future internet

MDPI

Article

Research on SWIM Services Dynamic Migration Method †

Zhijun Wu *, Shengyan Zhou, Liang Liu and Jin Lei

School of Electronics Information & Automation, Civil Aviation University of China, Tianjin 300300, China

* Correspondence: zjwu@cauc.edu.cn; Tel.: +86-022-24092827

† Part of this article has been published in the 4th IEEE International Conference on Big Data Intelligence and Computing (DataCom 2018), Athens, Greece, 12–15 August 2018.

Received: 3 June 2019; Accepted: 15 August 2019; Published: 27 August 2019

Abstract: Air traffic management (ATM) plays an important role in maintaining and promoting air traffic safety, maintaining air traffic order and ensuring smooth air traffic. As the core of air traffic management, it is essential to ensure the safe and stable operation of system-wide information management (SWIM). Facing the complex and ever-changing network environment, a SWIM services dynamic migration method is proposed in this paper. This method combines SWIM core services to select destination nodes and migrate services. The experiment proves that the method can hide the service node while ensuring service continuity and increase the difficulty of malicious detection. By comparing with others, this method is more suitable for SWIM in terms of invulnerability. The throughput and delay performance of the method can meet the needs of SWIM.

Keywords: system-wide information management (SWIM); service migration; invulnerability; quality of service (QoS); pseudo-random sequence

1. Introduction

With the continuous development of civil aviation industry, more and more aircraft enter the airspace, which brings great pressure to air traffic management (ATM), and brings new challenges to civil aviation data transmission and exchange. In order to guarantee the reliable and safe transmission of massive civil aviation data, EUROCONTROL first proposed the concept of system-wide information management (SWIM) to the Federal Aviation Administration (FAA) in 1997. In 2005, the International Civil Aviation Organization (ICAO) adopted SWIM as an international aviation information distribution system. In 2007, the United States and Europe deployed the next generation air transportation system (Next Gen) and Single European Sky ATM Research (SESAR) respectively, and both use SWIM as a framework for information communication and data sharing [1]. As the core of next-generation air traffic management, SWIM is a key component of civil aviation network information interaction and data sharing [2]. It connects all the components of the civil aviation information network and integrates various business resources of civil aviation (including airspace management, traffic management, monitoring management and aircraft systems, etc.). SWIM manages aeronautical information data, weather data, surveillance data, and flight information data.

With the continuous development of Internet technology, the variety of network attacks is endless, and the attack technology is constantly improving, and it is difficult to completely prevent network intrusion. Once the civil aviation information network is attacked or fails, it will cause huge security risks to the civil aviation. To this end, a series of security technologies (firewalls, anti-virus software, intrusion detection systems) have been introduced, which can improve system security to a certain extent, but the system cannot completely prevent malicious attacks, virus intrusions, and failures. For example, on 13 December 2014, a computer system failure caused a computer failure to shut down

the airspace, resulting in a large delay at the London Heathrow airport. On 21 June 2015, Polish Airlines ground operating system was hacked, causing the system to crash for five hours. Therefore, it is essential to ensure the safe operation of the civil aviation system.

As more and more users obtain civil aviation service data through SWIM network, SWIM service data interaction becomes more frequent and the security threats are becoming more prominent. At present, there are few studies on SWIM network security. The SESAR 14.2.2 and 16.2.1 projects are designed to define a security solution for the SWIM technology infrastructure and provide technical advice for the resolution of security threats. This paper conducts research from the perspective of active defense based on the project security suggestion. From the perspective of SWIM's overall architecture, Wu Zhijun analyzed the security technical standards of SWIM security services and infrastructure, and provided general technical standards support for the deployment and implementation of SWIM [3]. To ensure the security and reliability of SWIM services and to meet the heterogeneous needs of local, national, regional and global environments, Lu Xiaodong designed a multi-layered SWIM system architecture [4]. Qi Ming et al. constructed a SWIM security threat scenario based on the actual application scenarios, the security risk identification and risk analysis methods were used to establish the risk calculation formula, and finally the security threat and risk analysis plan was obtained, but there was no comprehensive risk. The evaluation value is used as a further emergency response strategy [5]. Mohammad Moallemi et al. studied the information security vulnerabilities and performance hazards of the main components of AAtS (Aircraft Access to SWIM) by identifying the information security vulnerabilities of NAS enterprise messaging services, and designed several test scenarios [6]. Wilson proposed a technical solution to improve the security of the SWIM, which can enhance information sharing operability and data security [7]. In the process of a civil aviation department as a SWIM service provider, SWIM service consumers and SWIM service providers use SWIM core services to achieve data transmission and information sharing. Although a series of security measures have been deployed in the SWIM core services, there is still no way to ensure that the system is completely protected against security threats.

Suppose a malicious attacker successfully bypasses the SWIM firewall and multiple security measures to enter the SWIM disguised as a legitimate user. The malicious attacker first obtains the SWIM advanced access right by using the security service in the SWIM core service, and then obtains the description information of the SWIM service provider through the registration center in the SWIM interface management service.

According to the description information of the SWIM service provider, a malicious attacker can launch a malicious attack after long-term detection of the SWIM service provider, which may cause the SWIM service provider to interrupt the service or even crash the system, or the malicious attacker successfully obtains the control of the SWIM service provider to provide untrustworthy service data to the outside world, thus affecting the analysis and decision-making of SWIM service consumers, and even affecting the safe and stable operation of the civil aviation industry. SWIM service providers will also face security threats such as natural disasters and system failures, which seriously affect the security and reliability of SWIM services. Therefore, in order to improve the fault tolerance capability of the system, this paper transforms the traditional passive defense into active defense from the perspective of protecting the SWIM service data source, and proposes a dynamic migration method of SWIM service to enhance the survivability of the system.

The main contributions of this paper as follows:

(1) According to the characteristics of the pseudo-random sequence, a new service migration trigger mechanism is designed, so that the SWIM service migration frequency can be regulated by the SWIM region.

(2) On this basis, according to the different service migration trigger mechanism, A destination node selection strategy based on SWIM core service and randomness is proposed in this paper, which guarantees seamless migration of SWIM services.

The remaining chapters of this paper are organized as follows: Section 2 firstly introduces the related concepts of SWIM and the current state of research on service migration. Section 3 introduces the SWIM security threats scenario. Section 4 designs a SWIM services dynamic migration method. Section 5 analyzes the validity of the method from both theory and simulation. Section 6 discusses and summarizes the full text.

2. Related Work

The SWIM shares service data through a global interoperability network architecture, which looks like a virtual service pool that combines multiple civil aviation services. It adopts loosely coupled architecture and unified standards to facilitate the transmission and sharing of heterogeneous data. The global interoperability network architecture is shown in Figure 1 [8,9].

