International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Series X

Supplement 18

(04/2013)

SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

ITU-T X.1205 – Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks

ITU-T X-series Recommendations – Supplement 18

ITU-T
International Telecommunication Union

ITU-T X-SERIES RECOMMENDATIONS

DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY

PUBLIC DATA NETWORKS	X.1–X.199
OPEN SYSTEMS INTERCONNECTION	X.200–X.299
INTERWORKING BETWEEN NETWORKS	X.300–X.399
MESSAGE HANDLING SYSTEMS	X.400–X.499
DIRECTORY	X.500–X.599
OSI NETWORKING AND SYSTEM ASPECTS	X.600–X.699
OSI MANAGEMENT	X.700–X.799
SECURITY	X.800–X.849
OSI APPLICATIONS	X.850–X.899
OPEN DISTRIBUTED PROCESSING	X.900–X.999
INFORMATION AND NETWORK SECURITY	
General security aspects	X.1000–X.1029
Network security	X.1030–X.1049
Security management	X.1050–X.1069
Telebiometrics	X.1080–X.1099
SECURE APPLICATIONS AND SERVICES	
Multicast security	X.1100–X.1109
Home network security	X.1110–X.1119
Mobile security	X.1120–X.1139
Web security	X.1140–X.1149
Security protocols	X.1150–X.1159
Peer-to-peer security	X.1160–X.1169
Networked ID security	X.1170–X.1179
IPTV security	X.1180–X.1199
CYBERSPACE SECURITY	
Cybersecurity	X.1200–X.1229
Countering spam	X.1230–X.1249
Identity management	X.1250–X.1279
SECURE APPLICATIONS AND SERVICES	
Emergency communications	X.1300–X.1309
Ubiquitous sensor network security	X.1310–X.1339
CYBERSECURITY INFORMATION EXCHANGE	
Overview of cybersecurity	X.1500–X.1519
Vulnerability/state exchange	X.1520–X.1539
Event/incident/heuristics exchange	X.1540–X.1549
Exchange of policies	X.1550–X.1559
Heuristics and information request	X.1560–X.1569
Identification and discovery	X.1570–X.1579
Assured exchange	X.1580–X.1589

For further details, please refer to the list of ITU-T Recommendations.

Supplement 18 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks

Summary

Telecommunication networks based on the IP protocol face many security threats. One of the most important threats is abnormal traffic, which can cause serious impact on the secure and steady operation of telecommunication networks. Abnormal traffic attacks consume large quantities of network resources and easily lead to network unsteadiness and link blockage. Moreover, abnormal traffic attacks have increasingly been aimed at achieving certain business objectives, and are a great challenge to telecommunication operators. Therefore, detecting and controlling abnormal traffic effectively has become an urgent task for telecommunication operators.

Supplement 18 to ITU-T X.1205 series of Recommendations identifies abnormal traffic detection technologies and control measures for IP-based telecommunication networks. The aim of this Supplement is to provide telecommunication operators with a comprehensive guideline for monitoring, detecting and controlling abnormal IP traffic.

History

Edition	Recommendation	Approval	Study Group
1.0	ITU-T X Suppl. 18	2013-04-26	17

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this publication, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this publication is voluntary. However, the publication may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the publication is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the publication is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this publication may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the publication development process.

As of the date of approval of this publication, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this publication. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

Supplement 18 to ITU-T X-series Recommendations

ITU-T X.1205 – Supplement on guidelines for abnormal traffic detection and control on IP-based telecommunication networks

1 Scope

This Supplement provides guidelines to telecommunication operators on how to utilize abnormal traffic detection and control technologies to protect their IP-based networks. This Supplement also describes the impacts of abnormal traffic and provides an overview of abnormal traffic detection technologies and control measures.

2 References

None.

3 Definitions

3.1 Terms defined elsewhere

None.

3.2 Terms defined in this Supplement

This Supplement defines the following terms:

3.2.1 abnormal traffic: Traffic other than the normal service and signalling traffic that is allowed by the network operator. Abnormal traffic is caused by distributed denial of service (DDoS), worm attacks, spam, etc.

3.2.2 abnormal traffic control system: Software systems or hardware products that control abnormal traffic based on information produced by the abnormal traffic detection system.

