SESSION-BASED TRAFFIC ANALYSIS SYSTEM

INVENTOR: Kyu-Min Choi, Seoul (KR)

ASSIGNEE: Plustech Inc., Seoul (KR)

NOTICE: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 302 days.

Appl. No.: 13/882,724
PCT Filed: Nov. 7, 2011
PCT No.: PCT/KR2011/008413
§ 371 (c)(1), (2), (4) Date: Jul. 15, 2013
PCT Pub. No.: WO2012/064056
PCT Pub. Date: May 18, 2012

Prior Publication Data

Foreign Application Priority Data
Nov. 9, 2010 (KR) 10-2010-0111031

Int. Cl.
H04L 12/26 (2006.01)
H04L 11/00 (2006.01)

U.S. Cl.
CPC 1H04L 43/08 (2013.01); 1H04L 43/022 (2013.01); 1H04L 43/028 (2013.01); 1H04L 43/026 (2013.01)

INTERNET

TRAFFIC MIRRORING MEANS

TRAFFIC ANALYSIS DEVICE

INTERNET USER

Field of Classification Search
USPC ........................................... 370/252, 225
See application file for complete search history.

References Cited
U.S. PATENT DOCUMENTS

FOREIGN PATENT DOCUMENTS
KR 1020100072975 A 7/2010

OTHER PUBLICATIONS
* cited by examiner

Primary Examiner — Kjet Tung
(74) Attorney, Agent, or Firm — Seed IP Law Group PLLC

ABSTRACT
The present invention relates to a session-based traffic analysis system that may accurately analyze an amount of traffic for each transmission control protocol (TCP) connection using only one-way packets. The system may accurately analyze an amount of two-way traffic using only one-way connection information.

15 Claims, 4 Drawing Sheets
FIG. 1

INTERNET

11 TRAFFIC MIRRORING MEANS

12 TRAFFIC ANALYSIS DEVICE

13 INTERNET USER
### FIG. 2

<table>
<thead>
<tr>
<th>Field</th>
<th>Bits</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>0</td>
</tr>
<tr>
<td>Header Length</td>
<td>4</td>
</tr>
<tr>
<td>Type of Service</td>
<td>8</td>
</tr>
<tr>
<td>Total Length</td>
<td>16</td>
</tr>
<tr>
<td>Identification</td>
<td>16</td>
</tr>
<tr>
<td>Flag</td>
<td>2</td>
</tr>
<tr>
<td>Fragment Offset</td>
<td>14</td>
</tr>
<tr>
<td>Time to Live</td>
<td>8</td>
</tr>
<tr>
<td>Protocol</td>
<td>8</td>
</tr>
<tr>
<td>Header Checksum</td>
<td>16</td>
</tr>
<tr>
<td>Source IP</td>
<td>32</td>
</tr>
<tr>
<td>Destination IP</td>
<td>32</td>
</tr>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>16-BIT SOURCE PORT NUMBER</td>
<td>16-bit source port number</td>
</tr>
<tr>
<td>32-BIT SOURCE PORT NUMBER</td>
<td>32-bit source port number</td>
</tr>
<tr>
<td>32-BIT ACKNOWLEDGEMENT NUMBER</td>
<td>32-bit acknowledgement number</td>
</tr>
<tr>
<td>16-BIT WINDOW SIZES</td>
<td>16-bit window sizes</td>
</tr>
<tr>
<td>16-BIT URGENT POINTER</td>
<td>16-bit urgent pointer</td>
</tr>
<tr>
<td>4TH BIT HEADER LENGTH</td>
<td>Reserved (6 bits)</td>
</tr>
<tr>
<td>16-BIT TCP CHECKSUM</td>
<td></td>
</tr>
</tbody>
</table>

**FIG. 3**

- Bit positions from 0 to 31.
FIG. 4

<table>
<thead>
<tr>
<th>SESSION VALUE (SOURCE IP, DESTINATION IP, SOURCE PORT, DESTINATION PORT)</th>
<th>INITIAL VALUE</th>
<th>FINAL VALUE</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>SEQUENCE</td>
<td>ACKNOWLEDGEMENT</td>
</tr>
<tr>
<td>100.100.100.100 200.200.200.200 80 3689</td>
<td>30000</td>
<td>60000</td>
</tr>
<tr>
<td>100.100.100.101 200.200.200.200 80 3609</td>
<td>30000</td>
<td>60000</td>
</tr>
<tr>
<td>100.100.100.102 200.200.200.200 80 3699</td>
<td>30000</td>
<td>60000</td>
</tr>
</tbody>
</table>

FIG. 5

START

MONITOR PACKET

EXTRACT SESSION VALUE FROM PACKET (SOURCE IP, DESTINATION IP, SOURCE PORT, DESTINATION PORT)

NEW SESSION VALUE?