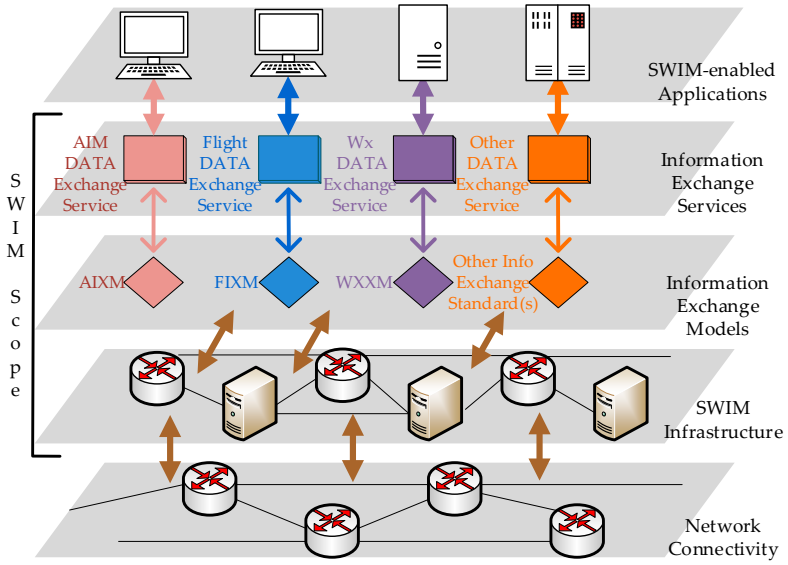

Figure 1. The global interoperability network architecture.

SWIM service providers (SP) and SWIM service consumers (SC) provide or consume SWIM services through SWIM-Enabled Applications, and they use a unified exchange models for data sharing, such as Aeronautical Information Exchange Model (AIXM), ATM Information Reference Model (AIRM), Weather Information Exchange Model (WXXM) and Flight Information Exchange Model (FIXM). SWIM Infrastructure provides the infrastructure for sharing information. It provides the core services such as interface management, request-reply and publish-subscribe messaging, service security, and enterprise service management [10].

SWIM is a distributed large-scale network. The SWIM service registration information list is distributed and has global consistency. In the SWIM service registration information list, there are multiple SPs with the same service topic, and the key service data is distributed in different places. The SWIM service information interaction process is shown in Figure 2.

Publish-subscribe is the main way of SWIM information interaction. First, SWIM service providers publish SWIM services in three steps through A–B–C, and register content in the registration information database including service topics, WSDL and other information. Then SWIM service consumers search SWIM service in three steps through 1–2–3, SWIM sends SC subscription information to SP, Finally SP push service information to subscribers. This multi-source architecture provides innate conditions for survivability enhancement and disaster recovery backup. Our main research focus is on the SWIM infrastructure layer, which uses SWIM core services to seamlessly migrate service permissions to enhance network survivability.

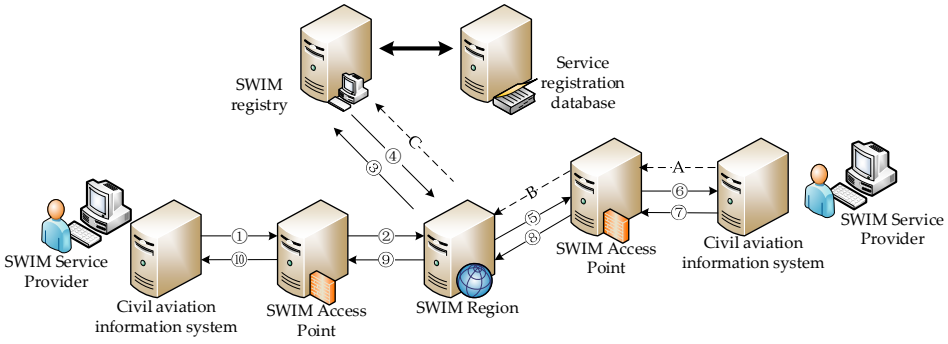

Figure 2. The system-wide information management (SWIM) service information interaction process.

At present, the research on the service migration mechanism has achieved a lot of results. Huang [11] uses a variety of random competition mechanism to implement process migration in a service cluster. Server drift is highly random, but an attacker may initiate a time interval attack. The migration mechanism lacks controllability and may cause network oscillations. Hong Xiaoliang et al. [12] improves the triggering mechanism and competition mechanism of service migration in [11]. It can effectively resist time interval attacks, but the single service migration mode reduces the randomness of service migration. Zhao Erhu et al. [13] proposes a service migration model abstracting the service model into a partially observable Markov decision process, and it can maximize customer benefits by computing service drift strategies. But the model trigger mechanism is unreasonable and can easily cause time conflicts. In [14], an active service migration model based on network survivability situational awareness is proposed by using the alarm information of various detection platforms. This model cannot jointly analyze alarm data, which is prone to false alarm drift and increase system workload. Mao Yingchi et al. [15] proposes an optimal Web service migration architecture in a cloud computing environment. The architecture uses the load as the migration service triggering metric, and the triggering conditions are single, the security of the service cannot be guaranteed.

3. SWIM Security Threat Scenario

In the SWIM network, the civil aviation meteorological department provides the aeronautical meteorological information service as a SWIM service provider (SP). The SWIM network security scenario is shown in Figure 3.

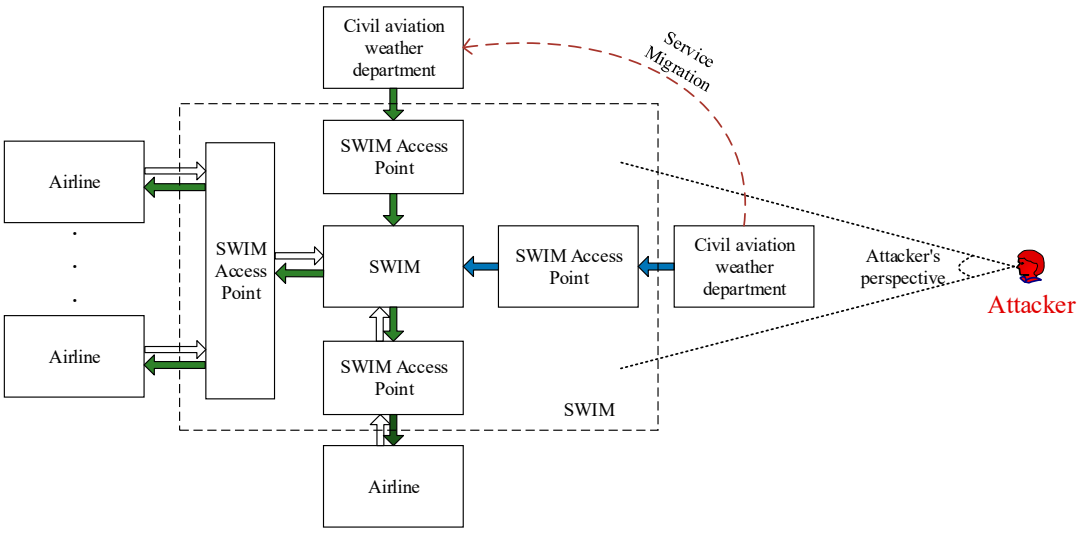

Figure 3. SWIM security threat scenario.

In the process of obtaining aviation weather information service through the SWIM network, it is assumed that a civil aviation meteorological department of China provides aviation weather information service to the airline. Due to the fixed nature of the traditional SWIM network topology, the network security threat has the characteristics of penetration and latency. The malicious attacker can capture the system vulnerabilities of the civil aviation meteorological department through long-term detection, and then launch a malicious attack to cause the aviation meteorological service to be interrupted. Therefore, how to transfer the SWIM service provider out of the scope of the attacker's attack perspective, making the attack launched by the attacker invalid or increasing the attack cost and widening the attack perspective is an important issue.

4. SWIM Service Dynamic Migration Method

The malicious attacker's malicious attack behavior can be divided into two stages. The first stage is the infiltration stage, which mainly performs the detection behavior such as vulnerability scanning, finds exploitable vulnerabilities of SWIM service providers, and formulates relevant attack strategies. The second phase is the attack phase. According to the previous detection results, the SWIM service provider launches a malicious attack, obtains the control of the SWIM service provider, or makes some destructive behaviors such as stealing and destroying. The attack process of a malicious attacker is shown in Figure 4.

