Hindawi
Wireless Communications and Mobile Computing
Volume 2021, Article ID 5539790, 16 pages
https://doi.org/10.1155/2021/5539790

Research Article

SMSEI-SDN: A Suppression Method of Security Incident Impact for the Inter-Domain Routing System Based on Software-Defined Networking

Huihu Zhu, Han Qiu, Junhu Zhu, and Di Chen

State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou 450001, China

Correspondence should be addressed to Han Qiu; qiuhan410@aliyun.com

Received 17 January 2021; Revised 12 April 2021; Accepted 30 April 2021; Published 18 May 2021

Academic Editor: Di Zhang

Security incidents such as natural disasters and power outages can cause inter-domain routing system regional failures, significantly impact the Internet's safety. Reducing the impact of security incidents is essential for maintaining the stability of the Internet. One of the major impacts of security incidents is that many UPDATE messages will generate, which may easily cause network oscillations. This paper presents the UPDATE messages analysis during the six security incidents and finds that many duplicates and invalid messages are the leading cause of network instability. To effectively process these UPDATE messages, this paper proposes an UPDATE message preprocessing algorithm by analyzing the UPDATE operating mechanism to remove duplicate and invalid messages. Aiming at the problem of slow route search in existing route update methods using software-defined networking (SDN), this paper designs a RIB hierarchical structure for multi-level retrieval and proposes SMSEI-SDN combination with current route update strategies. Experimental results show that when a security incident occurs, by removing duplicate and invalid messages, SMSEI-SDN can reduce the total number of messages by an average of 19% and a maximum of 34.9% within the 60 s of caching time. Besides, SMSEI-SDN can reduce the routing update time by more than 99.98% compared to existing methods. This work provides insights for network operators and researchers interested in security incident impact suppression in the inter-domain routing system.

1. Introduction

Security incidents such as natural disasters [1, 2] and power outages can cause inter-domain routing system regional failures, significantly impact the Internet's safety. In the inter-domain routing system, the failure information of nodes and edges will be propagated to the surrounding network through UPDATE messages, which will have a continuous impact on the surrounding networks. When the regional failures caused by the initial security incidents are significant, it may even cause a cascading failure [3]. Therefore, in order to reduce the impact of security incidents on the network and maintain the stability of the inter-domain routing system, it is necessary to study methods to suppress the propagation of security incidents' effects.

Border Gateway Protocol (BGP) is the de facto inter-domain routing standard on the Internet for the last three decades. The BGP protocol is sensitive to the topology. When the topology changes, it takes a long time for BGP to converge [4]. When the inter-domain routing system encounters a security incident, it will often cause node failure or link interruption and change the inter-domain routing system's network structure. Moreover, large-scale nodes and link failure will produce many invalid UPDATEs in a short period [5], which causing significant pressure on routing nodes. Once the routing node has exhausted its resources due to processing excessive UPDATE messages [6], it will cause a cascading failure. Also, the continuous propagation of invalid UPDATE messages will cause many invalid paths to be selected before finding a valid route, which will cause

constant network oscillations and making it difficult for the network to stabilize [7].

Therefore, to reduce the impact of security incidents on the inter-domain routing system, the key is to quickly and efficiently process the burst of UPDATE messages, reduce repeated routing updates, and make the inter-domain routing system quickly enter a stable state [8]. Because the existing BGP protocol has shortcomings, such as tight coupling between the control plane and the data plane and the lack of dynamic programmable routing strategies, it is difficult to solve the burst of UPDATE messages under the current framework correctly. Therefore, it is urgent to introduce new solutions to solve these problems and maintain the inter-domain routing system's regular operation. Software-defined networking (SDN) [9] provides the possibility to solve it. The SDN technology has the characteristics of separation of the control plane and the data plane and is dynamically programmable. Therefore, it can respond to different security incidents by formulating dynamic strategies according to the network's real-time status. Relevant research has proved that SDN has a good effect on routing convergence [10], but there is no practical solution for excessive UPDATE messages generated during security incidents. To deal with UPDATE message burst, we introduced SDN into the autonomous system's (AS) management. This paper first analyses the UPDATE message's composition characteristics when a security incident occurs. And then, we propose a targeted UPDATE message preprocessing algorithm based on the above characteristics. By designing the Routing Information Base (RIB) hierarchical structure for multi-level retrieval, the SDN-based inter-domain routing system security incident impact suppression method is realized.

We summarize our contributions as follows:

(1) We found that when a security incident occurs, a lot of invalid messages will be generated. By analyzing the mechanism of the UPDATE message, we found the method to identify invalid messages

(2) To process the burst of UPDATE messages, we proposed a preprocessing algorithm for UPDATE messages. The algorithm can reduce the number of messages that need to be processed in the routing update module

(3) To improve the routing update efficiency, we designed a multi-level search-oriented RIB hierarchical structure, which uses prefixes' composition characteristics to organize routing information into a 4-level index structure. Based on the hierarchical structure, we proposed SMSEI-SDN, which can effectively improve the UPDATE processing efficiency when a security incident occurs

The rest of this paper is organized as follows. In Section 2, we discuss the related works of this paper. In Section 3, we analyze the characteristics of UPDATE when a security incident occurred. In Sections 4 and 5, we present our solutions. Results of experimental evaluations are provided in Section 6. In Sections 7, we discuss open issues in security incidents impact. We conclude our paper in Section 8.

2. Related Works

In recent years, with the frequent occurrence of various security incidents [11], the security of inter-domain routing systems [12, 13] has received more attention. The existing research on the impact of security incidents mainly focuses on routing convergence.

2.1. Research on BGP Convergence. To cope with large-scale failures and improve the efficiency of BGP convergence, Sahoo et al. [14] studied the influence of different Minimum Route Advertisement Interval (MRAI) values on the convergence process under large-scale failure conditions. The study found that the optimal value of MRAI is related to the failure scale. For a network, the optimal value of MRAI is not unique, and simply changing the MRAI value cannot improve the convergence efficiency. The author also pointed out that batch processing of the same target node's network prefixes can improve convergence efficiency. However, this method needs to sort the received messages, which increases a higher overhead. To improve the convergence efficiency, the author also proposed a new method for removing the invalid routing [5], which is to count the nodes included in the UPDATE. When the node included WITHDRAW message, the node count is increased by 1, and when it is included in the ANNOUNCE message, the count is decreased by 1. When a security incident occurs, it is considered that the node with a higher count has failed; so when selecting a path, the related route is regarded as an invalid route. This method improves route selection efficiency but lacks accuracy and cannot deal with large-scale UPDATE message churn as security incidents occur.

To reduce the BGP convergence time, Alabdulkreem et al. [15] studied the influence of topology and optimization algorithms on the optimal value of MRAI, trying to improve the convergence efficiency of the network without adding additional conditions. The previous related studies have shown that the optimal MRAI value in large-scale failures is related to topology and the failure scale. Therefore, this method cannot be applied to large-scale failures. Besides, simply reducing the convergence time cannot fundamentally solve route flapping and resource consumption.

2.2. Research on Convergence Based on SDN. The previous analysis shows that changing the MRAI value affects the convergence process, which has limited effect in large-scale failures and cannot prevent the further propagation of failures. In recent years, researchers have also conducted many explorations on SDN technology for network convergence. Kotronis et al. [16] proposed a method based on centralized control outsourcing to deal with the problem of network failure message propagation. This method uses a controller to centrally control multiple AS nodes to achieve the goal of centralized management. When the controller receives new update information, it can enable the AS nodes under its control to update the routing information for the first time. Therefore,

centralized control can theoretically minimize the convergence time. However, establishing a trusted third party to process-related control information is difficult in the current commercialization situation. Besides, multi-node collaborative management requires higher processing performance. Therefore, there is a long distance to practical applications.

To improve the convergence efficiency of the inter-domain routing system, Chang et al. [10] proposed to combine IP network and SDN equipment to reduce the convergence time (in this paper, we call it IP-SDN). The author believes that the longer convergence time is that every time Forwarding Information Base (FIB) encounters a failure to update, it will consume a lot of time to traverse. To solve this problem, the author proposes to divide the FIB into two layers, including the original routing node and SDN switch. Two-level search can improve search efficiency but cannot reduce the frequency. The author mainly focuses on the routing update problem caused by neighboring nodes' direct failure and cannot solve UPDATE message processing caused by security incidents.

Alotaibi et al. [17] proposed a multi-state method for a long convergence time when studying multi-domain SDN networks, reducing the convergence delay between multi-domain SDN nodes. However, this method cannot solve the problem of invalid message processing between AS nodes in the case of large-scale failure.