YES

STORE NEW SESSION VALUE IN SESSION INFORMATION STORAGE TABLE

EXTRACT SEQUENCE NUMBER & ACKNOWLEDGEMENT NUMBER OF CORRESPONDING PACKET

SET SEQUENCE NUMBER & ACKNOWLEDGEMENT NUMBER TO BE USED AS INITIAL VALUE

NO

SEARCH SESSION INFORMATION STORAGE TABLE FOR PREDETERMINED SESSION VALUE

EXTRACT SEQUENCE NUMBER & ACKNOWLEDGEMENT NUMBER OF CORRESPONDING PACKET

STORE SEQUENCE NUMBER & ACKNOWLEDGEMENT NUMBER TO BE USED AS FINAL VALUE OF PREVIOUSLY STORED SESSION INFORMATION
SESSION-BASED TRAFFIC ANALYSIS SYSTEM

TECHNICAL FIELD

The present invention relates to a broadband traffic analysis system.

BACKGROUND ART

In recent times, the Internet may be easily used by anyone due to a drastic development and propagation of Internet technology. Accordingly, a number of Internet users is rapidly increasing, and methods for connecting to the Internet and usage patterns of the Internet have become complex and diversified. In addition, a broadband network for providing the Internet is complicated, and an Internet usage pattern is also diversified. Thus, a professional traffic analysis system is required to manage and operate a traffic network as an amount of traffic usage significantly increases due to the rapid increase and the drastic propagation of Internet users.

Here, the traffic analysis system refers to a system for analyzing a statistical amount of traffic, a current state of an Internet connection, a number of transmission control protocol (TCP) connection sessions, and a traffic usage for each service to analyze an increasing amount of traffic in the broadband network, and to analyze a factor causing interference against the network.

However, hundreds or thousands of high-cost and high-capacity traffic analysis systems are required to professionally analyze an entirety of upstream traffic and downstream traffic in the broadband network through segmentation. Accordingly, not only construction costs but also high costs for maintaining and repairing are incurred as a traffic rate increases. Thus, introducing a system for analyzing an entirety of the upstream traffic and the downstream traffic in the broadband network is difficult, in terms of costs and maintenance.

To solve the aforementioned issue, a traffic sample analysis method installed in a partial section of the broadband network to analyze traffic is currently adopted as a method for analyzing rapidly increasing high-capacity traffic of the broadband network. The traffic sample analysis method may eliminate the above-described issues in terms of costs and maintenance, which may result from using a plurality of analytical systems. However, traffic analysis is possible using only an extracted traffic sample, in lieu of the entirety of traffic. Accordingly, a result of the analysis may differ from an actual amount of traffic analysis and as a result, numerous errors in measurement may occur.

Accordingly, to overcome issues found in conventional high-cost and high-capacity traffic analysis systems, traffic sample analysis systems, and the like, there is a need for a traffic analysis method that may construct an efficient high-capacity traffic analysis system at low costs. However, a method satisfying all the requirements has yet to be proposed.

DISCLOSURE OF INVENTION

Technical Goals

An aspect of the present invention provides a session-based traffic analysis system which may replace a plurality of high-cost and high-capacity traffic analysis systems with a low-cost and efficient traffic analysis system, and may measure a total amount of traffic by analyzing a portion of upstream traffic that occupies about 1/3 of the total traffic in a broadband network.

Another aspect of the present invention provides a session-based traffic analysis system which may accurately analyze an amount of traffic for each transmission control protocol (TCP) connection using only some one-way packets based on TCP connection-oriented characteristics, that is, connection information of data storage for each TCP connection, and may accurately analyze an amount of two-way traffic using only some one-way connection information, as an amount of TCP data transmission to be transmitted is calculated based on a sequence number of the TCP connection information, and an amount of received TCP data transmission is calculated based on an acknowledgement number of the TCP connection information.