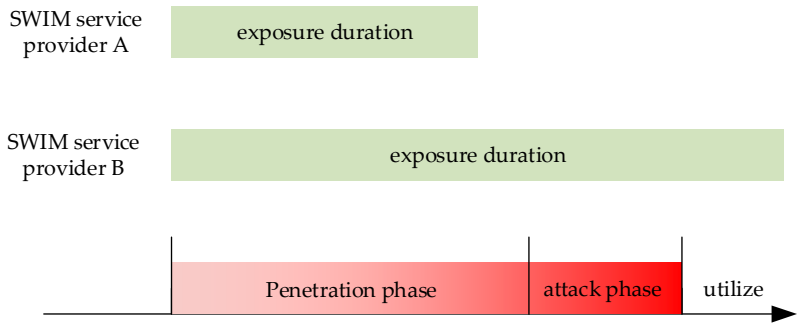

Figure 4. The attack process of a malicious attacker.

The exposure time refers to the difference between the time stamp provided by the SWIM service provider and the time when the service is stopped. If the SWIM service provider is exposed to the network for a long time, it will increase the probability of successful detection by the malicious attacker. As shown in Figure 4, the system exposure time of the SWIM service provider A is shorter than the penetration time of the malicious attacker, and the attacker's early penetration has not been completed, and the complete attack cannot be launched. If SWIM service provider A self-repairs during the offline phase and changes its characteristics, the early infiltration work of the malicious attacker will be invalid. The SWIM service provider B's system exposure time is sufficient for a malicious attacker to launch a complete attack, which will seriously threaten the security of the SWIM service. Assume that the time required for the infiltration phase is PSt, the time required for the attack phase is APt, and the exposure time of the SWIM service provider is E_t. In order to ensure the safe and reliable operation of the SWIM service provider, it is necessary to ensure that the SWIM service provider exposure time meets the Formula (1).

$$E_t < PS_t + AP_t. \tag{1}$$

There are two ways to ensure that the SWIM service provider meets the requirements of Equation (1). The first is to prolong the detection time of malicious attackers, mainly by fixing vulnerabilities, detecting attacks, building firewalls, etc. The second way is to shorten the exposure time of SWIM service providers.

SWIM is a distributed large-scale information network, and the distributed SWIM domain manages the SWIM service registration information of the whole network. In the SWIM network,

multiple heterogeneous SWIM service providers can provide SWIM services of the same service topic externally. The diversity of SWIM service providers creates innate conditions for the migration of SWIM services. From the perspective of increasing the survivability of SWIM services, this paper randomly selects different SPs to provide services to SWIMs based on the idea that "mobile targets are more secure", so that SWIM service data sources achieve random dynamic migration between different databases. By continuously and dynamically migrating to hide the service node, the exposure time of the SWIM service provider is shortened, the attack success rate is reduced, and the attack cost of the malicious attacker is increased. Then, how to guarantee the time randomness and spatial randomness of the mechanism are two key issues.

Time randomness refers to the randomness of the trigger time of the SWIM service dynamic migration mechanism. If the trigger mechanism uses a fixed-cycle trigger, the trigger period will be detected by the attacker, which will increase the probability of successful attack by the malicious attacker. In the process of providing services to SWIM, only the service migration mechanism is guaranteed to be trigged randomly, so that the service time window of each SP is different to achieve the purpose of confusing the attacker.

Spatial randomness refers to the randomness of the SWIM service dynamic migration method to select the destination node. If the migration destination node is selected according to a fixed law, the migration law will lose the meaning of the protection system once it is mastered by the attacker. Therefore, only ensuring the randomness of the destination node selection can increase the difficulty of detecting the service data source by malicious attackers and improve the survivability of the SWIM service.

Combined with the above analysis, this paper proposes a SWIM service dynamic migration method (SSM), as shown in Figure 5.

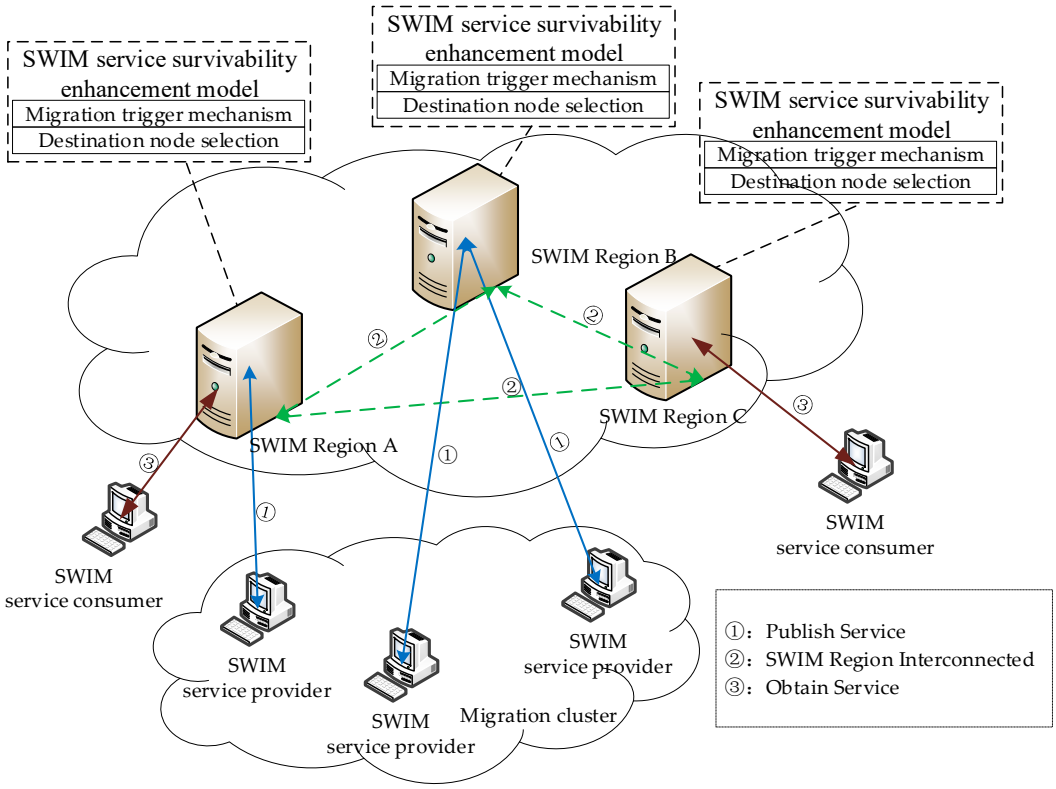

Figure 5. The SWIM service dynamic migration method.

The SWIM service dynamic migration method is deployed in the SWIM core service and consists of a migration trigger mechanism and a destination node selection mechanism. Considering the need of time randomness and spatial randomness, this chapter designs a trigger mechanism combining time interval and random sequence, and adopts the combination of Brownian motion method and optimal service quality to select the migration target SP, which fully weighs service concealment and security requirements. In the process of providing services to the SWIM, the SWIM registration center is used to obtain the service information of the entire network node, and the status information of each node of the entire network is obtained by using the service monitoring and performance monitoring/reporting log information, and is hidden by continuously and randomly transferring the service authority. Service nodes reduce the success rate of attacks and increase the attack cost of malicious attackers.