2.3. SDN-Related Research. In the early days of SDN, researchers considered applying SDN technology to inter-domain routing systems. After more than ten years of development, SDN has achieved good results in AS management, interAS interaction, and IXP management. Rothenberg et al. [18] discussed the possibility of applying SDN technology to the inter-domain routing system, proposed a hybrid network model with a controller as the core, and designed the Route Flow Control Platform (RDCP). Based on the idea of outsourcing, Kotronis et al. [16, 19] developed a method for centralized management of inter-domain routing using SDN technology to solve the problem of slow convergence. Lin et al. [20] proposed an SDN-IP network pair to solve the communication problem between the AS node managed by SDN and the legacy BGP node. It maintains a ZebOS BGP daemon at each border switch to receive the BGP information sent by the border routers from other ASes. On this basis, the WE-bridge mechanism [21] is proposed to solve network abstraction and information distribution problems. Gupta et al. [22] presented a software-defined IXP (an "SDX") solution to manage IXPs using SDN, which implements the functions of IXPs through SDN technology. To achieve the goal of using SDN to manage IXPs in industrial-grade networks, the author improved SDX and proposed industrial-scale software-defined Internet exchange point (iSDX) [23] and verified its feasibility.

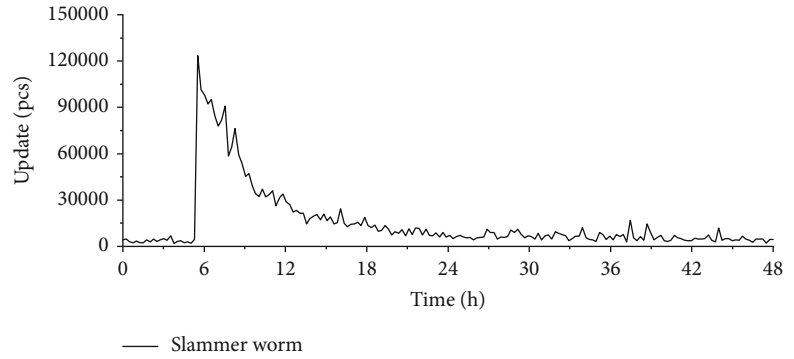
The use of SDN technology can realize the fine-grained network management of the AS. Chen et al. [24] proposed a multi-dimension link vector network view exchange mechanism (MLV) to realize fine-grained inter-domain routing management. Wang et al. [25] proposed an inter-domain routing network framework based on the SDN mechanism in response to the existing BGP architecture's rigid routing problem, which redesigned the inter-domain routing system protocol using SDN technology. Besides, Wang et al. [26] proposed an inter-domain routing control framework, named route chaining system (RCS). The platform supports flexible control of routing to ensure the regular operation of the network.

Previous studies have shown that the application of SDN technology to inter-domain routing systems has become increasingly mature. The dynamic programmable feature of SDN has prominent advantages for responding to unexpected security incidents. Therefore, this paper introduces SDN into the security field of inter-domain routing systems and uses SDN technology to achieve suppression methods against security incident effects.

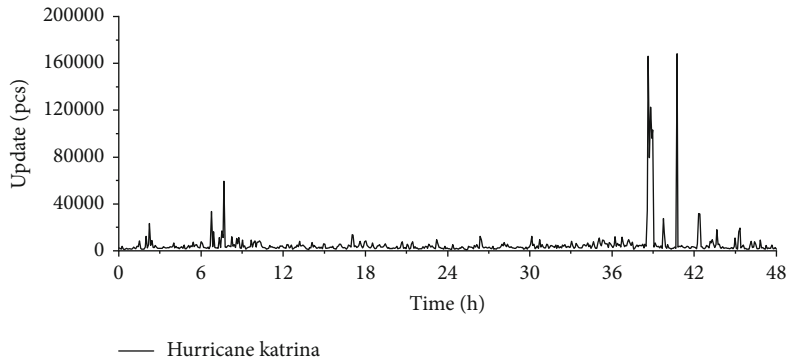
3. UPDATE Composition Characteristics under Security Incidents

To study methods to suppress the impact of security incidents and solve the problem that many UPDATE messages cannot be effectively processed when a security incident occurs, we conduct a systematic analysis of 6 typical security incidents of different types and periods. First, we use the data set of the rrc01 collection point in RIPE [27] to count the number of UPDATE messages within 48 hours before and after each security incident. The statistical results are shown in Figure 1. Figure 1 shows that the number of UPDATE messages increases sharply in all kinds of security incidents, much higher than those in the stable state. How to quickly and effectively deal with excessive UPDATE messages is the key to restraining the impact of security incidents.

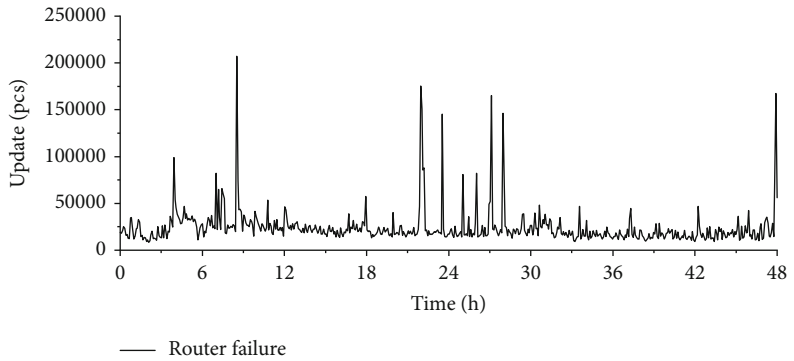
According to the BGP protocol, UPDATE messages can be divided into ANNOUNCE messages and WITHDRAW messages according to different functions. The primary function of ANNOUNCE message is to announce new routing information. When a new route is generated, it will be propagated through this type of message. The primary function of the WITHDRAW message is to withdraw the routing information. When a route is no longer valid, a WITHDRAW type update message is generated to withdraw the route. To find out the characteristics of a large number of UPDATE messages when a security incident occurs, we count the number of ANNOUNCE messages and WITHDRAW messages, respectively. The statistical results are shown in Figure 2. Figure 2 shows that the number of ANNOUNCE messages is much higher than the number of WITHDRAW messages when a security incident occurs. By analyzing the process of security incidents affecting the inter-domain routing system, we can find that the reason for the vast gap between the numbers of ANNOUNCE messages and WITHDRAW messages is that the two influence mechanisms are different. Security incidents will cause regional node failure, causing adjacent nodes in the region to generate WITHDRAW message information. The WITHDRAW message only advertises the prefix's unreachable information; so, only a tiny amount of the WITHDRAW message information is needed. The unreachability of a prefix will cause multiple routing information from different nodes to become invalid, which will cause a



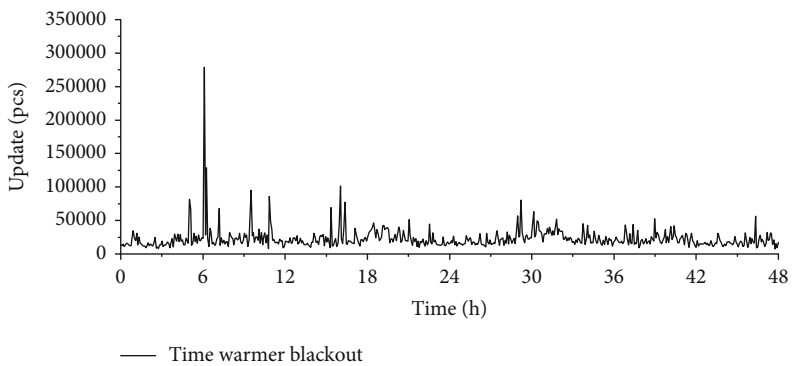
(a)



(b)

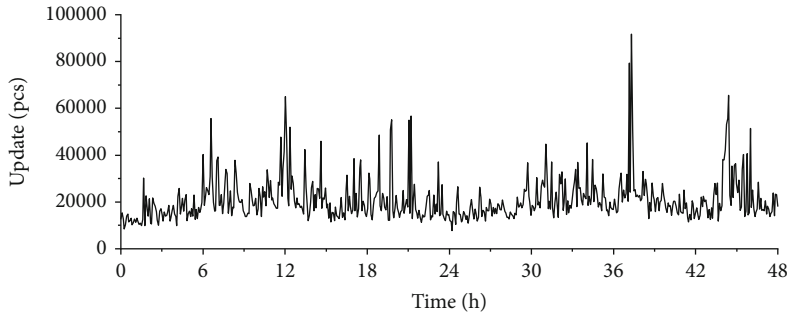


(c)

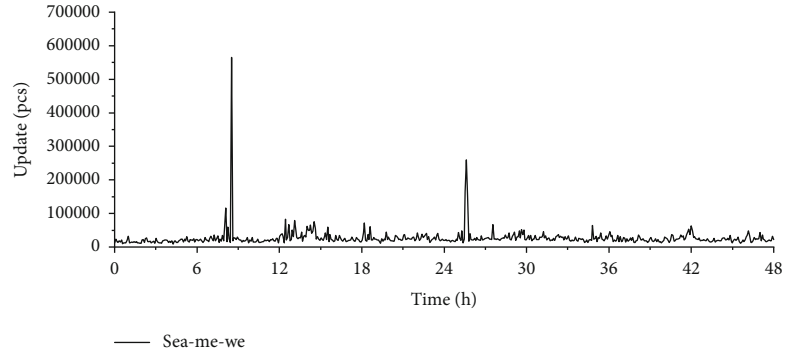


(d)

Figure 1: Continued.