Technical Solutions

According to an aspect of the present invention, there is provided a session-based traffic analysis system to analyze two-way traffic based on one-way traffic, with respect to broadband traffic using a transmission control protocol (TCP), the system including a traffic mirroring means to monitor the one-way traffic transmitted from a broadband network on the TCP, the one-way traffic corresponding to upstream traffic or downstream traffic, a session information extracting means to extract a sequence number and an acknowledgement number for each set of session information from the traffic monitored by the traffic mirroring means, a two-way traffic analyzing means to update an initial value and a final value for each of the sequence number and the acknowledgement number extracted by the session information extracting means, to determine an amount of traffic transmitted in a direction traffic is collected in based on the initial value and the final value of the sequence number, and to determine an amount of traffic transmitted in a direction opposite to the direction traffic is collected in based on the initial value and the final value of the acknowledgement number, and a storage medium to periodically log and store a traffic analysis result value obtained by the traffic analyzing means.

The session information extracting means may extract, from TCP header information of the traffic, sequence information to be used as a sequence number value, acknowledgement information to be used as an acknowledgement number value, and source Internet protocol (IP)/destination IP/source port/destination port values of an IP header and a TCP header to be used as a session information value.

The two-way traffic analyzing means may store a sequence number and an acknowledgement number of a session information value initially collected as initial values of the sequence number and the acknowledgement number, and may continuously store sequence numbers and acknowledgement numbers collected thereafter for the same session information value, as final values of the sequence number and the acknowledgement number.

The two-way traffic analyzing means may calculate the initial values and the final values of the sequence number and the acknowledgement number, may determine an amount of data transmitted in the direction the traffic is collected in based on an equation “final value of sequence number−initial value of sequence number”, and may determine an amount of data received in the direction opposite to the direction the
traffic is collected in based on an equation “final value of acknowledgment number-initial value of acknowledgment number”.

Advantageous Effects

According to embodiments of the present invention, the same analysis result value as a value obtained by analyzing total traffic may be induced by analyzing only a portion of upstream traffic that occupies about 1/5 of the total traffic, instead of analyzing the total traffic of a broadband network.

Accordingly, more than 1/5 of the number of traffic analysis servers required in the related art may be decreased. According to the decrease in the number of traffic analysis servers, costs for purchasing a traffic analysis server, or additional costs and range of management may be reduced. Accordingly, there may be provided a broadband network management method which is efficient in terms of time and costs.

Further, according to embodiments of the present invention, there may be provided a broadband network traffic analysis system using a low-capacity and general-purpose server capable of correcting a traffic analysis value, although a portion of TCP packets is missing while analyzing the traffic.

BRIEF DESCRIPTION OF DRAWINGS

FIG. 1 is a configuration diagram illustrating a state in which a session-based traffic analysis system according to an embodiment of the present invention is applied to a network.

FIG. 2 is a diagram illustrating a configuration of an Internet protocol (IP) header of an IP packet for extracting values of a source IP and a destination IP from among session values.

FIG. 3 is a diagram illustrating a configuration of a TCP header of an IP packet for extracting values of a source port, a destination port, a sequence number, and an acknowledgement number from among session values.

FIG. 4 illustrates a session information storage table for managing a session value, and values of a sequence number and an acknowledgement number extracted from the IP packet as an initial value and a final value.

FIG. 5 is a flowchart illustrating a session-based traffic analysis process according to an embodiment of the present invention.

BEST MODE FOR CARRYING OUT THE INVENTION

Provided is a session-based traffic analysis system to analyze two-way traffic based on one-way traffic, with respect to broadband traffic using a transmission control protocol (TCP). The system includes a traffic mirroring means to monitor the one-way traffic, more particularly, upstream traffic or downstream traffic transmitted from a broadband network to TCP. The system also includes a session information extracting means to extract a sequence number and an acknowledgement number for each session information from the traffic monitored by the traffic mirroring means. The system also includes a two-way traffic analyzing means. The two-way traffic analyzing means updates an initial value and a final value for each of the sequence number and the acknowledgement number extracted by the session information extracting means. The two-way traffic analyzing means determines an amount of traffic transmitted in a direction traffic is collected in based on the initial value and the final value of the sequence number. The two-way traffic analyzing means determines an amount of traffic transmitted in a direction opposite to the direction traffic is collected in based on the initial value and the final value of the acknowledgement number. The system also includes a storage medium to periodically log and store a traffic analysis result value obtained by the traffic analyzing means.

Mode for Carrying Out the Invention

Hereinafter, a session-based traffic analysis system according to embodiments of the present invention will be described in detail with reference to the accompanying drawings.