4.1. Migration Trigger Mechanism

It can be known from the nature of the pseudo-random sequence that the pseudo-random sequence can guarantee the randomness of '0' or '1' [16]. On the one hand, it can be predetermined, and can be repeatedly produced and reproduced. On the one hand, it has some random properties of a random sequence. A trigger mechanism based on pseudo-random sequence is established in the SWIM network. First, a series of pseudo-random sequences are generated by the shift register, and the pseudo-random sequence output '1' triggers the migration mechanism. However, in order to prevent the output of consecutive '1' or '0' in the pseudo-random sequence, the service drifts too fast, causing the SWIM network to oscillate, or the service drift is too slow, providing the opportunity for the malicious attacker to maliciously detect the SWIM network and reduce the security of the SWIM service. Therefore, a triggering strategy combining random sequence and interval control is proposed. The SWIM service dynamic migration mechanism is trigged only when the pseudo-random sequence outputs '1' within the range specified by the time interval. According to the different types of SWIM services, combined with the knowledge of civil aviation experts, it is possible to adjust the frequency of the dynamic migration of SWIM services by expanding or narrowing the width of the time interval. The dynamic migration trigger mechanism of the SWIM service is shown in Figure 6.

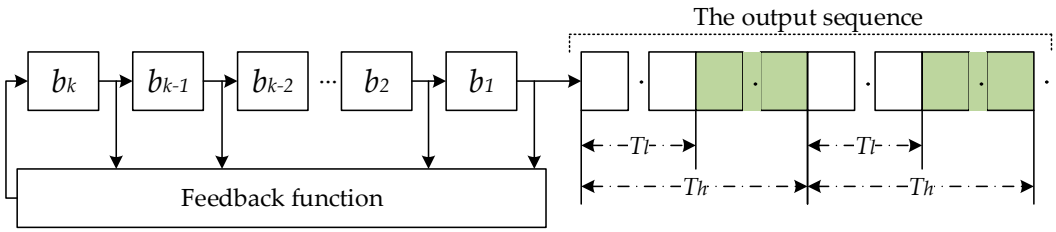

Figure 6. The migration trigger mechanism.

The dynamic migration mechanism of the SWIM service consists of two parts: a shift registers and a time interval. The shift registers outputs a pseudo-random number bit by bit with a period of *T*. The flow of the SWIM service dynamic migration trigger mechanism is shown in Figure 7. Among them, *Tl* provides the shortest service time for SP, and *Th* provides the longest service time for SP, where *Tl* and *Th* cannot be integer multiples of *T*, that is, the time interval is [*Tl*, *Th*]. In the time interval, the service migration mechanism is initiated when the pseudo-random number of the pseudo-random sequence output is '1'; or when the SP service time reaches *Th*, the service migration mechanism is trigged by the time interval.

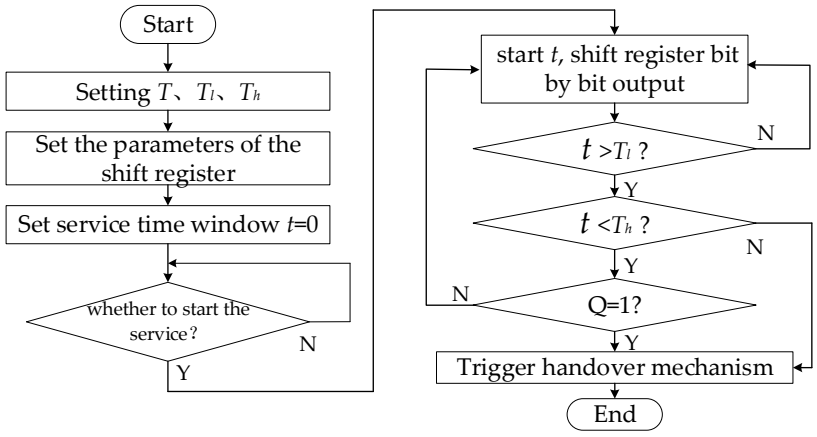

Figure 7. SWIM service dynamic migration trigger mechanism process.

4.2. Destination Node Selection Mechanism

In order to guarantee the random selection of migration destination nodes and consider the needs of SWIM network security, the destination node selection algorithm adopts the strategy of combining optimal quality of service (QoS) index with the Brownian movement model. When the model is trigged by a pseudo-random sequence, the Brownian movement model is used to randomly select SP from migration cluster to provide SWIM services; when trigged by the time interval timeout, the SP is selected by the optimal QoS value to provide SWIM services. The SWIM core service can monitor the services provided by the SWIM service provider [8]. This paper uses the service quality value as the indicator for selecting the target node. The QoS evaluation index system is shown in Table 1.

Table 1. The quality of service (QoS) evaluation index system.

Goal	Indicators	Description
QoS	capacity	limit the maximum number of the SC
	time behaviour	the response and processing times and throughput rates
	availability	reliability requirements under normal operation
	fault tolerance	the ability to continue to complete a service despite a hardware or software failure
	authenticity	the identity of a subject or resource can be proved to be the one claimed
	confidentiality	ensure that data are accessible only to those authorized to have access
	integrity	prevent unauthorized access to, or modification of data
	non-repudiation	the events or actions cannot be repudiated later

Capacity refers to the extent to which the SWIM service provider service is as described to the maximum extent of its description. As shown in Equation (2).

$$C_a = 1 - \left(\frac{C_{ar}}{C_{as}}\right). \tag{2}$$

Among them, C_{ar} is the number of times the SWIM subscribes to the SP in the actual running process, and C_{as} is the description of the service capacity when the SP service is registered.

Time behaviour refers to the extent to which the response, processing time, and throughput of the SWIM service in performing its services meet the requirements described in its description. As shown in Equation (3).

$$TB = 1 - 0.5 \times \left(\left(\frac{PT_r}{PT_s}\right) + \left(\frac{TP_r}{TP_s}\right)\right). \tag{3}$$

Among them, PT_r represents the actual service response and processing time, PT_s represents the description of response and processing time when the service is registered, TP_r and TP_s represent actual throughput and describe throughput, respectively.

Availability Av refers to the degree to which the service is required for reliability under normal operation. As shown in Equation (4).

$$A_v = \frac{MTBF}{MTTR + MTBF}. \tag{4}$$

Among them, $MTBF$ is the average time between failures, and $MTTR$ is the average recovery time.

Fault-tolerant refers to the degree to which redundancy backup infrastructure guarantees tolerance even if there is a hardware or software failure and the service is still operating as expected. As shown in Equation (5).

$$FT = \begin{cases} 1 & If\ there\ is\ a\ backup \\ 0 & If\ there\ is\ no\ backup \end{cases}. \tag{5}$$

Authenticity refers to the extent to which the identity of a topic or resource can be proven to be its claimed identity. As shown in Equation (6).

$$A_u = \begin{cases} 1 & requires\ a\ certification\ for\ authentication \\ 0 & doesn't\ require\ a\ certification\ for\ authentication \end{cases}. \tag{6}$$

Confidentiality refers to the extent to which information access requires user authentication and communication encryption to ensure that data can only be accessed by authorized accesses. As shown in Equation (7).

$$C_{on} = \begin{cases} 1 & requires\ user\ authentication\ and\ communication\ encryption \\ 0 & doesn't\ requires\ user\ authentication\ and\ communication\ encryption \end{cases}. \tag{7}$$

Integrity refers to the ability of a service to prevent unauthorized access or modification of data. As shown in Equation (8).

$$I_{nt} = \begin{cases} 1 & requires\ access\ control \\ 0 & doesn't\ requires\ access\ control \end{cases}. \tag{8}$$

