

The Real-time Session Inspection Method using Heartbeat Signal

Jong Beom Kim*, Hyeon Yang*, Kyeong Ho Park**, Si Young Lee**, Seong Gon Choi*

*Broadband Network Lab., Chungbuk National University, Korea

**Xabyss Inc., Korea

dragonslash@cbnu.ac.kr, adieu@cbnu.ac.kr, khpark@xabyss.com*,
edward.lee70@xabyss.com*, choisg@cbnu.ac.kr

Abstract— In this paper, we present how to store the session information from the Heartbeat signal, which is generated at regular intervals during the network session, in real packet analysis tools. Since the existing session information retrieval method checks the session information at the end of the session, information cannot be confirmed in the case of an active session. To verify the information of the active session, this paper utilizes the heartbeat signal generated by the session every certain period. By analyzing active session information, it is possible to analyze information about flows and packets in a session in real time.

Keywords— Networking, Packet Inspection, Heartbeat Signal, Active Session

I. INTRODUCTION

Today we are called the information age, and we are living in an increasingly heavy internet environment. In a growing network environment, many packets are transmitted and communicated every day [1].

As the network grows, security threats through the network environment are also increasing. Recently, network-based attacks such as Distributed Denial of Service (DDoS) attacks have been occurring frequently, and these attacks have caused severe damage to individuals and companies, and even to the country [2].

As the damage caused by network-based attacks has increased, studies have been actively conducted to prevent or defend against such attacks. Now, many security tools such as network packet analyzers and intrusion detection systems have appeared [3], [4].

The network packet analyzer, which is one of the widely used security systems, checks the flow in the session to check whether there is a problem in the packet inside the flow. In the present packet analysis process, a method of inspecting an internal packet after a network session is completely terminated is used. However, since this method cannot inquire information of an active session, it cannot check a problem of a packet received in real time [5].

To overcome this problem, this paper used a method called a Heartbeat which periodically generated by an active session. The Heartbeat signal is a packet signal generated periodically by the session to indicate that the session is alive in communication between the transmitting side and the receiving side [6].

We analyze active session information and internal packets by applying this method to real packet analyzer. The packet analyzer analyzes the packets transmitted and received in the network and stores and classifies the information through session creation and termination. It receives the heartbeat signal from the packet analyzer and extracts session information from the information. By doing so, it implements the function of analyzing the information of the active session and confirms the packets transmitted through the flows and flows in the active session.

In Chapter 2, we present related papers on packet analysis and heartbeat signal, which is the basis of the technology proposed in this paper. Chapter 3 describes the description of the technology implemented in this paper. Chapter 4 presents the system environment and technology implementation results for the technology implementation. Chapter 5 concludes the paper.

II. RELATED WORKS

This clause describes the packet analysis method using session information analysis and the heartbeat signal among the technologies that are the basis of the active session information inspection method using the proposed technology Heartbeat signal.

A. About Threat from Active Session

For packet analysis, it is necessary to analyze the session information. Packets are passed through the flow, and flows with the same 5-tuple are bundled into a single session. Therefore, analyzing session information is essential for flow and packet analysis.

A session is largely divided into a terminated state and an active state. A session is created at the beginning of a communication and is terminated after all the packets have been delivered. The state where packets are all delivered is called the end state, and the session in the state where the packet is being delivered is called the active state [7].

The process of fetching session information from the current packet analyzer is performed through a start signal generated at the beginning of the session and a termination signal generated at the end of the session. The session information in the terminated state can be analyzed because the packet analyzer already holds the start signal and the end

signal information of the session. On the other hand, a session in the active state cannot be acquired because the session information has not yet been terminated, and thus the termination signal cannot be analyzed.

B. About Heartbeat Signal

The Heartbeat signal is a short signal that is periodically generated to ensure the connectivity of the session configured in a communication process of the sending and receiving sides. Through the Heartbeat signal, the receiver can confirm that the session has not terminated and that the packet is still being transmitted.

Heartbeat has been proposed to guarantee session connectivity in a computer system. The heartbeat signal transmits a simple inquiry to the receiver and confirms that the session with the receiver is connected through the ACK sent by the receiver [8].

The heartbeat signal transmits the information including the information of the receiving side and the transmitting side, that is, the packet including the 5-tuple when transmitting a simple inquiry. This 5-tuple contains the same information as the 5-tuple of the ongoing session.