(e)



(f)

Figure 1: Trends of UPDATE messages when different security incidents occur. (a) Slammer Worm, Jan.25, 2003. (b) Hurricane Katrina, Aug.29, 2005. (c) CISCO 512 K router failure, Aug.13, 2014. (d) Time Warmer blackout, Aug.27, 2014. (e) Malaysia route leak, June 12, 2015. (f) SEA-ME-WE-4 cable cut, May.17, 2016.

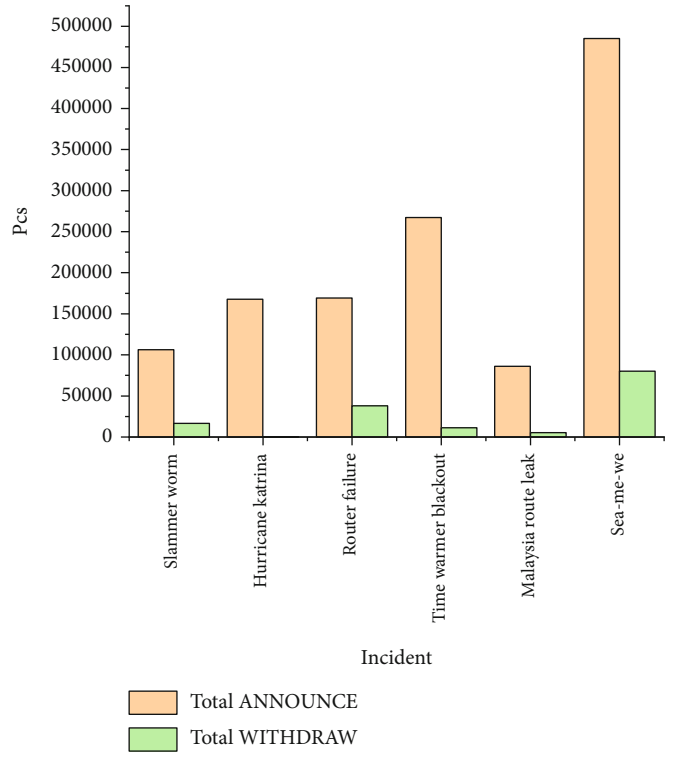


Figure 2: The number of ANNOUNCE and WITHDRAW messages when the number of UPDATEs is the largest.

large number of nodes to reroute, and then generate a large number of ANNOUNCE type messages.

To further analyze the UPDATE message's composition characteristics when a security incident occurs, based on the above data, we separately count the identical ANNOUNCE messages and WITHDRAW messages. We find that when a security incident occurs, the duplicate messages in the UPDATE collected from the observation point account for a relatively high proportion. We separately count the number of different ANNOUNCE messages and WITHDRAW messages compared with the initial total number shown in Figure 3. Figure 3(a) shows the number distribution before and after the repeated ANNOUNCE message is removed. Figure 3(b) shows the number distribution before and after the duplicated WITHDRAW message is removed. It can be seen from Figure 3 that, except for Hurricane Katrina, the UPDATE messages generated by other incidents contain a lot of repeated information, especially the Time Warmer blackout and Malaysia route leak. The repetition rate of ANNOUNCE messages is close to 50%.

From the previous analysis, it can be seen that there are two different update operations for the same network prefix P1. The ANNOUNCE message can be used to announce the P1 information, and the WITHDRAW message can be used to withdraw the reachability information of P1. Suppose two different types of UPDATE messages for P1 are continuously received at a node. In that case, the first message information will not change the network's final routing status, and we will regard it as an invalid message. When a security incident occurs, it is easy to generate consecutive different types of operations for the same prefix, which leads to network oscillations. Therefore, statistical analysis of this type of information is required. Besides, in the BGP protocol, routes with the same network prefix and next hop have a higher priority with a shorter path length. Therefore, if a node continuously receives two ANNOUNCE messages with the same prefix and next hop, but the path length is different, the ANNOUNCE with the longer path will not be updated to the RIB. Therefore, this type of message is also treated as an invalid message in this paper.

Through the above analysis, we can see that there will be a large number of repeated and invalid messages when a security incident occurs. We conduct comprehensive research of the above data set. After removing duplication and invalid UPDATE messages, the total number of messages after eliminating duplication and the total amount of original messages are counted. The results of the total number of three types of messages are shown in Figure 4.

Figure 4 shows that based on removing duplicate messages, by removing invalid messages, the total number of messages can be reduced a lot, which shows that the proportion of invalid messages is very high. In particular, the message information generated by incidents such as Slammer worm, CISCO 512 K router failure, and Malaysia route leak can still remove many invalid messages, reducing the total number of messages by more than 50%.

Through the above analysis, we can find that a large number of UPDATE messages generated in security incidents have the following component characteristics:

(1) Receive repeated WITHDRAW messages in a short time

(2) Receive repeated ANNOUNCE messages in a short time

(3) After receiving the ANNOUNCE message, a WITHDRAW message was received quickly, which caused the original ANNOUNCE message to become invalid

(4) After receiving the WITHDRAW message, receive the ANNOUNCE message with the same prefix and the next hop quickly, which causes the WITHDRAW message for the corresponding prefix to become invalid

(5) After receiving the ANNOUNCE message, the ANNOUNCE message with the same prefix and next hop is received in a short time, and the AS-PATH path length is shorter, causing repeated updates and waste of resources

4. SMSEI-SDN

From the previous analysis, we find that many UPDATE messages will be generated when a security incident occurs, and there are many repeated and invalid message information in these UPDATE messages. Elmokashfi et al. [28] analyzed unstable network incidents in the backbone network for up to 6 years and found that repeated UPDATE messages are the leading cause of network fluctuations. Therefore, how to deal with a large number of repeated and invalid messages generated when a security incident occurs is the key to restraining the impact of security incidents and maintaining the security and stability of the inter-domain routing system. This paper preprocesses the UPDATE message by establishing a cache mechanism before updating the RIB to reduce duplicate and invalid messages. The purpose is to minimize the invalid messages transmitted to the RIB and reduce routing the nodes' resource consumption.

4.1. UPDATE Message Preprocessing. This paper aims to reduce the number of duplicate and invalid messages transmitted to RIB by preprocessing the UPDATE message. How to preprocess the message first needs to determine which messages are repeated and invalid. This section first analyses the mechanism of the UPDATE message.

4.1.1. Mechanism of the UPDATE Message. According to the BGP protocol, when the border route receives an UPDATE message, it will update the RIB based on the message. It can be seen from the previous analysis that UPDATE messages are mainly divided into two types, ANNOUNCE messages that announce new routing information and WITHDRAW messages that disclose withdrawal information. The functions of the two types of messages are different, and the processing methods are also quite other.

When an ANNOUNCE message A1 (P1, N1, L1) is received, the prefix is P1, the next hop is N1, and the path length is L1. The RIB is updated according to the message information, and A1 is written into the RIB. When a new

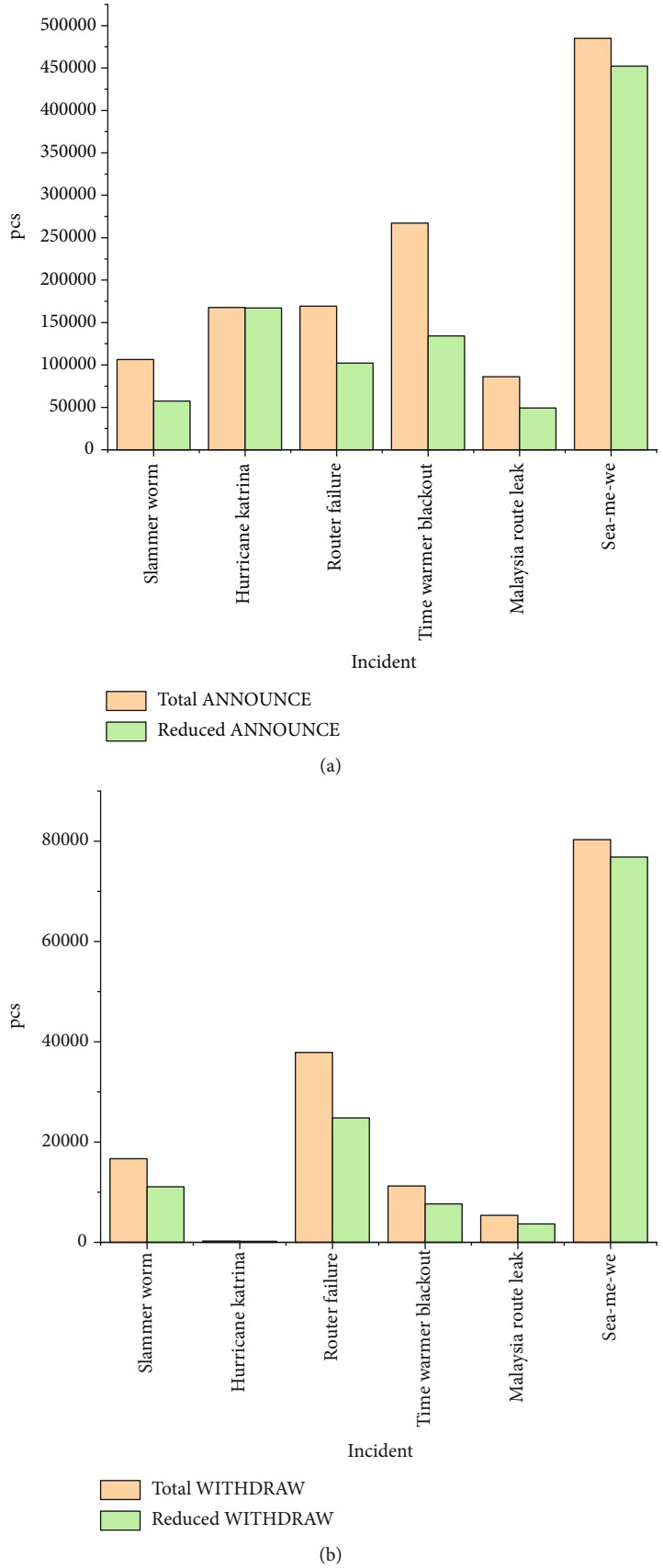


Figure 3: UPDATE message composition. (a) shows the comparison of the number of ANNOUNCE messages before and after removing the duplicate content. (b) shows the comparison of the number of messages before and after the repeated WITHDRAW message is drawn.