3.2.3 abnormal traffic detection system: Software systems or hardware products that detect abnormal traffic.

4 Abbreviations and acronyms

This Supplement uses the following abbreviations and acronyms:

ACL Access Control List

BRAS Broadband Remote Access Server

CPU Central Processing Unit

DDoS Distributed Denial of Service

DoS Denial of Service

FIN Final (one of the control bits in the TCP protocol header)

FTP File Transfer Protocol

IP Internet Protocol

IXP Internet eXchange Point

MPLS Multiprotocol Label Switching

OD Origin – Destination

PCA Principal Component Analysis

QoE Quality of Experience

QoS Quality of Service

RIPE Réseaux IP Européens

RST Reset (one of the control bits in the TCP protocol header)

TCP Transmission Control Protocol

UDP User Datagram Protocol

5 Conventions

None.

6 Impacts of abnormal traffic on telecommunication networks

6.1 Impacts on network availability

Certain types of abnormal traffic can impede or prevent the ability of networks to provide services as a result of congestion or service failure of the network equipment and links. A distributed denial of service (DDoS) attack is a good example of one type of abnormal traffic that can affect network availability.

A DDoS attack is derived from the traditional denial of service (DoS) attack. A traditional DoS attack commonly adopts the one-to-one attack mode. A DoS attack will have a negative impact on a target that has limited resources such as, processing ability, memory or bandwidth. However, with the rapid increase of computer ability, memory capacity, and network bandwidth, DoS attacks initiated by a single host have become ineffective. A DDoS attack makes use of a large number of zombie computers, each performing small-scale attacks, but coordinated in their efforts in performing large scale distributed DoS attacks, thus resulting in a higher bandwidth, focused attack.

6.2 Impacts on network quality of service

Some abnormal traffic can affect the network's quality of service (QoS), by influencing the available bandwidth, packet latency and jitter.

6.3 Impacts on service income

Some abnormal traffic originates from service applications that are not consistent with the interests of network operators. These unexpected services may reduce the income of the operators, who consider them as a type of abnormal traffic and thus may put them under control.

6.4 Impacts on customer's quality of experience

From a customer's point of view, a decrease in network availability and QoS usually leads to a degraded quality of experience (QoE). In addition, some abnormal traffic, such as spam, is not only annoying, but also occupies a large portion of a network's bandwidth. Spam also causes network equipment to work in a heavy load state for long periods of time, and blocks a customer's normal services such as Internet access, e-mail and video-on-demand. This also has a negative impact on the customer's QoE.

7 Abnormal traffic detection technology

7.1 Anomaly detection

Anomaly detection methods model the normal state of a network. If current network traffic is different from the normal modelled (i.e., baseline) traffic, it is considered abnormal.

This method is usually based on a statistical analysis mechanism. The detection accuracy of this method is closely related to the establishment algorithm of the normal traffic model. The parameters of the algorithm must be chosen carefully and intelligent self-learning capabilities are usually needed.

Because this method does not depend on a database of known attacks (i.e., signatures), it can detect unknown attacks, resulting in a lower false negative rate. This is an advantage over the misuse detection method described below. However, the false positive rate of the anomaly detection method can be higher than that produced using the misuse detection method.

7.2 Misuse detection

In misuse detection methods, network traffic data is compared against large databases of documented attack signatures. If they match, then the network traffic is considered abnormal.

An attack knowledge database is one that stores the attack features extracted from known attack data. The attack knowledge database is the key factor that influences the detection accuracy of a misuse detection method.

Using a proper matching algorithm, misuse detection can reduce the false positive rate significantly. However, the false negative rate is difficult to reduce because this method cannot detect unknown new attacks. In addition, small changes of attack features may also result in false negatives.

7.3 Synthetic analysis

The main advantage of misuse detection is that the detection accuracy of known attacks can be very high. However, its main disadvantage is that it can only detect known attacks. Any new, unknown attacks will cause false negatives. Anomaly detection methods can detect known or unknown attacks, so the false negative rate can be significantly lowered as compared with misuse detection methods. Nevertheless, the main weakness of anomaly detection is that its detection accuracy is not very high and there may be many false positives.