III. SESSION INSPECTION METHOD USING HEARTBEAT

This clause shows the method used to store the heartbeat signal and the method to retrieve session information through stored signals. The packet analyzer retrieves information about the session by retrieving the start and end signals and analyzes the flows and packets in the session. Since the current packet analyzer to search the session in this way does not get the termination signal of the session until the session is completely shut down, that is information on the state of the active session cannot be analyzed.

To solve this problem, we used the method of obtaining information of active session by using Heartbeat signal. The heartbeat signal is a kind of signal that is used in the network communication process, and it is a short packet to be exchanged to guarantee session connectivity.

A. Heartbeat signal

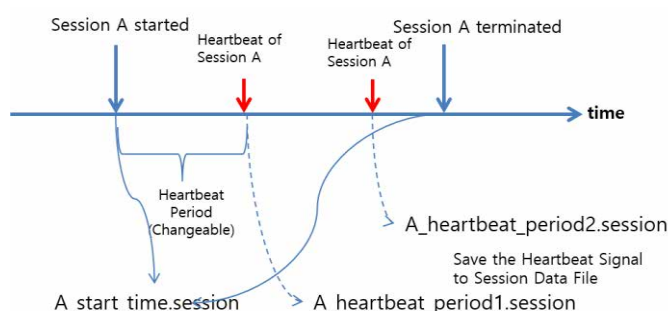


Figure 1. Heartbeat signal generation

An existing method for retrieving session information is to store a start signal generated when a session is created and a termination signal generated when a session ends.

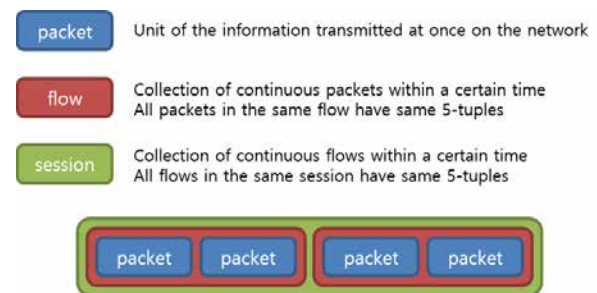


Figure 2. Structure of typical session including flows and packets

As shown in Figure 1, the heartbeat signal is generated at regular intervals defined by the Heartbeat Timer until the session is created and terminated. If the Heartbeat Timer is shortened, the Heartbeat signal is generated more frequently.

If you send a Heartbeat query packet every cycle set in the Heartbeat Timer, sending the answer to the query is the main idea of the Heartbeat signal.

The sender and receiver communicating through the session use the heartbeat signal to confirm that the session is alive.

The heartbeat signal generated by the session also has the characteristics of the packet because it is transmitted through the packets in the session. Referring to Figure 2, which shows the structure of the session, flows, and packets in the same session have the same 5-tuple.

In a typical communication, packets with the same 5-tuple are in the same flow, session. With this feature, the 5-tuple of the Heartbeat signal can acquire the 5-tuple of the whole session and store the session information.

The generated heartbeat signals are stored in the heartbeat records of each session. By storing the signals of the same session together, it is possible to efficiently store the information generated from the same session when inquiring the session information.

The size of the Heartbeat record is determined by the time the session is maintained. Heartbeat records may not be generated if the session is held for a sufficiently short period of time. On the other hand, if the duration of the session is longer, the size of the Heartbeat record also increases.

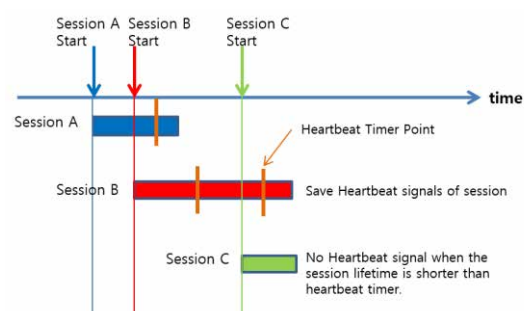


Figure 3. Saving Heartbeat signals in various types of sessions

The Heartbeat Timer is used to determine the size of the Heartbeat record and is determined as shown in Figure 3. Since the session generates a heartbeat signal every cycle set by the heartbeat timer, if the session's lifetime is shorter than

the set heartbeat timer, the heartbeat signal is not generated and the heartbeat record is not generated.