Non-repudiation refers to the extent to which an operation or event has occurred, so that it cannot be denied in the future. As shown in Equation (9).

$$NonR = \begin{cases} 1 & with\ digital\ sign \\ 0 & without\ digital\ sign \end{cases} \tag{9}$$

The QoS index of each SWIM service provider consists of an octet, which represents the quality of service of the SWIM service k provided by the service provider i in the SWIM network, as shown in Equation (10).

$$QoS_{ik} = \left[\begin{array}{cccccccc} Ca_{ik} & TB_{ik} & Av_{ik} & FT_{ik} & Au_{ik} & Con_{ik} & Int_{ik} & NonR_{ik} \end{array} \right] \tag{10}$$

The SWIM domain periodically updates and records the QoS index of each SWIM service provider. When the dynamic migration mechanism is trigged by the time interval, the service node SP needs to hand over the service authority to the optimal quality of service node, and the destination node selection module acquires the QoS index of the candidate destination node in the migration cluster, and calculates the SWIM service provision according to Equation (11). The total QoS index of the service k provided by i.

$$Qos_{ik}^{total} = \sum_{j=1}^{n} w_{ik}^{j} \times Qos_{ik}^{j} \tag{11}$$

$$w_{ik}^{j} = \frac{\sum\limits_{i \neq j} t_{trigger} - t_i^j}{(n-1)\sum\limits_{i=1}^{n} t_{trigger} - t_i^j} \tag{12}$$

where QoS_{ik}^{total} represents the total QoS index of the service k provided by the SWIM service provider i, w_{ik}^{j} represents the degree of influence of the j-th QoS record of the SWIM service provider i on the service k, and $t_{trigger}$ represents the service dynamic migration mechanism trigger timestamp, t_i^j represents the timestamp of the j-th QoS record of the SWIM service provider i.

The total QoS index of all candidate nodes in the migration cluster can be obtained by Equation (11), and the candidate node QoS index matrix is constructed.

$$QoS_k\prime = \begin{bmatrix} Ca_{1k} & TB_{1k} & Av_{1k} & FT_{1k} & Au_{1k} & Con_{1k} & Int_{1k} & NonR_{1k} \\ Ca_{2k} & TB_{2k} & Av_{2k} & FT_{2k} & Au_{2k} & Con_{2k} & Int_{2k} & NonR_{2k} \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ Ca_{nk} & TB_{nk} & Av_{nk} & FT_{nk} & Au_{nk} & Con_{nk} & Int_{nk} & NonR_{nk} \end{bmatrix}. \tag{13}$$

The sensitivity of the service to be transferred service k to the indicators of the QoS index is shown in Equation (14).

$$\mu = \begin{bmatrix} \mu_1 & \mu_2 & \mu_3 & \mu_4 & \mu_5 & \mu_6 & \mu_7 & \mu_8 \end{bmatrix} \tag{14}$$

According to Equation (15), the QoS index of each SP of the SWIM service topic k is calculated and ranked, and the optimal QoS node is selected as the service migration destination node.

$$QoS_k'' = QoS_k' \times \mu \tag{15}$$

4.3. Implementation of Migration Mechanism

In the process of SWIM providing services to the SC, the implementation process of the SWIM service dynamic migration method is shown in Algorithm 1. The SWIM service dynamic migration method obtains the number of SWIM service providers providing the service topic in the SWIM network, and the quality of service according to the service subject of the SC subscription. Determine the range of the time interval, the parameters of the shift register, and the output period of the pseudo-random sequence. The timer is started in the SWIM network, and the pseudo-random sequence is output bit by bit. According to the output sequence of the shift register and the timing value, it is determined whether the dynamic migration mechanism of the SWIM service is trigged. According to different triggering reasons, the service migration target node is selected by using different strategies, and the SWIM service dynamic migration module sends the service request to the migration destination. The node, or the transfer destination node transfers data to the service message queue.

Algorithm 1. The implementation process of the system-wide information management (SWIM) service dynamic migration method.

Input: T, T_l, T_h, T, Q
Output:
Begin
If $t > T_h$
  Time interval trigger migration mechanism;
  $t = 0$;
 Else if $T_l < t < T_h \& Q(t) = 1$
  The migration mechanism is trigged by a pseudo-random sequence;
  $t = 0$;
 End if
End if
If Trigger by time interval
  Obtains QoS records of network-wide service nodes;
  Select the optimal QoS node;
 Else if Trigger trigged by pseudo-random
  Randomly selecting migration nodes;
 End if
End if
Sends service status information to the destination node;
The message queue establishes a connection with the migration destination node;
End

5. Experimental Results and Analysis

SWIM is a large-scale network system and used in civil aviation systems. It utilizes existing civil aviation equipment resources, as a heterogeneous data resource integration system, unifies services data formats, and as a virtual information pool to provide services to civil aviation organizations. In order to verify the performance of the SWIM service dynamic migration method, a SWIM simulation test platform was built. The topology is shown in Figure 8.

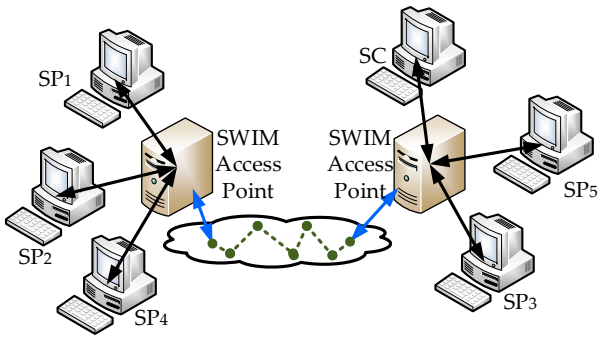

Figure 8. SWIM simulation test platform.

The SC acquires the SWIM services as a SWIM services consumer, SP_1, SP_2 and SP_3 composes an aeronautical information services migration cluster to provide aeronautical information service for SWIM system, SP_4 and SP_5 provides a flight information service. In simulation test, SC acquires a flight information services via SWIM access point. Among them, the flight information services data and aeronautical information services data were respectively provided by an airline and an air traffic control technology center in China, the SWIM flight information exchange model (FIXM) [17] and the SWIM aeronautical information exchange model (AIXM) [18] is a standard that provides flight information services and aeronautical information services to SCs. The experimental PC hardware configuration is shown in Table 2.

Table 2. The experimental PC hardware configuration.

Name	Operation System	CPU	Memory
SC	Ubuntu 14.04	i5-4590 3.30 GHz	4GB
SWIM Access Point	Ubuntu 14.04	i5-4590 3.30 GHz	2GB
SP	Ubuntu 14.04	i5-4590 3.30 GHz	4GB

The simulation experiment mainly analyzed the feasibility and effectiveness of the SWIM service dynamic migration method from three parts. The first part was based on the SWIM network topology structure constructed in Figure 8 to simulate the SWIM services interaction process and analyze the feasibility of the SWIM service dynamic migration method according to the statistical data of the SWIM. The second part is a mathematical model for establishing the SWIM key services dynamic migration method, it was compared with the SASS and TOKEN models to verify the validity of the SSM model. The third part was to evaluate the method from the two parts of throughput and service average delay.