Based on the above analysis, these two methods can be combined to achieve higher efficiency and detection of abnormal traffic. The corresponding deployment mode is described below:

1) Anomaly detection is used first, to provide primary filtering for high bandwidth traffic. Then normal traffic can be differentiated and does not need to be inspected further. Only the traffic that is different from the normal model needs to be further inspected using the misuse detection method, greatly reducing its work load. This deployment mode demonstrates its merits in high efficiency and low false negative rates.
2) Misuse detection is used to perform accurate feature matching only against the traffic identified by anomaly detection, thus taking advantage of its merits in low false positive rates.

NOTE − Some attacks cannot be addressed by either detection mode.

8 Abnormal traffic control measures

8.1 Control mode

There are three ways to control abnormal network traffic: in-path (in-line), out-of-path (bypass), and a combination of both (i.e., in-path, out-of-path cooperation). All three are different in several aspects, including: deployment, effect, performance, influence on network, etc.

8.1.1 In-path control

For the in-path control mode, the detection and control equipment resides directly in the network link. This provides an advantage in that the equipment can control or filter the abnormal traffic directly as it is detected. However, there are four disadvantages to this control mode:

The first is the single-point failure. Because the equipment is a necessary element of the network link, if the equipment is damaged and no longer works, the network link will be broken. A solution to this problem is to add additional equipment as a backup, or implement a bypass switch policy.

The second problem is the forwarding performance and the ability for detection database updating. When traffic load is high and exceeds the process capability of the in-path control equipment, the network QoS will be impacted. Moreover, the detection database of the equipment needs to be periodically updated. In in-path control mode, the online update of the database is more difficult than the offline update.

The third problem is that routing policies need to be changed in some cases. In some network scenarios, the traffic routing path may be asymmetric. In order to allow the abnormal traffic detection system to detect full traffic sessions, routing policies must be changed.

The fourth problem is that the latency introduced by the detection and control equipment under the in-path control mode may significantly reduce the customer's QoE for some applications.

When the detection and control equipment is deployed in a high bandwidth core network (such as the 10G metro network), the above problems will become more serious.

8.1.2 Out-of-path control

For the out-of-path (i.e., bypass) control mode, the detection and control equipment does not reside in the network link directly. Rather, it obtains a complete copy of the network traffic from a mirror port and performs the detection analysis on this traffic copy.

The significant advantage of out-of-path control is that the equipment has no impact on the existing network topology. Moreover, performance problems can be solved by adding additional detection and control equipment.

The main problem of the out-of-path mode is traffic control. For applications based on the transmission control protocol (TCP), connections can be closed by sending TCP Reset (RST)/Final (FIN) packets, or can be slowed down by reducing the TCP session window value. For applications using the user datagram protocol (UDP), in order to control abnormal traffic flow, the application protocol needs to be analysed, which is difficult and requires a great amount of work.

8.1.3 In-path out-of-path cooperation

In this mode, the in-path control equipment and the out-of-path detection equipment cooperate to perform the detection and control functions. For example, the out-of-path detection equipment sends commands to the in-path equipment such as the broadband remote access server (BRAS) or firewall equipment to perform traffic flow control. The advantage of this mode is that it makes use of the powerful control functions of the in-line equipment without introducing new fault points into the network.

8.2 Control granularity

There are two types of traffic control technologies based on the control granularity, as follows.

8.2.1 Packet-based traffic control

Packet-based traffic control technology checks each Internet protocol (IP) packet against specific access control lists (ACLs) to decide whether the packet can be permitted. The ACLs are defined based on the packet header information such as, source IP address, destination IP address, source port, destination port, transport protocol type, and packet length. Packet-based traffic control technology discards all rejected packets based on ACLs.

The most obvious advantages of the packet-based traffic control technology are high filtering speed and high efficiency. However, because it only controls traffic based on single packets and cannot check the protocol session state, the control granularity is limited. Moreover, for the multi-channel

protocols (such as file transfer protocol (FTP)) where one or more data channels are negotiated dynamically during the session, the port information associated with these channels is not known in advance. Therefore, the packet-based traffic control technology is ineffective for these protocols since the required ACLs cannot be defined with the necessary (dynamic) port information.

8.2.2 Session-based traffic control

Session-based traffic control technology controls traffic based on the session status of the application or transport protocols. Session status information of all connections is maintained and used for controlling the traffic dynamically. For example, for TCP connections, session-based traffic control can detect handshake messages and maintain current handshake status. TCP packets which do not coincide with the status information are discarded.