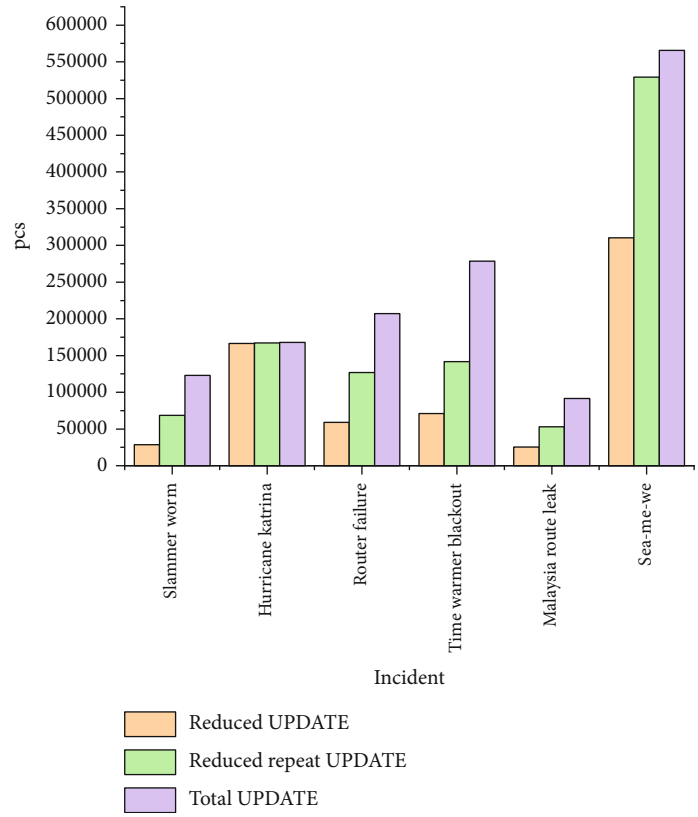


Figure 4: Distribution diagram of the total amount of UPDATE messages after different processing. Reduced UPDATE represents the total number of messages after removing duplicate and invalid UPDATE messages. Reduced repeat UPDATE represents the total number of messages after only removing duplicate UPDATE messages. Total UPDATE represents the total number of original messages.

UPDATE message is received, it is divided into the following situations: (1) when receiving a WITHDRAW message W1 (P1, N1), all routing information containing (P1, N1) will be withdrawn; so, the update information of message A1 will also be removed. (2) When ANNOUNCE message A2 (P1, N1, L1) is received, the RIB is updated based on the message because the message information is already in the RIB. Therefore, the result of the update is that the RIB has not changed. (3) When receiving ANNOUNCE message A3 (P1, N1, L2), if $L1 < L2$, message A3 does not provide a better path selection, and so after the update process, RIB will not change. Otherwise, A1 will be removed and updated to A3.

When receiving a WITHDRAW message W2 (P2, N2), all routing information with the prefix P2 and the next hop N2 is withdrawn. When a new UPDATE message is received, it is divided into the following situations according to different contents: (1) When a WITHDRAW message W3 (P2, L2) is received, the function of the message is also to withdraw all messages containing (P2, L2). (2) When the received message is the ANNOUNCE message A4 (P2, N2, L3), directly update the RIB based on the updated W2.

4.1.2. UPDATE Message Preprocessing Rules. Based on the above UPDATE message processing method and the different effects of ANNOUNCE message and WITHDRAW message in a separate order, we design corresponding processing rules, respectively, to reduce the repeated and invalid message information as much as possible in the preprocessing stage. The specific rules are as follows:

(1) For repeated WITHDRAW messages received within a short period, the previous analysis shows that the latter WITHDRAW message's effect can completely cover the previous WITHDRAW message's impact, so only the latter WITHDRAW message needs to be retained

(2) The repeated ANNOUNCE message received in a short period has the same processing methods as the WITHDRAW message. The purpose of the ANNOUNCE message is to update the RIB with new routing information. After the previous ANNOUNCE message updates the RIB, no matter what kind of update is made, the specific information needs to be updated to the RIB when the same ANNOUNCE message is received again. Therefore, the second ANNOUNCE message's scope contains the first message, and we can combine the two and keep only the latter

(3) The previous analysis shows that the new WITHDRAW message will withdraw all routing information with the same prefix and next hop. Therefore, all previously received ANNOUNCEs with the same prefix and next hop as the new WITHDRAW can be directly discarded in a buffering period

(4) When a new ANNOUNCE message is received, it is checked whether there is a WITHDRAW message for the same route in the buffering period. We find that the WITHDRAW message can withdraw all the same prefix and next hop routing information from the previous analysis. Therefore, after the WITHDRAW message is updated, there will be no routing information with the same prefix and next hop in the RIB, and the ANNOUNCE message can be marked. When the RIB is updated, the ANNOUNCE message does not need to be compared, and the update operation is directly performed

(5) When a new ANNOUNCE message is received, check whether an ANNOUNCE message with the same prefix and the next hop but with a longer path length is received during the buffer period. The previous analysis shows that the new shorter path ANNOUNCE message can replace the routing information with the same prefix and the next hop, but the longer route. Therefore, if there is an ANNOUNCE with a longer path during the cache time, it can be discarded directly

4.1.3. UPDATE Message Preprocessing Algorithm. Based on the five processing rules in 4.1.2, we propose an UPDATE message preprocessing algorithm for repeated and invalid UPDATE message information generated when a security incident occurs. The algorithm's primary process is as follows: for different UPDATE messages, establish ANNOUNCE message dictionary and WITHDRAW message dictionary, respectively. For each newly received message, determine whether it is an ANNOUNCE message or a WITHDRAW message.

For ANNOUNCE, first, determine whether the prefix is already in the ANNOUNCE message dictionary. If it is not in its dictionary, add it to the dictionary. If it is in its dictionary, continue to judge whether the original information needs to be updated based on the next hop and AS-PATH path length. If the next hop is different, update the routing information. Otherwise, if the path is shorter, update the routing information.

For WITHDRAW, determine whether the prefix is already in the WITHDRAW message dictionary; if it is not, add it to the WITHDRAW dictionary; if it is, do nothing. Then, determine whether it is in the ANNOUNCE dictionary. If so, determine whether the next hop address is the same, and if it is the same, remove it from the ANNOUNCE dictionary.

4.2. RIB Hierarchical Structure for Multi-level Retrieval. The analysis in Section 3 shows that the number of UPDATE messages caused by different security incidents and the proportion of ANNOUNCE is different. Besides, the processing of UPDATE messages has certain timeliness. If the cache time is too long, the convergence of the entire system will increase, and it will make the network continue to be in an unstable state. If the cache time is too short, duplicate and invalid packets cannot be effectively removed. Therefore, it is necessary to dynamically adjust the buffer time of UPDATE message preprocessing based on the characteristics of different security incidents, the scale of impact of security incidents, and message processing timeliness. Under the existing network framework, routing strategies cannot be dynamically adjusted according to the security status. Therefore, we introduce SDN technology and use SDN technology to implement dynamic routing management methods. This method is used to update the routing strategy in real-time according to different UPDATE message characteristics caused by security incidents.

After the UPDATE message is preprocessed, the routing information of the underlying network needs to be updated. We find that many UPDATE messages will be generated when a security incident occurs from the previous analysis. The number of these UPDATE messages is much higher than the number of UPDATE messages in a stable state. Using the UPDATE message preprocessing algorithm proposed in 4.1.3 can remove duplicate and invalid message information and reduce the total number of messages. However, due to the extensive range of security incidents, the number of UPDATE messages generated is too large. The total number of preprocessed messages is much higher than the total number of messages in the normal state. IP-SDN [10] is based on a two-level routing information storage structure. This structure can achieve better results when the RIB is small, and the number of update messages is negligible. Therefore, it is necessary to design a new routing storage structure to quickly find and update routing information when a security incident occurs.