5.1. Services Continuity Analysis

The SWIM service consumer sends a SOAP request to obtain the aeronautical information service. After receiving the request, the service agent in the SWIM uses the SWIM interface to manage the service registration request service registration information, and then selects an SP to provide the service data to the service agent, and starts the SSM method. When the SSM triggers the migration mechanism, the SSM selects the migration destination node according to the triggering reason, and the SWIM sends the service state information to the migration destination node, and the migration destination node establishes a connection with the service proxy, and transmits data to the message queue in the service proxy. The continuity of the SWIM service on the SWIM service consumer perception level is achieved. The interaction process is shown in Figure 9.

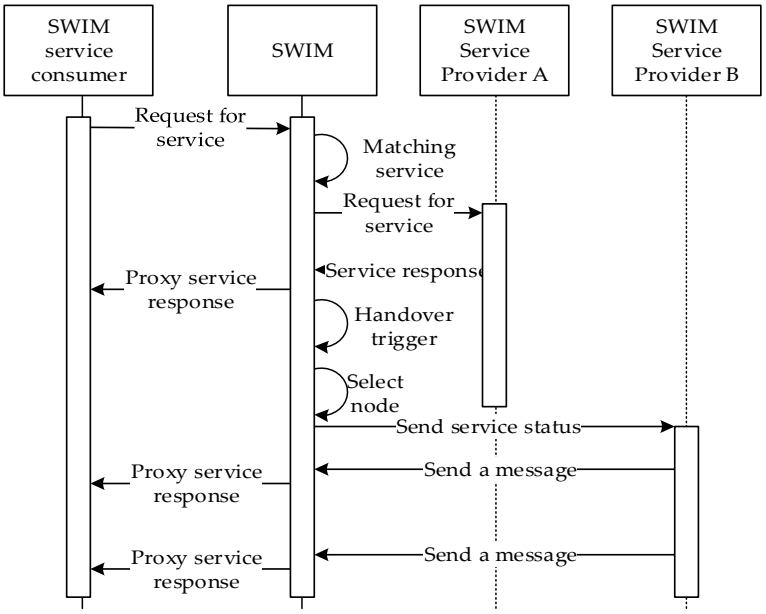

Figure 9. SSM method interaction process.

First, the parameters in the method are initialized and the time interval is set to Tl = 150 s, Th = 250 s, the update interval for each bit of the pseudo random sequence is 60 s. The pseudo-random sequence output from the shift register is {000001101001010110011110100110101110011011011100}. According to the statistics of the SWIM management center, the migration time and migration nodes are shown in Figure 10.

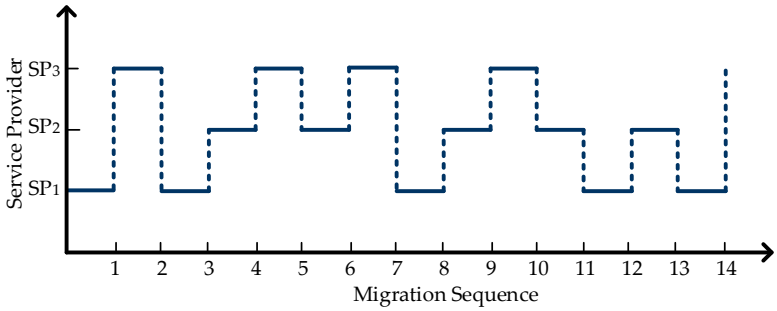

Figure 10. The sequence in time of migration node.

There are a total of 14 drifts and the total services time is 50 * 60 = 3000 s. During this period, a total of 15 SPs provide services to SWIM respectively. The average exposure time of each server is 200 s, the SWIM service dynamic migration method can be the balance of services continuity, reduces the services time window of the SP. Therefore, it is feasible to use this model to achieve hidden goals and continuous services.

5.2. Services Invulnerability Analysis

The invulnerability is proposed in [13] to describe the system's ability to resist destructive attacks. It means that in the system, the number of servers in migration clusters is n, the probability that the server will migrate to the i-th server is P_i. Drawing on the concept of information entropy, the invulnerability is expressed as:

$$R_d = -\sum_{i=1}^{n} P_i \log(P_i), n \geq 2 \tag{16}$$

The higher the services invulnerability is, the higher the randomness of services migration is, and the more difficult for malicious attackers to detect system vulnerabilities is, the more secure the system is.

First, the time interval length is L: refers to the number of bits of the pseudo-random sequence contained in the time interval $[Tl, Th]$. From the definition of services invulnerability, only when the output of pseudo-random sequence is '1' within the time interval will it trigger, and in the time interval, the probability that each bit of the pseudo-random sequence outputs '0' or '1' is equal, then only when all of the output sequence in the time interval is '0', the migration mechanism will not be trigged by the pseudo-random sequence. Therefore, the services invulnerability of the proposed model is defined as follows:

$$R_d = -\left[(\frac{1}{2}^L) \times \log(\frac{1}{2}^L) + (n-1)(1-\frac{1}{2}^L) \frac{1}{(n-1)} \times \log((1-\frac{1}{2}^L) \frac{1}{(n-1)}) \right]. \tag{17}$$

In the SASS model [11], services migration is trigged by a pseudo-random sequence. The probability of '0' or '1' in the pseudo-random sequence is equal. due to the SASS model target node selection strategy is the Brownian movement model. Then, the probability that each service be selected is equal. From the definition of the invulnerability, the SASS model's services invulnerability is as follows:

$$R_d = -\left[\frac{1}{2} \log(\frac{1}{2}) + (n-1) \frac{1}{2(n-1)} \log(\frac{1}{2(n-1)}) \right]. \tag{18}$$

The TOKEN model is trigged according to the time slice and random sequence [12]. The probability of triggering is as same as the SASS model. However, the TOKEN model selects the destination node based on the minimum load. Assume that in the migration cluster, the number of minimum load

servers is n_0, and $1 \leq n_0 \leq n-1$. The probability that minimum load servers is selected is the same, so the TOKEN model's services invulnerability is as follows:

$$R_d = -\left[\frac{1}{2}\log(\frac{1}{2}) + n_0 \times \frac{1}{2n_0}\log(\frac{1}{2n_0})\right], 1 \leq n_0 \leq n-1. \quad (19)$$

The SWIM service dynamic migration method is compared the services invulnerability with the SASS model and TOKEN model. The comparison results are shown in Figure 11. First, as the size of the migration cluster continues to expand, the number of the alternative servers are increases, so the probability of each server being selected become smaller, the randomness of this system are increases. Therefore, the invulnerability of the three models is increasing. When $L = 1$, the SWIM service dynamic migration method has the same degree of invulnerability as the SASS model and TOKEN model at $n_0 = n - 1$. This is because at that time, the SWIM service dynamic migration method triggers the migration mechanism is only determined by a bit pseudo-random sequence, and the probability of the output sequence outputs '0' or '1' is the same. At the same time, the Brownian movement model is used to randomly select the destination node. Therefore, when the SSM model is $L = 1$, the invulnerability is the same as the SASS model. In the TOKEN model, $n_0 = n - 1$ means that the load of the other nodes is the same, which is the optimal situation. We can randomly select the destination node; therefore, the three models have the same degree of invulnerability.

With the same size of the migration cluster, the randomness of the services migration is smaller with the decrease of the services cluster size. Therefore, the services invulnerability of the TOKEN model will continue to decrease, as shown in Figure 9, when $n_0 = n - 1$, $n_0 = n - 2$ and $n_0 = n - 3$, the TOKEN model services invulnerability as shown in the change curve; in the SWIM service dynamic migration model, as the size of the migration cluster increases, the SSM model's services invulnerability increases continuously and is significantly better than the SASS and TOKEN models. Although, when $n = 2$, the SWIM service dynamic migration model's services invulnerability is lower than the SSAS and TOKEN models at the time, SWIM is a large-scale distributed system. There are not only two SWIM services providers with the same services topic. the SWIM service dynamic migration model's invulnerability performance can meet the requirements of the SWIM network.