Session-based traffic control technology supports multichannel protocols. In a multichannel protocol scenario, the protocol initiates a control connection with a fixed port and transfers data to one or more connections which are negotiated dynamically. Because data transport ports are unpredictable, packet-based traffic control technology cannot control the traffic correctly in these scenarios. In contrast, the session-based traffic control technology can work well here. The session-based traffic control technology can observe the protocol status and add ACLs dynamically based on the negotiation information of the data channel. When the data channel is disconnected, ACLs are deleted accordingly. In this manner, the session-based traffic control technology can correctly control multichannel protocol traffic.

Appendix I

Overview of anomaly detection algorithms, systems and practices

I.1 Introduction

This appendix describes some of the most popular algorithms used in anomaly detection. In addition, and some typical work in several network operators group is briefly introduced.

I.2 Algorithm overview

In reference to their monitoring scope, anomaly detection systems can be divided into two categories: single link anomaly detection systems, and wide-network anomaly detection systems.

A typical single-link anomaly detection system aims to detect anomalous behaviour of the network traffic transferred through a link.

A wide-network anomaly detection system, however, attempts to detect abnormal behaviour of the traffic within a network consisting of multiple links. In order to benefit the analysis, many wide-network anomaly detection systems organize the collected network traffic data as origin-destination (OD) flows as illustrated in Figure I.1.

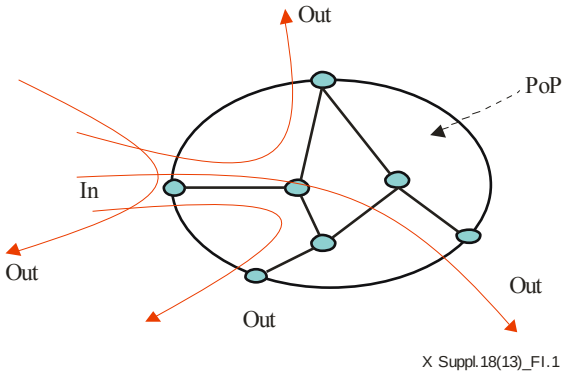

Figure I.1 – Origin-Destination flows

I.2.1 Algorithm examples used in single-link anomaly detection systems

This clause introduces three types of algorithms used in single-link anomaly detection systems: the time series analysis algorithm, the wavelet algorithm, and the clustering algorithm.

Time series analysis algorithms are developed to predict the next value or verify the current state of a time series based on historical records. A common feature of time series analysis algorithms is that the weights of historical values in the process of predicting future values decrease as time passes. [b-Brutlag] proposes a single-link anomaly detection approach based on an enhanced Holt-Winters forecasting algorithm. This system organizes the collected traffic data at different time points as a time series and uses the enhanced Holt-Winters forecasting algorithm to verify whether any abnormal network behaviour is detected on the monitored link.

Wavelet algorithms use wavelets, which are functions that satisfy certain mathematical requirements, to process signals at different scales or resolutions. For example, if a signal is analysed with a large time "window", gross features (the low frequency part of the signal) will be detected. Similarly, if a signal is analysed with a small time "window", detailed features (the high frequency part of the signal) will be detected. [b-Barford] proposes a wavelet-based anomaly detection system which uses a wavelet algorithm to divide the signals of the network traffic into different frequency-bands and analyses the signals in different bands respectively. In the paper, multiple types of anomalies (e.g., flash crowd, DoS) which cause changes of the network traffic in

different frequencies are introduced. By analysing the deviations observed at different bands, this system can effectively clarify one type of anomaly from another.

Clustering algorithms are designed to find patterns in unlabelled data with many dimensions; the data similar in certain aspects will be automatically classified into the same cluster. [b-Münz] uses a *k*-means algorithm to construct the anomaly detection system. This work is based on the assumption that most traffic volumes transported in the monitored network are normal. Initially, a *k*-means algorithm with unlabelled data, which consists of both normal as well as attack traffic, is trained. The group with the largest number of members is regarded as normal traffic, while others are treated as attacks. After this, the weighted Euclidean distance function is used to evaluate the similarity between an observed data with the centroids of the corresponding traffic clusters.