In conclusion, to utilize the heartbeat signal for session analysis, the heartbeat signal is generated every period by applying the heartbeat timer to the session, and the generated heartbeat signal is stored in the heartbeat record and used for packet analysis.

B. Session Searching Method

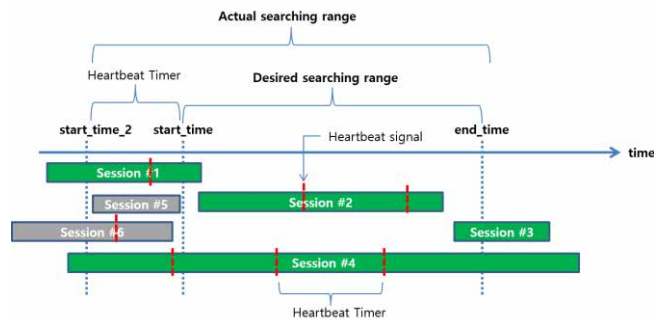


Figure 4. Virtual environment for session retrieval

To retrieve the session information through the heartbeat signal, a method of searching through the heartbeat record is required in addition to a method of searching for the session information of the existing starting point and ending point. In this paper, we define a search algorithm for retrieving session information through the Heartbeat record, as shown in Figure 4.

Figure 4 shows the virtual environment for session retrieval. There are six examples of sessions with different characteristics and specific time ranges to be searched by the user.

The specific time range determined by the user for the session search is determined by *start_time* and *end_time*. *start_time* is the time to start the search, and *end_time* is the time to end the search. The user retrieves session information existing from *start_time* to *end_time*. Among the search target sessions, some end sessions exist before the *end_time* and the end time information of the session exists, and some sessions exist in the active state because they do not end within the *end_time*.

To retrieve the session information, the retrieval result is obtained through the following five steps.

1) Find Ended Session: In this step, a session in which end time information exists, that is, an end session, is searched among the session information in the range. In the example, session #2, session #3, and session #5, which are ending sessions, are to be searched. Session #5 is excluded from the search result because it is not included in the time range. In other words, Session #2 and Session #3 become search results, and the search results are stored in *finished_session_list*.

2) Find Heartbeat Record: In this step, the session in which Heartbeat information exists is searched. A short session in which a Heartbeat record is retrieved and no Heartbeat signal is generated is not retrieved at this stage. In the example, Session #1, Session #2,

Session #4, and Session #6 are retrieved. The search results are stored in the *heartbeat_session_list*.

3) Remove Duplicates: In this step, duplicate results are removed from the results retrieved in steps 1 and 2. In the *finished_session_list* created in step 1, information of sessions 2 and 3 is stored. In the *heartbeat_session_list* generated in step 2, session #1, session #2, session #4 and session #6 are stored. Session #2 also exists in *finished_session_list* and exists in *heartbeat_session_list*. Therefore, at this stage, duplication of session #2 is removed.

4) Start time and end time check: In this step, session information having both the session start time and the session end time out of the search range is searched and removed from the searched session information. In Session #1, Session #2, Session #3, Session #4, and Session #6, Session #6 is removed from the search results because Session #6 is not in scope.

5) Print Result: In this process, the search results are output so that they can be utilized in the packet analysis tool. As a result, the final result in the example shown in Fig. 4 is Session #1, Session #2, Session #3, and Session #4, with the session #2 and session #6 removed from *finished_session_list* and *heartbeat_session_list*, and the packet analysis tool displays information about the four sessions do.