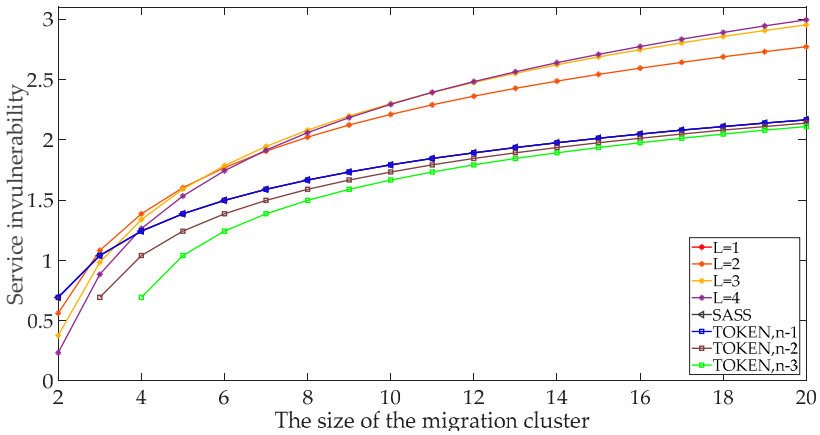

Figure 11. Comparison of services invulnerability.

In the SWIM service dynamic migration method, the size of the time interval is L, which will affect the services invulnerability. The relationship between the time interval length and the services invulnerability is shown in Figure 12. In the same L, the probability of the SWIM service dynamic migration method triggering is the same. The larger of the cluster size is, the greater the randomness of the servers being selected, and the higher the services invulnerability is; With the increase of L, the services invulnerability rate does not increase, but rises to a certain point and then drop, this point

is the optimal value for the size of the migration cluster. In this case, the migration cluster can achieve the maximum degree of invulnerability.

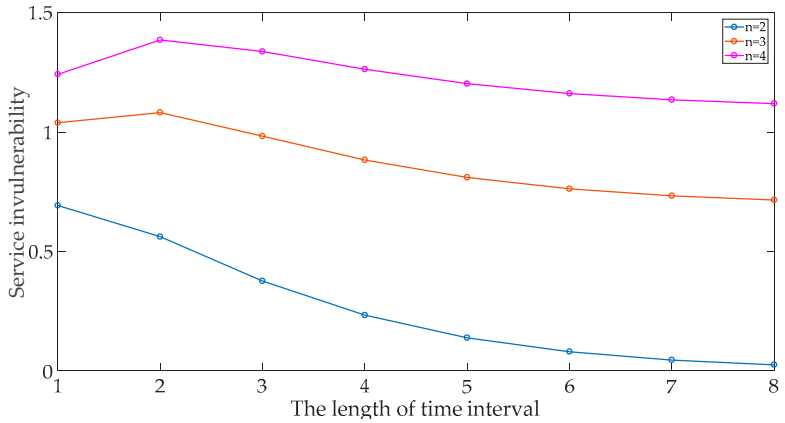

Figure 12. Performance analysis of the SWIM service dynamic migration method.

Through experimental analysis, the SWIM service dynamic migration method can adapt to the requirements of the SWIM large-scale network. At the same time, according to the size of the migration cluster, the value of the L change can maximize the system's invulnerability and ensure that the SWIM network is maintained reliable secure services capabilities in a complex network environment and enhance the survivability of SWIM.

Through experimental analysis, the SSM model can adapt to the requirements of SWIM large-scale network, and at the same time, according to the size of the migration cluster, by changing the value of L, the system service damage resistance is optimized. Compared with the SASS model and the TOKEN model, it is proved that the SSM model has certain advantages in service damage resistance. The following is a verification of whether the SSM method can meet the performance requirements of SWIM from both throughput and service delay.

5.3. Model Performance Analysis

Through the above analysis, the method has a high degree of invulnerability. According to the SWIM official manual, the validity of the model is verified from both throughput and delay [9].

The simulated SC subscribes to the aeronautical information service. The SWIM network throughput test results are shown in Figure 13. In the first 50 min, both networks maintain good throughput. At 50 min, the network is maliciously attacked and the SWIM network resources were occupied. As a result, the SWIM throughput is declining. Since the method can avoid attacks and tolerate disasters, the SWIM network throughput of deploying this method is significantly slower than that of SWIM networks without the method, and it has higher damage resistance.

In the process of SWIM providing services, the average service delay is an important indicator to describe the performance of SWIM services. We want to reduce the delay as much as possible, but by deploying migration security measures in SWIM, it will increase the work of the system. The network security attack and defense process are a trade-off process. We simulated 500 SCs to obtain aeronautical information services through SWIM, and statistics the average service delay. The average service delay of SWIM is shown in Figure 14. In a secure environment, both can guarantee a lower service delay. In an abnormal network environment, the original SWIM network fails to evade the attack. The SC obtains the connection timeout return information, and the average network service delay will increase. The SWIM network deploying the method can still maintain a good state.

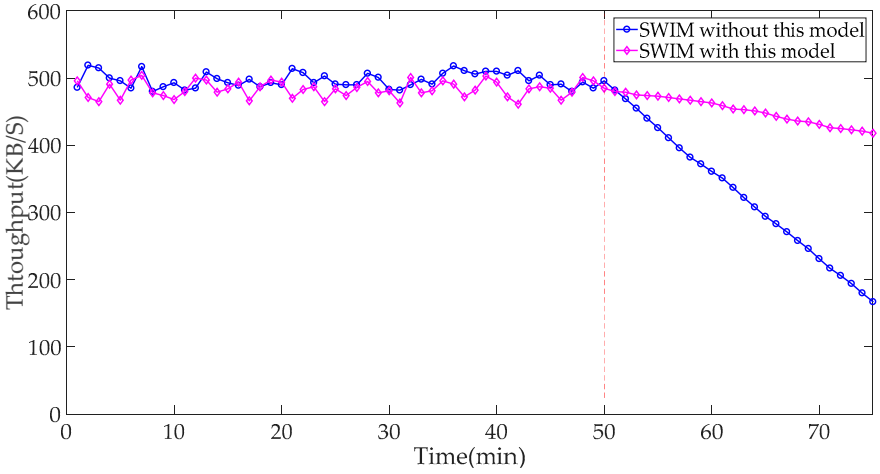

Figure 13. Throughput performance comparison.

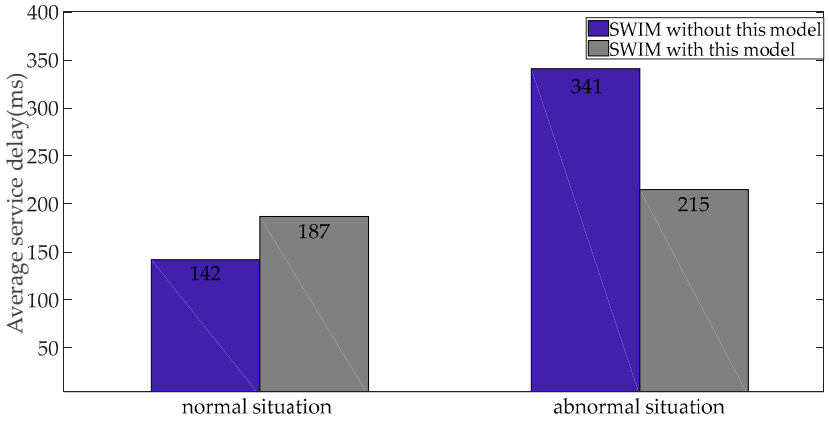

Figure 14. Average service delay comparison.