I.2.2 Algorithm examples used in wide-network anomaly detection systems

In this clause, two types of algorithms used in wide-network anomaly detection systems are introduced: the Kalman filter, and the clustering analysis and the principal component analysis (PCA).

The Kalman filter is a set of mathematical equations that are able to recursively estimate the state of a process, in a way that minimizes the mean of the squared error. This filter supports estimations of past, present, and future states, and it can do so even from a series of noisy measurements. [b-Soule] proposes a wide-network anomaly detection system which collects traffic data of all the OD flows of a monitored network and organizes them as a traffic matrix. In this approach, the Kalman filter algorithm is used to predict the future normal state of the traffic matrix. The deviation between the predication and the actual observed traffic matrix state thus can be utilized to detect abnormal events.

PCA is able to transform n correlated variables into a sequence of n uncorrelated variables (principal components). The principal components are linear combinations of the original variables. Typically, the *ith* principal component of the transformation is the linear combination of the original variables with the *ith* largest variance. In many data sets, the first several principal components contribute most of the variance in the original data set, and disregarding the remaining principal components only results in minimal loss of the variance. Therefore, the first d principal components can be used to express the data in a reduced form, where $d < n$. [b-Lakhina] makes use of PCA to detect traffic anomaly. This approach is able to: 1) correctly identify the underlying OD flow which is the source of the anomaly, and 2) accurately estimate the amount of traffic involved in the anomalous OD flow.

I.3 Work in network operator groups

The North American Network Operators' Group (NANOG), see [b-NANOG], reviews current industry best practices for planning and traffic engineering in IP and multi-protocol label switching (MPLS) networks. The subjects typically covered include traffic/demand matrices and traffic engineering options and approaches, etc.

In the Latin American and Caribbean Region Network Operators Group (LACNOG), see [b-LACNOG], two topics on "traffic engineering" and "peerings, regional traffic exchange and Internet exchange points (IXPs)" are being investigated.

The Test Traffic Working Group of RIPE, see [b-RIPE], uses test traffic boxes located in the networks to measure the performance parameters of the Internet. By discussing project results and providing comments, the administrative and technical coordination necessary to maintain and develop the Internet can be ensured.

Bibliography

[b-Barford] Barford, P., Kline, J., Plonka, D., and Ron, A. (2002), *A signal analysis of network traffic anomalies*, Proceedings of the 2nd ACM SIGCOMM Workshop on Internet measurement.

[b-Brutlag] Brutlag, J.D. (2000), *Aberrant Behavior Detection in Time Series for Network Monitoring*, USENIX.

[b-LACNOG] Latin American and Caribbean Network Operators Group, *Routing: Traffic engineering; Peerings, regional traffic exchange and IXPs*. <http://www2.lacnic.net/en/eventos/lacnicxviii/index.html>

[b-Lakhina] Lakhina, A., Crovella, M., and Diot, C. (2004), *Diagnosing Network-Wide Traffic Anomalies*, Proc. ACM SIGCOMM (2004) 19.

[b-Münz] Münz, G., Li, S., and Carle, G. (2007), *Traffic anomaly detection using k-means clustering,* Proceedings of Leistungs-,Zuverlässigkeits-und Verlässlichkeitsbewertung von Kommunikationsnetzen und Verteilten Systemen, GI/ITG-Workshop MMBnet.

[b-NANOG] North American Network Operators' Group, *Best Practices in Network Planning and Traffic Engineering.* <http://www.nanog.org/meetings/nanog52/abstracts.php?pt=MTc2NyZuYW5vZzUy&nm=nanog52>

[b-RIPE] Réseaux IP Européens, Test Traffic Working Group. <http://www.ripe.net/ripe/groups/inactive-working-groups/test-traffic-working-group>

[b-Soule] Soule, A., Salamatian, K., and Taft, N. (2005), *Combining Filtering and Statistical Methods for Anomaly Detection*, Proceedings of the 5th ACM SIGCOMM conference on Internet measurement.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	General tariff principles
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Terminals and subjective and objective assessment methods
Series Q	Switching and signalling
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	**Data networks, open system communications and security**
Series Y	Global information infrastructure, Internet protocol aspects and next-generation networks
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2013