Here, the following description is only an example of implementation of the present invention and thus, the present invention is neither limited thereto nor restricted thereby.

FIG. 1 is a configuration diagram of a network system illustrating a state in which a corresponding system performing a session-based traffic analysis method according to an embodiment of the present invention is applied to a network.

As illustrated in FIG. 1, to analyze traffic occurring with respect to an Internet user 13, a session-based traffic analysis system according to an embodiment of the present invention includes a traffic mirroring means 11 to lead traffic into a traffic analysis device 12 using a tap, a switch device, and the like, and the traffic analysis device 12 to analyze the lead traffic based on a session.

FIG. 2 is a diagram illustrating a configuration of an Internet protocol (IP) header of a packet which is analyzed when a source IP 21 and a destination IP 22 are extracted from among session information values.

The source IP 21 of FIG. 2 indicates an IP address of a transmitter which transmits data, and the destination IP 22 indicates an IP address of a receiver which receives data.

FIG. 3 is a diagram illustrating a configuration of a transmission control protocol (TCP) header of a packet which is analyzed when information of a source port 31 and a destination port 32, and a sequence number 33 and an acknowledgement number 34 for the session-based traffic analysis are extracted from among session information values.

The source port 31 indicates a connection number of a data transmitter, and the destination port 32 indicates a connection number of a data receiver.

The sequence number 33 is a serial number which is assigned in an order when data to be transmitted through a network is divided into packets.

The acknowledgement number 34 is a serial number of received data.

Here, the sequence number is the serial number of data to be transmitted and thus, an increase in a value between an initially collected sequence number value and a finally collected sequence number value based on session information indicates an amount of data actually transmitted with respect to corresponding session information.

In addition, the acknowledgement number is the serial number of received data and thus, an increase in a value between an initially collected acknowledgement number value and a finally collected acknowledgement number value based on session information indicates an amount of data actually received with respect to corresponding session information.

FIG. 4 is a session information storage table storing an initial sequence number value, a final sequence number value, an initial acknowledgement number value, and a final acknowledgement value for each set of session information.

Using values stored in the session information storage table, an amount of data transmitted by a corresponding session is calculated based on an equation of “final value of sequence number-initial value of sequence number”, and an
amount of data received by the corresponding session is calculated based on an equation "final value of acknowledgment number-initial value of acknowledgment number".

Here, the initial sequence number value stores a sequence number value which is extracted when a minimum packet having a session value is collected.

The final sequence number value is maintained by continuously updating, to be used as the final acknowledgment number value, a sequence number value of a corresponding packet extracted when a packet having the same session value as an initial session value is collected because a packet having the initial session value is already collected.

Further, the initial acknowledgement number value stores the sequence number value extracted when a minimum packet having a session value is already collected.

The final acknowledgement number value is maintained by continuously updating, to be used as the final acknowledge- ment number value, an acknowledgement number value of a corresponding packet extracted when a packet having the same session value as the initial session value is collected because the packet having an initial session value is already collected.

FIG. 5 is a flowchart illustrating a session-based traffic analysis process.

As illustrated in FIG. 5, the session-based traffic analysis process in the broadband network according to an embodiment of the present invention generates a session value key by monitoring a packet transmitted on a network in operation SS1, and by extracting a session value, more particularly, information about a source IP, a destination IP, a source port, and a destination port included in the monitored packet in operation SS2.

Whether the generated session value is a session value present in the session information storage table or a new session value may be determined in operation SS3.

When the corresponding session value is determined to be the new session value absent in the session information storage table, the extracted new session value is stored in the session information storage table in operation SS4. A sequence number and an acknowledgement number of the corresponding packet are extracted in operation SS5. The extracted sequence number and acknowledge number are stored in the session information storage table to be used as an initial value of the stored new session value in operation SS6.

Conversely, when the corresponding session value is determined to be present in the session information storage table, the session information storage table is searched for an existing session value in operation SS7.

In operation SS8, the sequence number and the acknowledg- ment number of the corresponding packet are extracted, and the initial value and the final value of the sequence number, and the initial value and the final value of the acknowledge- ment number are stored in the session information storage table for each session value of all packets by repeatedly performing operations SS6 and SS9 for each packet being monitored.

In addition, based on session values stored in the session information storage table through the aforementioned process, a traffic analysis value, for example, a data transmission amount and a data reception amount may be calculated according to the following equations.

\[
\text{Data transmission amount} = \text{final value of acknowledgment number} - \text{initial value of acknowledgment number}
\]

As described above, although the session-based traffic analysis system in the broadband network according to embodiments of the present invention is described, the present invention is neither limited thereto nor restricted thereby.