With SDN technology, the storage form and routing update algorithm of the network can be dynamically updated and adjusted according to different network conditions. This paper uses the network prefix as the basis of the RIB index. According to the different characteristics of IPv4 and IPv6, the RIB hierarchy structure for multi-level search is designed. According to the IPv4 network prefix type, the network prefix P1 (A.B.C.D/E) is divided into four index items: A, B, C, and D/E. The last layer of index links the hash table of the same network prefix routing information, and the storage structure is shown in Figure 5. When a new UPDATE message is received, the message prefix is split into four levels, and the routing information position is quickly determined through multi-level matching. Then, update the RIB according to the routing rules. The RIB of the IPv6 protocol is similar to IPv4. The first three parts of the prefix are used as index items, and the remaining part is used as the fourth level index items. The routing update mechanism is the same as that of IPv4.

4.3. A Suppression Method of Security Incident Impact Based on SDN. This paper introduces SDN technology into AS node management. It uses the dynamic programmable features of SDN technology to conduct dynamic routing management based on the network status. The UPDATE message preprocessing algorithm is used to remove the duplicate and invalid UPDATE message information. The RIB hierarchical storage structure for multi-level search is used to improve the routing retrieval efficiency. By setting the caching time reasonably, A suppression method of

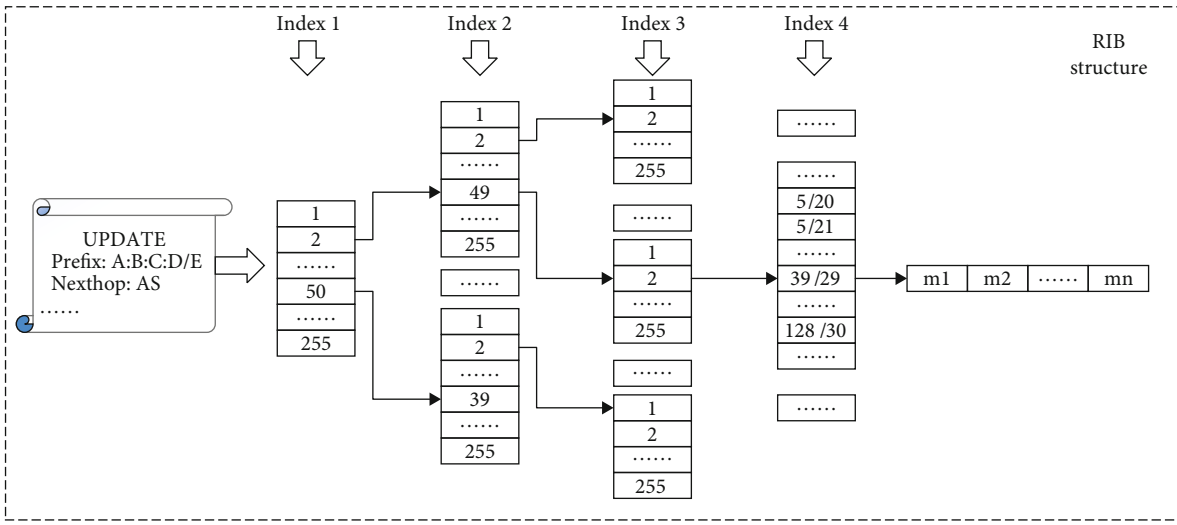


Figure 5: IPv4 RIB organization structure.

security incident impact for the inter-domain routing system based on SDN (SMSEI-SDN) is realized based on the existing routing update algorithm and controller strategy. The primary process of this method is shown in Figure 6.

When the network is in a normal state, no preprocessing operation is performed on the message, and the RIB is directly updated, and then the route is pushed. When a security incident occurs, enter the UPDATE message preprocessing module, start the timer to start timing, preprocess the newly input UPDATE message, and store the preprocessed message information in cache data. When the timer reaches the set cache time threshold, the timer is reset, and the route update is triggered. The route update module reads the cache data to be processed from the cache data module, then resets the cache data, re-enters the cache state, and starts a new preprocessing round. When the detected security incident ends, it enters the normal processing state.

5. Implement

To suppress the effects of failures caused by security incidents in the inter-domain routing system, maintain the Internet's security and stability, we design an SDN-based AS dynamic management framework (SDN-AS) to implement SMSEI-SDN. Figure 7 shows the SDN-AS implementation, which has two main parts: the UPDATE exchange mechanism, which realizes the ability to exchange BGP routing information with the legacy AS, and the SMSEI-SDN controller, which is mainly used for routing management of AS nodes.

UPDATE exchange mechanism. It is responsible for establishing a session between SDN-AS and legacy AS. SDN-AS can integrate SMSEI-SDN into the inter-domain routing system through this component, realize the incremental deployment of SMSEI-SDN without changing the large structure of the inter-domain routing system, and better realize the suppression of security incidents. BGP daemon is implemented by exabgp technology. SDN-AS uses BGP daemon to establish a peer-to-peer connection with legacy AS and transmits the UPDATE information.

SMSEI-SDN controller. It is realized by introducing UPDATE message preprocessing algorithm and routing update algorithm based on the RIB hierarchical structure based on Ryu controller. Its principal function is to interact with the AS in the inter-domain routing system for UPDATE information exchange and SDN-AS routing management. When a security incident occurs, SMSEI-SDN can preprocess excessive UPDATE messages and perform rapid routing updates through the routing update module.

6. Experimentation and Evaluation

We now evaluate the efficacy of our UPDATE message preprocessing algorithm and SMSEI-SDN via simulation on a small illustrative topology (in the Ubuntu environment on a machine with 16 cores of CPU and 64GB of RAM). Our simplified topology is shown in Figure 8. Figure 8(a) consists of 3 nodes, namely, our SMSEI-SDN node and two legacy nodes. We use the RIB information in the rrc01 collection in the RIPE project to implement the basal RIB of SMSEI-SDN. We simulate the UPDATE message's delivery process when a security event occurs by sending the UPDATE message in the rrc01 data set from AS1 to the SMSEI-SDN. We evaluate the effectiveness of the preprocessing algorithm and routing update algorithm by the processing of UPDATE messages. Based on the network environment in Figure 8(a), the SMSEI-SDN comparative experimental network is constructed using IP-SDN method RIB construction rules and basic routing update algorithm as shown in Figure 8(b).

6.1. Evaluation of UPDATE Message Preprocessing Algorithm. In this part, using the above experimental method and the network topology in Figure 8(a), we evaluate the effectiveness of the preprocessing algorithm by preprocessing the UPDATE message when a security event occurs, comparing the number of messages before and after preprocessing and the time required for routing updates. For the six security incidents mentioned above, select the data set of the collection period when the number of UPDATE messages is the

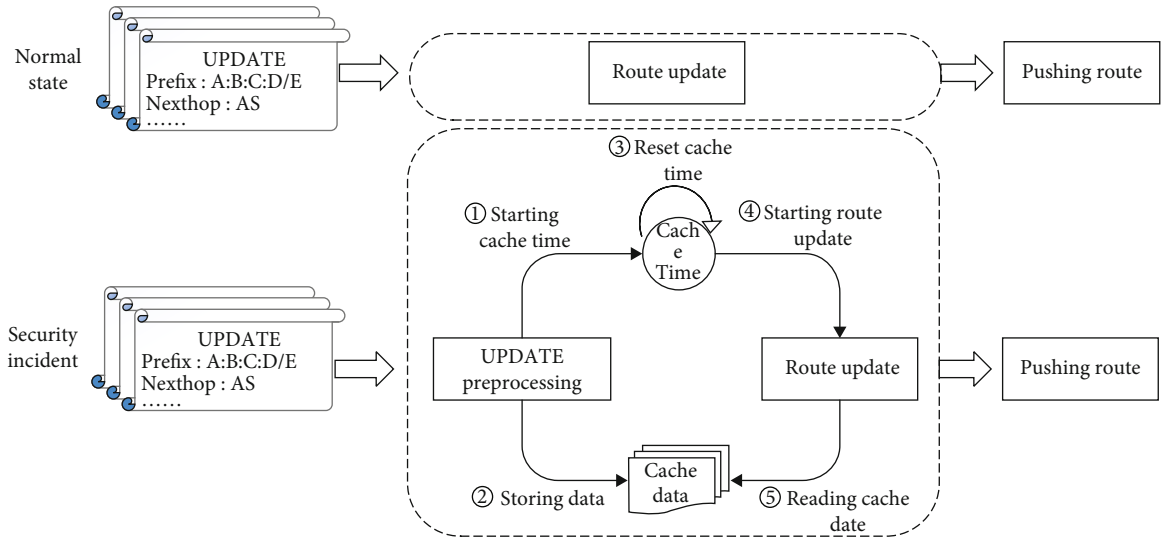


Figure 6: Working mechanism of SMSEI-SDN.