IV. IMPLEMENTATION RESULT

시작 시각	끝 시각	프로토콜	출발지 IP:포트	도착지 IP:포트	크기 (byte)
10-17 10:42:33.657	10-17 10:42:33.657	UDP	10.189.0.100:60742	203.248.252.2:53	79
10-17 10:42:33.672	10-17 10:42:33.673	UDP	10.189.0.64:17500	10.255.255.255:17500	440
10-17 10:42:33.657	10-17 10:42:33.657	UDP	203.248.252.2:53	10.189.0.100:60742	495
10-17 10:42:33.643	10-17 10:42:33.648	TCP	10.189.0.49:27050	58.231.141.11:12005	316
10-17 10:42:33.648	10-17 10:42:33.651	TCP	58.231.141.11:12005	10.189.0.49:27050	344
10-17 10:42:33.672	10-17 10:42:33.672	UDP	10.189.0.64:17500	255.255.255.255:17500	880
10-17 10:42:33.710	10-17 10:42:33.710	UDP	10.189.0.83:42435	142.54.205.4:23032	148
10-17 10:42:33.727	10-17 10:42:33.727	UDP	10.189.0.83:42435	67.151.179.73:23466	148
10-17 10:42:33.712	10-17 10:42:33.712	UDP	10.189.0.83:42435	36.4.82.97:38017	148
10-17 10:42:33.710	10-17 10:42:33.710	UDP	10.189.0.83:42435	206.45.178.105:48842	148
10-17 10:42:33.729	10-17 10:42:33.729	UDP	36.4.82.97:38017	10.189.0.83:42435	363

Figure 5. The entire session list

This clause implemented the Heartbeat Timer setting and the session information retrieval method including the Heartbeat record so that the Heartbeat signal can be utilized in the actual packet analysis tool.

This paper implemented Heartbeat Timer so that active session generates heartbeat signal at every certain time, and generated Heartbeat signal is configured to generate Heartbeat record for each session.

The implementation of the technology uses a packet analysis tool that operates in a real communication environment and implements the session retrieval method presented in Chapter 3 in an environment where a session is created and destroyed and an active session exists.

To confirm that the implemented method works, we experimented based on the sessions occurring in the actual network environment shown in Figure 5. It is determined whether a specific time range is determined among the plurality of sessions, and information of the active session can be retrieved by searching session information within the corresponding range.

시작 시간	종료 시간	프로토콜	출발지 IP/포트	도착지 IP/포트	크기 (byte)
10-17 10:42:33.657	10-17 10:42:33.657	UDP	10.189.0.100:60742	203.248.252.2:53	79
10-17 10:42:33.672	10-17 10:42:33.673	UDP	10.189.0.64:17500	10.255.255.255:17500	440
10-17 10:42:33.657	10-17 10:42:33.657	UDP	203.248.252.2:53	10.189.0.100:60742	495
10-17 10:42:33.643	10-17 10:42:33.648	TCP	10.189.0.49:27050	58.231.141.11:12005	316
10-17 10:42:33.648	10-17 10:42:33.651	TCP	58.231.141.11:12005	10.189.0.49:27050	344
10-17 10:42:33.672	10-17 10:42:33.672	UDP	10.189.0.64:17500	255.255.255.255:17500	880

Figure 6. Active state session appears in the search results

Figure 5 shows the entire session being searched. Among these sessions, a time range is set and a session search operation is performed to search for a session within a specific time range.

We set the time range to include at least one active session in the search range and retrieve the session information. Figure 6 shows that the active session appears in the search results.

Through the session information obtained from the search result, information inside the session can be analyzed. We can see the list of flows in the active session as shown in Figure 7.

Figure 8 shows the information of the packets in the flow shown in Figure 7. When a specific packet is selected from the searched packet list, the corresponding packet data can be confirmed.

As can be seen in Figure 6 ~ 8, the active session can be searched through the heartbeat signal detection method and the flow and packet information in the session can be analyzed through the retrieved active session information.

구분	시작 시간	종료 시간	프로토콜	출발지 IP/포트	도착지 IP/포트	크기 (byte)
대용세션	10-17 10:42:33.643	10-17 10:42:33.648	TCP	10.189.0.49:27050	58.231.141.11:12005	316
선택세션	10-17 10:42:33.648	10-17 10:42:33.651	TCP	58.231.141.11:12005	10.189.0.49:27050	344

Figure 7. The list of flows in the active session

패킷	타임스탬프	크기 (byte)
1	10-17 10:42:33.648126	66
2	10-17 10:42:33.648131	158
3	10-17 10:42:33.648134	60
4	10-17 10:42:33.651277	60

패킷 헤더

```

08 60 00 ca da 59 00 26 66 22 ce 01 08 00 43
00 .Y.6 E....E.
00 28 54 00 40 00 72 06 e1 ef 3a e7 8d 0a bd .
(T.8.x. .i.....
00 31 2e e5 69 aa 6e 09 8c 8e 5f 7e 19 7a 50
10 .i..i.n. .-..xP.
01 00 ef d4 00 00 00 00 00 00 00 00 a4 00
  
```

Figure 8. The information of the packets in the flow

V. CONCLUSIONS

In this paper, we use the heartbeat signal generated by the active session at regular intervals for session search. To solve the disadvantage of the existing packet analysis technique which can analyze only the information of the completely terminated session, a heartbeat signal which is generated automatically at a certain period of the session is also used for acquiring the session information.