Although an installation is described to be performed in the session-based analysis device 12 in the above-mentioned embodiment, the present invention may be configured as a system which may perform predetermined processes as described above and is independent in terms of hardware. For example, the present invention may be provided in a form of software, such as an application installed on a server side or a client side to operate in a broadband network analysis and to operate by requesting a traffic analysis.

Here, when the present invention is provided in the form of software as described above, the present invention may be provided in various forms based on necessity. For example, the present invention may be provided in a form of a record medium in which a program executing the above-mentioned predetermined processes is stored, or in a form of a download program to be downloaded and installed through the Internet.

Accordingly, the present invention is not limited to the above-described embodiments. Instead, it would be appreciated by those skilled in the art that changes may be made to these embodiments without departing from the principles and spirit of the invention, the scope of which is defined by the claims and their equivalents.

**INDUSTRY APPLICABILITY**

According to embodiments of the present invention, there may be provided a session-based traffic analysis system which may replace conventional high-cost and high-capacity traffic analysis systems and traffic sample analysis systems, and may measure a total amount of traffic by analyzing a portion of upstream traffic that occupies about 1/5 of the total traffic in a broadband network to manage an efficient high-capacity traffic analysis system at low costs.

According to other embodiments of the present invention, there may be also provided a session-based traffic analysis system which may accurately analyze an amount of traffic for each transmission control protocol (TCP) connection using only some one-way packets based on TCP connection-oriented characteristics, more particularly, connection information of data storage for each TCP connection, and may accurately analyze an amount of two-way traffic using only some one-way connection information, as an amount of TCP data transmission to be transmitted is calculated based on a sequence number of the TCP connection information, and an amount of received TCP data transmission is calculated based on an acknowledgement number of the TCP connection information.

The invention claimed is:

1. A session-based traffic analysis system to analyze two- way traffic based on one-way traffic, with respect to broad- band traffic using a transmission control protocol (TCP), the session-based traffic analysis system comprising:

   - at least one processor which implements a traffic mirror operatively coupled to a broadband network which monitors the one-way traffic transmitted from the broadband network on the TCP, the one-way traffic corresponding to either upstream traffic or downstream traffic;
at least one processor which implements a traffic analysis subsystem operatively coupled to a nontransitory storage medium and operatively coupled to the traffic mirror to receive the traffic monitored thereby, the traffic analysis subsystem:
extracts a sequence number and an acknowledgement number for each set of session information from the traffic monitored by the traffic mirror;
updates an initial value and a final value for each of the extracted sequence number and the extracted acknowledgement number;
determines an amount of traffic transmitted in a direction in which traffic is collected based on the initial value and the final value of the sequence number;
determines an amount of traffic transmitted in a direction opposite to the direction in which traffic is collected based on the initial value and the final value of the acknowledgement number; and
stores a traffic analysis result value in the nontransitory storage medium based at least in part on at least one of the determined amount of traffic transmitted in a direction in which traffic is collected or the determined amount of traffic transmitted in a direction opposite to the direction in which traffic is collected.

2. The session-based traffic analysis system of claim 1, wherein the traffic analysis subsystem extracts, from TCP header information of the traffic, sequence information to be used as a sequence number value, acknowledgement information to be used as an acknowledgement number value, and source Internet protocol (IP) address, destination IP address, and session port values of an IP header and a TCP header to be used as a session information value.

3. The session-based traffic analysis system of claim 1, wherein the traffic analysis subsystem stores a sequence number and an acknowledgement number of a session information value initially collected as initial values of the sequence number and the acknowledgement number, and continuously stores sequence numbers and acknowledgement numbers collected thereafter for the same session information value, as final values of the sequence number and the acknowledgement number.

4. The session-based traffic analysis system of claim 3, wherein the traffic analysis subsystem:
calculates the initial values and the final values of the sequence number and the acknowledgement number, determines an amount of data transmitted in the direction the traffic is collected based on an equation: “final value of sequence number−initial value of sequence number”; and

determines an amount of data received in the direction opposite to the direction the traffic is collected as the final value of acknowledgement number−initial value of acknowledgement number”.