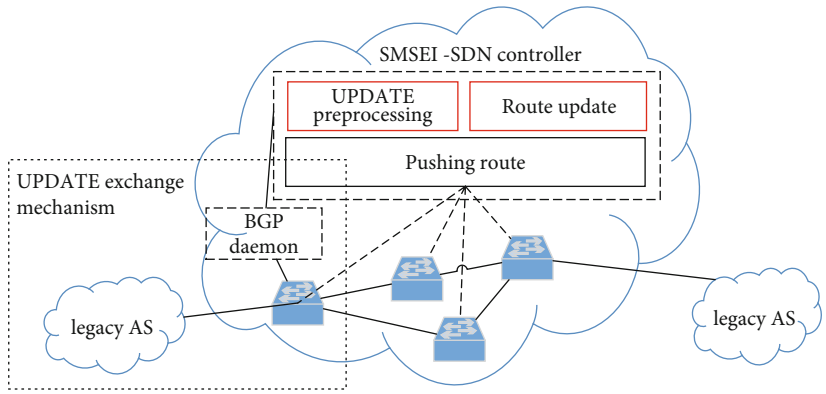


Figure 7: An SDN-based AS dynamic management framework.

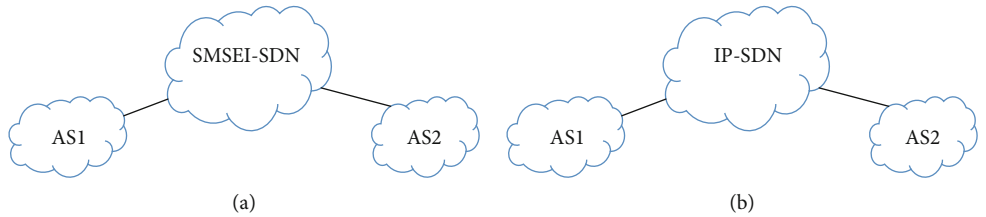
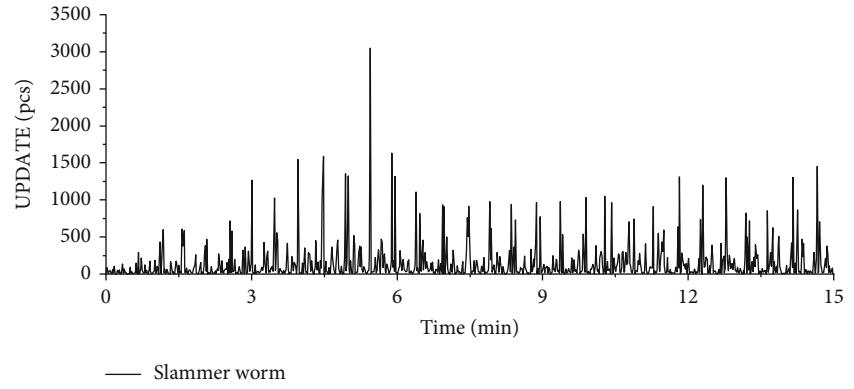


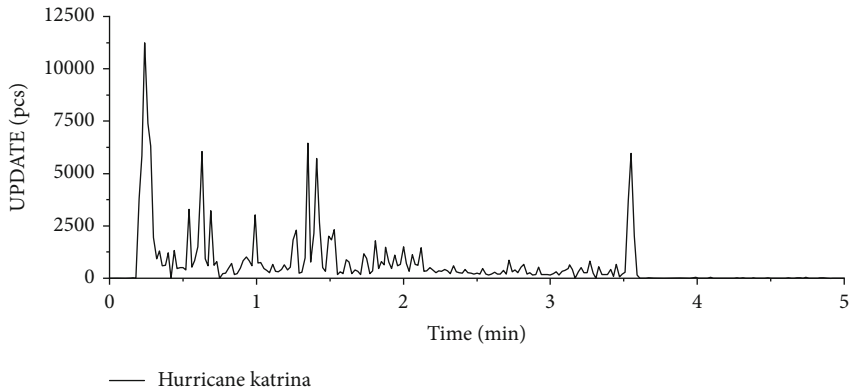
Figure 8: Small experimental topology. (a) SMSEI-SDN experimental network. (b) IP-SDN experimental network.

largest and count the number of packets per second. The results are shown in Figure 9.

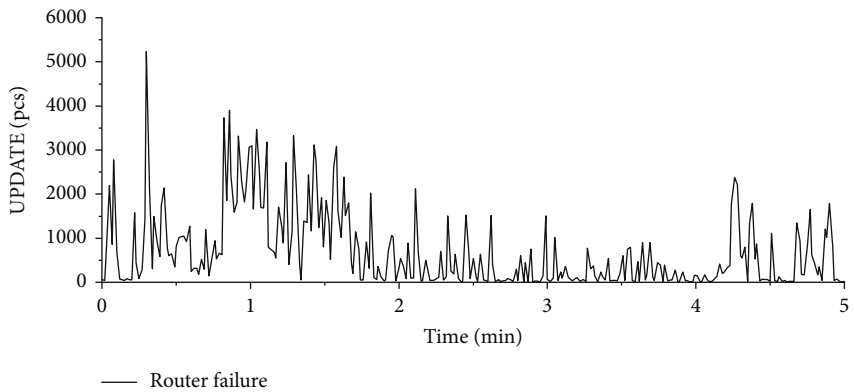
We can see from Figure 9 that when a security incident occurs, the number of messages received every second is several thousand, and the highest can reach more than 14,000. We choose the blackout that frequently occurs in the real world (Time Warmer blackout in this paper) to analyze. Since the minimum time unit of each message's timestamp is seconds, and the message processing timeliness, our experiment's minimum buffer time interval is set to 1 s. The maximum is set to 60 s. In this incident, when the UPDATE message reaches the peak value, we start to do 1 s, 2 s, 3 s, 4 s, 5 s, 10 s, 15 s, 20 s, 25 s, 30 s, 40 s, 50 s, and 60 s time buffering. The UPDATE original messages in the buffering interval are preprocessed. The comparison between the total number of preprocessed messages and the number of initial messages is shown in Figure 10. It can be seen from Figure 10 that the longer the cache interval, the more pronounced the change in the number of UPDATEs before and after preprocessing. Analysis of the data shows that SMSEI-SDN can reduce the total number of messages by an average of 19%. Besides, when the cache time is in 60 s, the total number of messages can be reduced by 34.9%.



(a)



(b)



(c)

Figure 9: Continued.

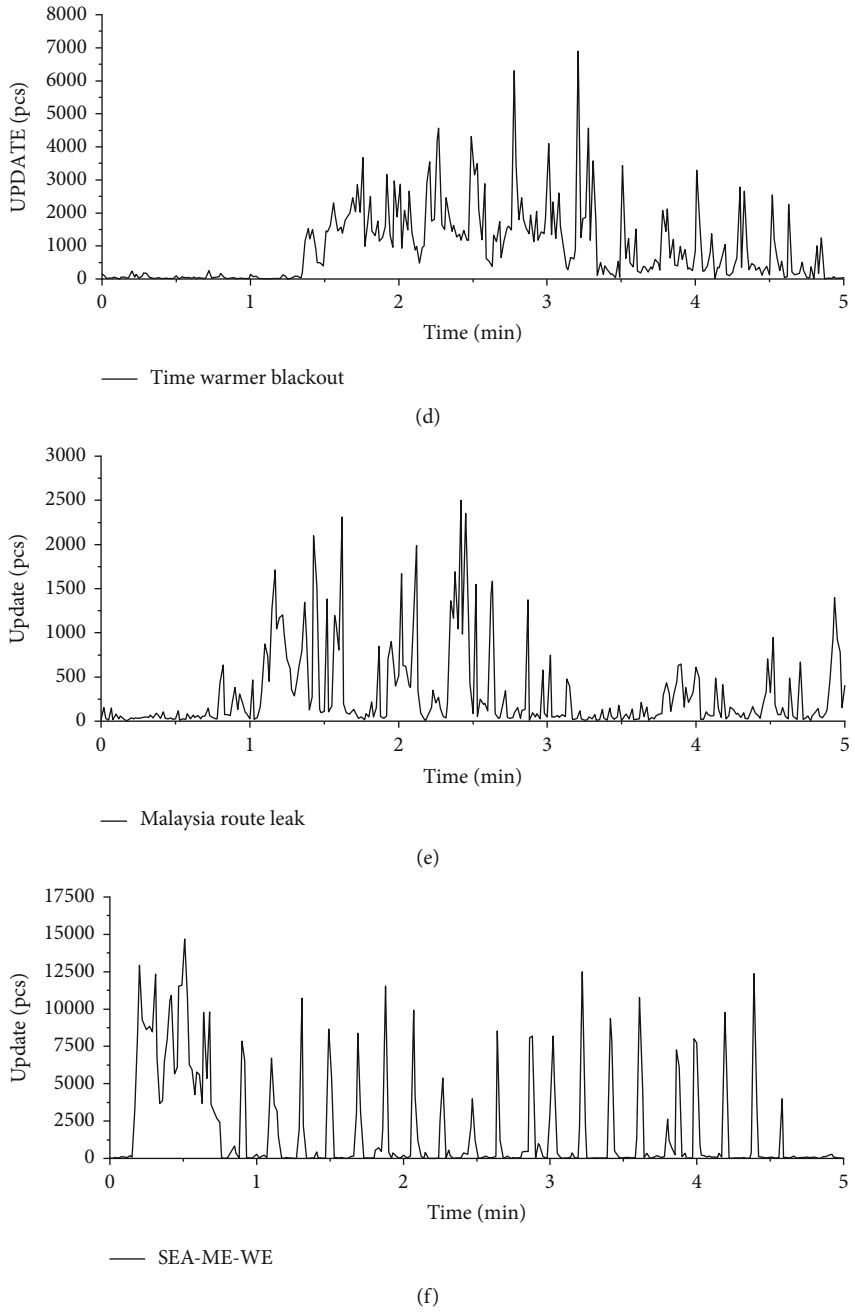


Figure 9: The changing trend of the number of packets per second. (a) Slammer worm. (b) Hurricane Katrina. (c) CISCO 512 K router failure. (d) Time Warmer blackout. (e) Malaysia route leak. (f) SEA-ME-WE-4 cable.

