57 ms when using the cache, reducing the latency by about 40% compared to not using the cache.
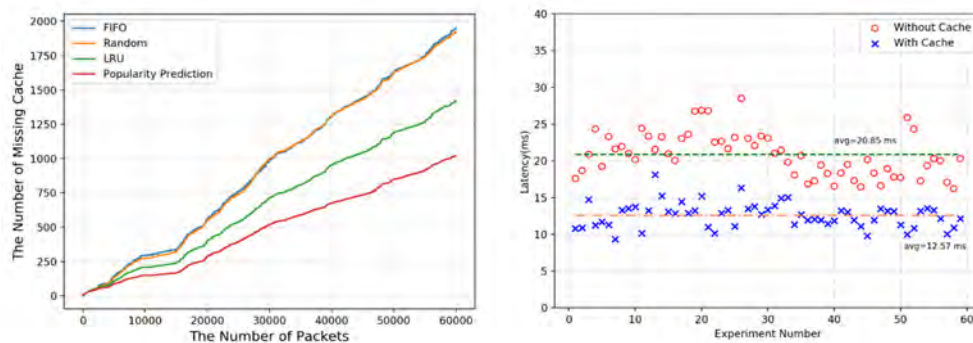

Fig. 5 Comparison of replacement mechanisms and the impact of cache mechanism

5. Summary

In this paper, we analyzed the effect of the limited satellite-ground link on the performance of satellite network system. To alleviate such a bottleneck, we designed a lightweight data distribution mechanism based on request aggregation and service subscription, which can greatly economize the link bandwidth, and thus improving the availability of satellite services. Furthermore, a caching mechanism based on resource popularity prediction was proposed to reduce service delivery delay. We experimentally demonstrated that our mechanism can greatly reduce the consumption of satellite-ground link bandwidth. Specifically, it can reduce the bandwidth consumption to 1/n of the original consumption for a network with n devices. Regarding transmission security, we achieve it through digital signature technology.

References

[1]. Sacchi C, Bhasin K, Kadowaki N, et al. Toward the "space 2.0" Era. Communications Magazine IEEE. Vol. 53 (2015) No. 3, p. 16-17.

[2]. Evans B, Werner M, Lutz E, et al. Integration of satellite and terrestrial systems in future multimedia communications. IEEE Wireless Communications. Vol. 12 (2005) No. 5, p. 72-80.

[3]. Djeddai, Lekhemissi, R. K. Liu. IPSecOPEP: IPSec over PEPs architecture, for secure and optimized communications over satellite links. IEEE International Conference on Software Engineering and Service Science. Beijing, China, 2017, p. 264-268.

[4]. Roseti C, Luglio M, Provenzano S, et al. A Cross-Layer Architecture for Satellite Network Security: CL-Ipsec. Advanced Satellite Mobile Systems. Bologna, Italy, 2008, p. 82-87.

[5]. Roy-Chowdhury, Ayan, J. S. Baras. Performance-Aware Security of Unicast Communication in Hybrid Satellite Networks. IEEE International Conference on Communications. Dresden, Germany, 2009, p. 1-6.

[6]. Benson, Theophilus, Aditya Akella, et al. Network traffic characteristics of data centers in the wild. ACM Internet Measurement Conference. Melbourne, Australia, 2010, p. 267-280.