The SWIM network performance of the SSM model is compared with the SWIM network performance indicators of the SSM model. The performance comparison results are shown in Table 3. As can be seen from Table 3, under normal circumstances, SSM can guarantee the continuity of SWIM services, and its throughput and service delay can meet the performance requirements of SWIM; In an abnormal environment, the performance of SSM is significantly better than that of SWIM networks without SSM models deployed.

Table 3. Performance comparison between the two models.

Model	Average Throughput (bytes/s)		Average Service Delay (ms)	
	Normal Situation	Abnormal Situation	Normal Situation	Abnormal Situation
With SSM	483.4	343.1	127	155
Without SSM	497.1	241.1	112	207

Network security attack and defense itself is a game process that weighs the pros and cons. The SWIM service dynamic migration method is based on the security sacrifice of SWIM service performance in the security environment in exchange for the security and stability of SWIM service performance under abnormal network environment. Effectively improve the damage resistance of SWIM, increase the attack difficulty of malicious attackers, and improve the survivability of SWIM services.

6. Conclusions

Aiming at the complexity of network environment and the importance of SWIM service, this paper first analyzes the security threats faced by SWIM. From the perspective of survivability enhancement, this paper proposes a SWIM service dynamic migration method, which can conceal nodes and increase the difficulty of malicious attacks. In this mechanism, a trigger mechanism combining time interval and pseudo-random sequence is designed to ensure the continuity and controllability of service triggering. Then the destination node selection strategy is studied, and the SWIM core service is used to ensure the spatial randomness and security balance of the SWIM service. Compared with the SASS model and the TOKEN model, it is proved that the SWIM service dynamic migration method has strong invulnerability, and the mechanism can meet the performance requirements of SWIM. This study has certain significance for SWIM emergency response. In the face of large-scale network attacks, the SWIM service dynamic handover mechanism relies on the handover cluster behind it to share the attack pressure to ensure maximum network performance in the harsh network environment. This requires that each SWIM service provider itself be somewhat resistant to aggression. In view of the existing problems in this paper, in the future research, we can also analyze and study the security threat scenario of large scale damage of SWIM network, and design a SWIM service rapid recovery mechanism by using cloud services, cloud storage and other technologies to improve the emergency response capacity of the system. The future is an era of informatization and digitization. Big data, blockchain, artificial intelligence and other new generation information technologies are widely used in all walks of life, creating great economic and social value. In the future, the new generation of information technology can be used for in-depth analysis and processing of SWIM security threats to ensure safe and efficient operation.

Author Contributions: Z.W., S.Z., L.L. and J.L. conducted the research along with analysis and results.

Funding: This research was funded by the National Natural Science Foundation, grant number U1533107, and the Major Program of Natural Science Foundation of Tianjin, grant number 17JCZDJC30900.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Delosieres, L.; Nadjmtehrani, S. Batman Store and Forward: The Best of the Two Worlds. In Proceedings of the 2012 IEEE International Conference on Pervasive Computing and Communications Workshops, Lugano, Switzerland, 19–23 March 2012; pp. 721–727.
2. Dario, D.C.; Antonio, S.; Georg, T. SWIM: A next generation ATM Information Bus-The SWIM-SUIT pro-totype. In Proceedings of the 2010 14th IEEE International Enterprise Dis-tributed Object Computing Conference Workshops (EDOCW), Vitoria, Brazil, 25–29 October 2010; pp. 41–46.
3. Wu, Z.J.; Zhao, T.; Lei, J. Research on SWIM Security Technology Standards. *Netinfo Secur.* **2014**, *1*, 1–4.
4. Lu, X.D.; Koga, T. Real-Time Oriented System Wide Information Management for Service Assurance. In Proceedings of the 2015 IEEE Twelfth International Symposium on Autonomous Decentralized Systems, Taichung, Taiwan, 25–27 March 2015; pp. 175–180.
5. Qi, M.; Xing, W.Z. Scheme Design for Data Security Threats and Risk Analysis of Civil Aviation System Wide Information Management. In Proceedings of the 19th National Youth Communication Academic Conference, Shanghai, China, 15 October 2014; pp. 12–18.
6. Moallemi, M.; Carlos, A.C.P.; Massood, T.; Biruk, A. Information Security in the Aircraft Access to System Wide Information Management Infrastructure. In Proceedings of the 2016 Integrated Communications Navigation and Surveillance (ICNS), Herndon, VA, USA, 19–21 April 2016; pp. 1A3-1–1A3-7.
7. Wilaon, I.; Yang, S. Security for System Wide Information Management. In Proceedings of the 2017 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 18–20 April 2017; pp. 1–13.
8. SESAR. SWIM (GG AG) Architectural Definition—Final, Edition00.10.01. Available online: https://www.sesarju.eu/sites/default/files/solutions/06_ADD_P14.1.3-D30-SWIM_Architectural_Definition_Final.pdf (accessed on 18 October 2017).

9. SESAR Joint Undertaking. SWIM-TI Yellow Profile Technical Specification 2.1, Edition00.10.00. 2014. Available online: http://www.sesarju.eu/sites/default/files/solutions/07_TS_Solution_20_14.01.04.D44-004-SWIM-TI_Yellow_Profile_Technical_Specification.pdf (accessed on 7 April 2017).
10. International Civil Aviation Organization. *SWIM Concept—Draft Version 0.9, ICAO Air Traffic Management Requirements and Performance Panel (ATMRPP)*; International Civil Aviation Organization: Montreal, QC, Canada, 2013.
11. Huang, Z.G.; Lu, X.C.; Hu, H.P. The survivability technique and its implementation case study. *J. China Inst. Commun.* **2004**, *25*, 137–145.
12. Hong, X.L.; Guo, Y.X. Research on the Mechanism of Service Migration. *J. Inf. Eng. Univ.* **2008**, *9*, 131–134.
13. Zhao, E.H.; Yang, X.L.; Peng, Y.F.; Long, K.P. CPSM: Client-Side Proactive Service Migration Model for Enhancing IP Network Survivability. *ACTA Electron. Sin.* **2010**, *38*, 2134–2139.
14. Chen, T.P.; Meng, X.R.; Cui, W.Y.; Xu, Y. A Proactive Service Migration Model Based on Network Survivability Situation Awareness. *J. Air Force Eng. Univ. Nat. Sci. Ed.* **2015**, *16*, 64–68.
15. Mao, Y.C.; Xu, Z.Y.; Wang, L.B.; Wang, J.L. An Optimal Web Services Migration Framework in the Cloud Computing. In Proceedings of the 2015 8th International Conference on Intelligent Computation Technology and Automation (ICICTA), Nanchang, China, 14–15 June 2015; pp. 153–156.
16. Xiao, G.Z.; Liang, C.J.; Wang, Y.M. *Pseudo Random Sequence and Its Applications*; National Defense Industry Press: Beijing, China, 1985.
17. FIXM-Flight Information Exchange Model, FAA/Eurocontrol. Available online: http://www.fixm.aero/ (accessed on 5 June 2017).
18. AIXM-Aeronautical Information Exchange Model, FAA/Eurocontrol. March 2013. Available online: http://www.aixm.aero (accessed on 14 May 2017).