We use the SMSEI-SDN method to update the UPDATE messages with different buffer time intervals before and after preprocessing, and the processing time is shown in Figure 11.

Comparing Figures 10 and 11, it can be seen that the changing trend of UPDATE message processing time is consistent with the changing direction of the number of UPDATE messages. When the cache time is short, the update time will be faster, and the relative ratio of efficiency improvement is low. As the cache time increases, the message processing efficiency is significantly improved after preprocessing. The relative change ratio of the number of messages and the relative change ratio of UPDATE updates time are statistically analyzed. The results are shown in Figure 12.

We can see from Figure 12 that the trend of reduction in the number of UPDATE messages before and after preprocessing is basically the same as the trend of reduction in processing time, indicating that preprocessing of messages can significantly improve routing update efficiency. As the cache time increases, the overall efficiency improvement ratio continues to grow. From the general improvement trend, the preprocessing can increase efficiency by at least 5%. When the cache time is in 60 s, the efficiency is improved by more than 27.8%.

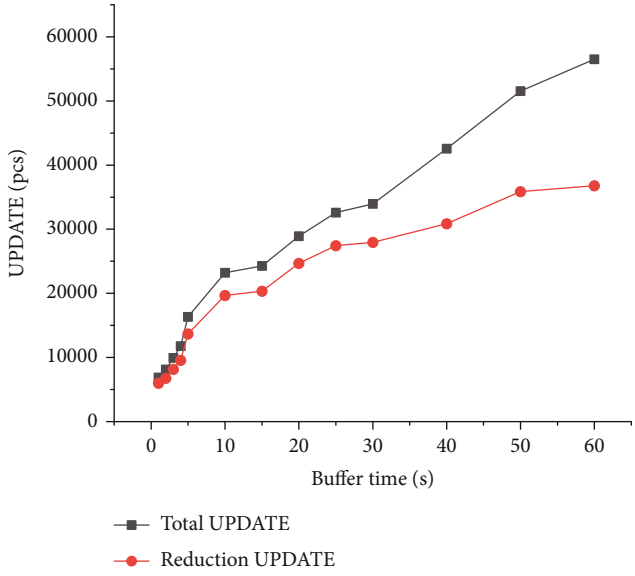


Figure 10: Change trend of the number of messages before and after UPDATE message preprocessing.

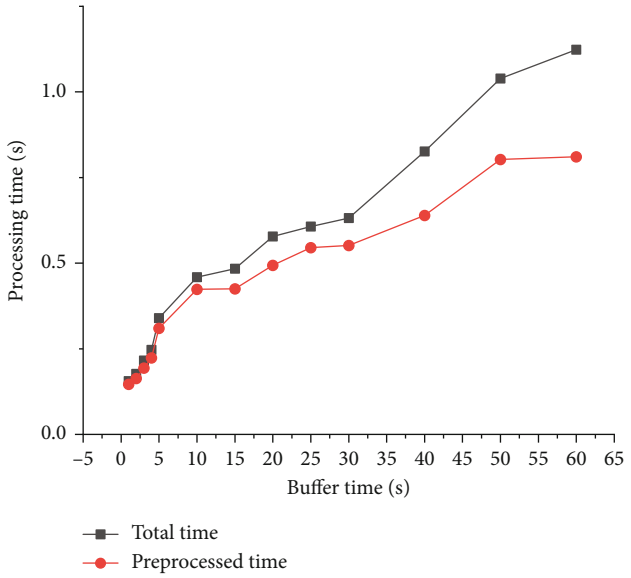


Figure 11: Change trend of UPDATE message update time with cache time.

Although the number of invalid messages removed is relatively low in the case of short cache time, the removal of invalid messages reduces the risk of network oscillations and enables the network to stabilize quickly. Besides, in large-scale network failures, the public network's convergence time is longer and can reach more than 30 mins. Therefore, under large-scale network failures, deploying SDN nodes on some key ASs and setting a longer cache time can effectively remove invalid information, reduce resource consumption, and enable the network to stabilize quickly.

6.2. Evaluation of SMSEI-SDN. SMSEI-SDN improves the processing efficiency of UPDATE messages at the level of a

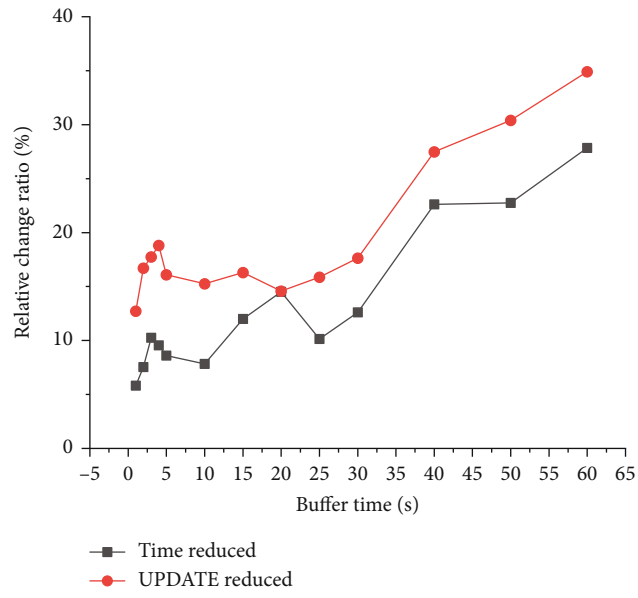


Figure 12: The relative change ratio of the number of messages and the update time before and after preprocessing.

single AS. IP-SDN [10] is also based on a single AS, combining IP networks and SDN switches to study UPDATE message processing. This paper uses the IP-SDN method and the SMSEI-SDN method to construct a routing information table based on the RIB information at the corresponding time in the RIPE data set. And the scale of the information table reaches 58 million. The experimental network topology is shown in Figure 8. We split the received UPDATE information into UPDATE message sub-datasets of different sizes according to different buffering time intervals. After that, we use the IP-SDN method and the SMSEI-SDN method to update the RIB using the sub-data set and count the time to update the RIB. The statistical results are shown in Figure 13.

It can be seen from Figure 11 that the processing time of SMSEI-SDN for UPDATE messages is much lower than that of the IP-SDN. Analysis of the data shows that SMSEI-SDN reduces the processing time by more than 99.98% compared to IP-SDN. And when the cache time is more excellent than the 40 s, the processing time of IP-SDN is ten thousand times that of SMSEI-SDN. There are three main reasons: (1) the IP-SDN method is mainly used for scenarios where adjacent nodes' edges are directly disconnected under small-scale network conditions. In this scenario, it has a unique processing mechanism to make the convergence time faster. Still, under large-scale network conditions, it needs to process many UPDATE messages, which exceeds its original design scale and processing capacity. (2) The SMSEI-SDN method reduces the number of UPDATE messages through preprocessing, reducing the time to update RIB. (3) When the IP-SDN method constructs the initial routing information table, it only divides the routing information table into two layers for processing. It organizes all routing information with the prefix as the index. Therefore, in a larger-scale routing information table, the search time required for each update is longer. When more UPDATE messages need to be updated, the total update time will be longer. The SMSEI-SDN method

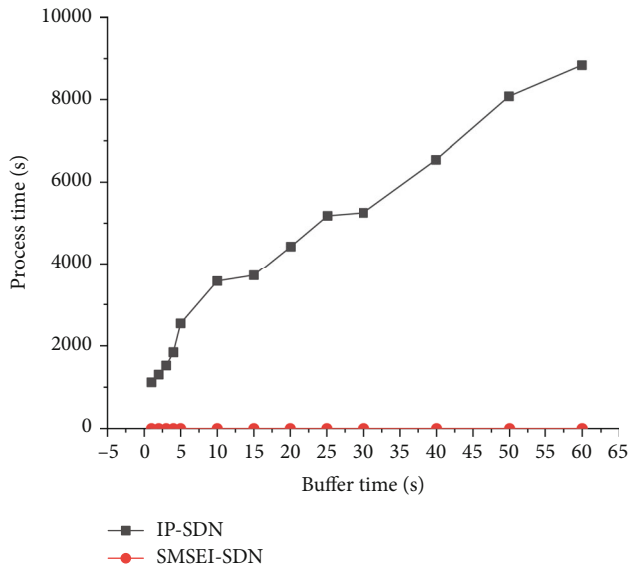


Figure 13: Comparison of UPDATE message processing time between SMSEI-SDN and IP-SDN methods for different buffering time intervals when a security incident occurs.

uses a multi-level search-oriented hierarchical structure to construct a routing information table, making the single search time shorter and effectively reduces the routing update delay.