By implementing the session information retrieval method using the Heartbeat signal in the packet analyzer for checking the actual network packets, it was possible to retrieve the active session and analyze the packet.

By allowing the active session to be searched for network packet analysis, a faster and more efficient packet analysis algorithm can be created by analyzing the packets constituting the active session before the session is completely terminated.

ACKNOWLEDGMENT

This work was supported by the National Research Foundation of Korea(NRF) grant funded by the Korea government(M SIP) (No. NRF-2015R1A2A2A03004152). This work was supported by "Human Resources Program in Energy Technology" of the Korea Institute of Energy Technology Evaluation and Planning (KETEP), granted financial resource from the Ministry of Trade, Industry & Energy, Republic of Korea. (No. 20164030201330).

*corresponding author is S.G. Choi (choisg@cgnu.ac.kr)

REFERENCES

- [1] Cisco, "Cisco® Visual Networking Index Forecast and Service Adoption for 2014 to 2019", CISCO, 2014.
- [2] D. H. Noh, D. Y. You, and B. K. An, "A Solution Method for DDoS Attack using CDN Technology", *The Journal of the Institute of Internet, Broadcasting and Communication*, vol. 9, pp. 91-96, 2009.
- [3] Wei Yen, Ming-Fang Lee, "Defending Application DDoS with Constant Random Request Attacks", *Communications 2005 Asia-Pacific Conference* on, pp. 620-624, 2005.
- [4] Archana S. Pimpalkar, A. R. Bhagat Patil, "Detection and defense mechanisms against DDoS attacks: A review", *Innovations in Information Embedded and Communication Systems(ICIECS) 2015 International Conference* on, pp. 1-6, 2015.

- [5] Erik Hjelmvik, Passive Network Security Analysis with NetworkMiner, Available: <http://www.forensicfocus.com/>
- [6] Definition of Heartbeat, The pcmag Encyclopedia. Available: <http://pcmag.com>
- [7] RFC 4271: A Border Gateway Protocol 4(BGP-4).
- [8] Aguilera Marcos Kawazoe, Chen Wei, Toueg Sam, "Heartbeat: A Timeout-Free Failure Detector for Quiescent Reliable Communication", *Distributed Algorithms. Springer Berlin Heidelberg*, Mar. 4. 2015.



Jong Beom Kim received B.S. degree in the College of Electrical & Computer Engineering, Chungbuk National University, Korea in 2017. He is currently a M.S. candidate in School of Electrical & Computer Engineering, Chungbuk National University. His research interest is network programming.



Hyeon Yang received B.S. and M.S. degree in the College of Electrical and Computer Engineering, Chungbuk National University, Korea in 2011 and 2012 respectively. He is currently a Ph.D. candidate in School of Electrical & Computer Engineering, Chungbuk National University. His research interests include smart grid and network security.



Kyeong Ho Park received B.S. degree from Kyeongbuk National University in 2000 and M.S. degree from Korea Polytechnic University in 2013. He had been research and develop in Samsung Electronic's research center. Since 2015, He has been developing the network security device in Xabyss Inc.



Si Young Lee received B.S., M.S., Ph.D. degree from Kyeongbuk National University in 1995, 1997, and 2000 respectively. He has been research director and CTO for a few venture company since 2000, and CEO in Xabyss Inc. since 2014. His research interest is software-defined network device (SDND).



Seong Gon Choi received B.S. degree in Electronics Engineering from Kyeongbuk National University in 1990, and M.S. and Ph.D. degree from KAIST, Korea in 1999 and 2004, respectively. He is currently a professor in the College of Electrical & Computer Engineering, Chungbuk National University. His research interests include smart grid, IoT, mobile communication, high-speed network architecture and protocol.