5. A traffic analysis system, the traffic analysis system comprising:
at least one processor which implements a traffic mirror operatively coupled to a network which monitors one-way traffic on a transmission control protocol (TCP), the one-way traffic corresponding to either a first direction or a second direction, wherein traffic in the second direction is opposite to traffic in the first direction;
at least one processor which implements a traffic analysis subsystem operatively coupled to the traffic mirror to receive the traffic monitored thereby, the traffic analysis subsystem:
extracts a sequence number and an acknowledgement number for session information from the monitored one-way traffic;
determines an initial value of the sequence number and a final value of the sequence number;
determines an initial value of the acknowledgement number and a final value of the acknowledgement number;
determines an amount of traffic in the first direction based on a difference between the initial value of the sequence number and the final value of the sequence number; and
determines an amount of traffic in the second direction based on a difference between the initial value of the acknowledgement number and the final value of the acknowledgement number.

6. The traffic analysis system of claim 5, wherein the traffic analysis subsystem:
extracts the sequence number from a TCP header of the one-way traffic;
extracts the acknowledgement number from the TCP header of the one-way traffic; and
obtains the session information from a source Internet Protocol (IP) address, a destination IP address, a source port, and a destination port of the TCP header of the one-way traffic.

7. The traffic analysis system of claim 5, wherein the traffic analysis subsystem:
determines, to be the initial value of the sequence number, a sequence number initially collected for the session information; and
determines, to be the initial value of the acknowledgement number, an acknowledgement number initially collected for the session information.

8. The traffic analysis system of claim 7, wherein the traffic analysis subsystem:
updates, to be the final value of the sequence number, a sequence number collected subsequently for the session information; and

determines, to be the final value of the acknowledgement number, an acknowledgement number collected subsequently for the session information.

9. The traffic analysis system of claim 5, further comprising:
a nontransitory storage unit for periodically logging and storing a traffic analysis result.

10. The traffic analysis system of claim 5, wherein traffic in the second direction is downstream traffic when traffic in the first direction is upstream traffic, and traffic in the second direction is upstream traffic when traffic in the first direction is downstream traffic.

11. A traffic analysis method, the traffic analysis method comprising:
monitoring, by a processor-based traffic mirror, one-way traffic on a transmission control protocol (TCP), the one-way traffic corresponding to either traffic in a first direction or traffic in a second direction;
extracting, by a processor-based traffic analysis subsystem, a sequence number and an acknowledgement number for session information from the monitored one-way traffic;

determining, by the processor-based traffic analysis subsystem, an initial value of the sequence number and a final value of the sequence number; and
determining, by the processor-based traffic analysis subsystem, an initial value of the acknowledgement number and a final value of the acknowledgement number,
determining, by the processor-based traffic analysis sub-
system, an amount of traffic in the first direction based
on the initial value of the sequence number and the final
value of the sequence number;

determining, by the processor-based traffic analysis sub-
system, an amount of traffic in the second direction
based on the initial value of the acknowledgement num-
ber and the final value of the acknowledgement number,
wherein traffic in the second direction is opposite to traffic
in the first direction.

12. The traffic analysis method of claim 11, wherein the
extraction of the sequence number and the acknowledgement
number comprises:

extracting the sequence number from a TCP header of the
one-way traffic;

extracting the acknowledgement number from the TCP
header of the one-way traffic; and

obtaining the session information from a source Internet
Protocol (IP) address, a destination IP address, a source
port, and a destination port of the TCP header of the
one-way traffic.

13. The traffic analysis method of claim 11, wherein the
determination of the sequence number and the acknowledge-
ment number comprises:

determining, to be the initial value of the sequence number,
a sequence number initially collected for the session
information, and

determining, to be the initial value of the acknowledg-
ment number, an acknowledgement number initially
collected for the session information.

14. The traffic analysis method of claim 13, wherein the
determination of the sequence number and the acknowledgement
number further comprises:

updating, to be the final value of the sequence number, a
sequence number collected subsequently for the session
information as, and

updating, to be the final value of the acknowledgement
number, an acknowledgement number collected subse-
quently for the session information.

15. The traffic analysis method of claim 11, wherein the
determination of an amount of traffic in the first direction
based on the initial value of the sequence number and the
final value of the sequence number comprises:

determining an amount of traffic in the first direction based
on a difference between the initial value of the sequence
number and the final value of the sequence number, and

the determination of an amount of traffic in a second direction
based on the initial value of the acknowledgement num-
ber and the final value of the acknowledgement number

comprises:

determining an amount of traffic in a second direction
based on a difference between the initial value of the
acknowledgement number and the final value of the
acknowledgement number.