7. Discussion

According to the previous statistical analysis, when a security incident occurs, many UPDATE messages will be generated in the inter-domain routing system. There are a large number of repeated and invalid messages in these UPDATE messages. Without preprocessing, these invalid messages would cause a lot of waste of resources and cause repeated network oscillations and even cascading failure. Therefore, it is necessary to preprocess these repeated and invalid messages, reduce resource consumption, and avoid network oscillations. This paper focuses on solving this problem. The experiment results show that SMSEI-SDN can achieve a specific effect, but determining the optimal cache time for preprocessing requires subsequent research and analysis.

Another important reason for the continuous oscillation of the inter-domain routing system is that the link that is about to be congested is not effectively avoided during path planning, resulting in constant failure of new links during the load redistribution process and even cascading failure. Using SDN technology to design a new routing update algorithm to solve cascading link failure caused by load redistribution will be a problem that we need to solve in the future.

8. Conclusion

This paper first analyzed UPDATE messages' composition characteristics when the inter-domain routing system encounters large-scale security incidents and found many repeated and invalid messages in the UPDATE messages generated during security incidents. After that, we designed five basic rules for handling duplicate and invalid messages by analyzing UPDATE messages' mechanisms. Furthermore, we proposed an UPDATE message preprocessing algorithm, which can remove same and invalid messages when a security incident occurs and reduce the total message volume by up to 34.9% after preprocessing. To solve the problem of slow route search in the existing SDN method, we designed a multi-level search-oriented RIB hierarchical structure, combined with the routing update strategy, and then realized SMSEI-SDN. Experimental results show that SMSEI-SDN reduces the processing time of excessive UPDATE messages by more than 99.98% compared to IP-SDN when a security incident occurs. Therefore, the use of SMSEI-SDN can improve the efficiency of routing updates and suppress the spread of security incident's impact.

Data Availability

The datasets of this work are available from the corresponding author on reasonable request.

Conflicts of Interest

The authors declare no conflicts of interest in publishing this article.

Acknowledgments

This work was funded by the National Natural Science Foundation of China (Nos. 61502528 and 61402525).

References

[1] Y. Nemoto and K. Hamaguchi, "Resilient ICT research based on lessons learned from the great East Japan earthquake," *IEEE Communications Magazine*, vol. 52, no. 3, pp. 38–43, 2014.

[2] S. Erjongmanee and C. Ji, "Large-scale network-service disruption: dependencies and external factors," *IEEE Transactions on Network and Service Management*, vol. 8, no. 4, pp. 375–386, 2011.

[3] J. Tapolcai, B. Vass, Z. Heszberger et al., "A tractable stochastic model of correlated link failures caused by disasters," in *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications*, pp. 2105–2113, Honolulu, HI, USA, 2018.

[4] C. Labovitz, A. Ahuja, A. Bose, and F. Jahanian, "Delayed internet routing convergence," *IEEE/ACM Transactions on Networking IEEE/ACM Transactions on Networking*, vol. 9, no. 3, pp. 293–306, 2001.

[5] A. Sahoo, K. Kant, and P. Mohapatra, "Speculative route invalidation to improve BGP convergence delay under large-scale failures," in *Proceedings of 15th International Conference on Computer Communications and Networks*, pp. 461–466, Arlington, VA, USA, 2006.

[6] W. Deng, P. Zhu, X. Lu, and B. Plattner, "On evaluating BGP routing stress attack," *The Journal of Communication*, vol. 5, no. 1, pp. 13–22, 2010.

[7] A. Sahoo, K. Kant, and P. Mohapatra, "BGP convergence delay under large-scale failures: characterization and solutions," *Computer Communications*, vol. 32, no. 7, pp. 1–14, 2009.

[8] A. Mitseva, A. Panchenko, and T. Engel, "The state of affairs in BGP security: a survey of attacks and defenses," *Computer Communications*, vol. 124, pp. 45–60, 2018.

[9] N. McKeown, T. Anderson, H. Balakrishnan et al., "OpenFlow: enabling innovation in campus networks," *ACM SIGCOMM Computer Communication Review*, vol. 38, no. 2, pp. 69–74, 2008.

[10] M. A. Chang, T. Holterbach, M. Happe, and L. Vanbever, "Supercharge me: boost router convergence with SDN," *ACM SIGCOMM Computer Communication Review ACM SIGCOMM Computer Communication Review*, vol. 45, no. 4, pp. 341-342, 2015.

[11] G. Aceto, A. Botta, P. Marchetta, V. Persico, and A. Pescapé, "A comprehensive survey on internet outages," *Journal of Network and Computer Applications*, vol. 113, pp. 36–63, 2018.

[12] K. Butler, T. R. Farley, P. McDaniel, and J. Rexford, "A survey of BGP security issues and solutions," *Proceedings of the IEEE*, vol. 98, no. 1, pp. 100–122, 2010.

[13] G. Huston, M. Rossi, and G. Armitage, "Securing BGP — a literature survey," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 199–222, 2011.

[14] A. Sahoo, K. Kant, and P. Mohapatra, "Improving BGP convergence delay for large-scale failures," in *International Conference on Dependable Systems and Networks (DSN'06)*, pp. 323–332, Philadelphia, PA, USA, 2006.

[15] E. A. Alabdulkreem, H. S. Al-Raweshidy, and M. F. Abbod, "MRAI optimization for BGP convergence time reduction without increasing the number of advertisement messages," *Procedia Computer Science*, vol. 62, pp. 419–426, 2015.

[16] V. Kotronis, A. Gämperli, and X. Dimitropoulos, "Routing centralization across domains via SDN: a model and emulation framework for BGP evolution," *Computer Networks*, vol. 92, pp. 227–239, 2015.

[17] H. Alotaibi, S. Li, and M. A. Gregory, "Utilising SDN to Counter BGP Convergence Delays," in *2019 29th International Telecommunication Networks and Applications Conference (ITNAC)*, pp. 1–6, Auckland, New Zealand, 2019.

[18] C. E. Rothenberg, M. R. Nascimento, M. R. Salvador, C. N. A. Corrêa, S. C. De Lucena, and R. Raszuk, "Revisiting routing control platforms with the eyes and muscles of software-defined networking," in *Proceedings of the first workshop on Hot topics in software defined networks - HotSDN '12*, pp. 13–18, Helsinki, Finland, 2012.

[19] V. Kotronis, X. Dimitropoulos, and B. Ager, "Outsourcing the routing control logic: better internet routing based on SDN principles," in *Proceedings of the 11th ACM Workshop on Hot Topics in Networks - HotNets-XI*, pp. 55–60, Redmond Washington, 2012.

[20] P. Lin, J. Hart, U. Krishnaswamy et al., "Seamless interworking of SDN and IP," *ACM SIGCOMM Computer Communication Review*, vol. 43, no. 4, pp. 475-476, 2013.

[21] P. Lin, J. Bi, S. Wolff et al., "A west-east bridge based SDN inter-domain testbed," *IEEE Communications Magazine*, vol. 53, no. 2, pp. 190–197, 2015.

[22] A. Gupta, L. Vanbever, M. Shahbaz et al., "SDX: A software defined internet exchange," *ACM SIGCOMM computer communication review*, vol. 44, no. 4, pp. 551–562, 2015.

[23] A. Gupta, R. MacDavid, R. Birkner et al., "An industrial-scale software defined internet exchange point," in *13th {USENIX} Symposium on Networked Systems Design and Implementation ({NSDI} 16)*, pp. 1–14, Santa Clara, CA, 2016.

[24] Z. Chen, J. Bi, Y. Fu, Y. Wang, and A. Xu, "MLV: a multi-dimension routing information exchange mechanism for inter-domain SDN," in *2015 IEEE 23rd International Conference on Network Protocols (ICNP)*, pp. 438–445, San Francisco, CA, USA, 2015.

[25] Y. Wang, J. Bi, P. Lin, Y. Lin, and K. Zhang, "SDI: a multi-domain SDN mechanism for fine-grained inter-domain routing," *Annales des Telecommunications*, vol. 71, no. 11–12, pp. 625–637, 2016.

[26] Y. Wang, J. Bi, and K. Zhang, "A SDN-based framework for fine-grained inter-domain routing diversity," *Mobile Networks and Applications*, vol. 22, no. 5, pp. 906–917, 2017.

[27] RIPE database, *Ripe Network Coordination Centre*, 2021, https://www.ripe.net/analyse/internet-measurements/routing-information-service-ris/ris-raw-data.

[28] A. Elmokashfi, A. Kvalbein, and C. Dovrolis, "BGP churn evolution: a perspective from the core," *IEEE/ACM Transactions on Networking*, vol. 20, no. 2, pp. 571–584, 2012.