Traffic Detection Method for VoIP Applications using Flow Data

R P Joshi, Ashis Saklani, Rajendra Singh Shahi

[1]*Assistant Professor Kumaon Institute of Technology (BTKIT) Dwarahat, Almora, Uttarakhand*
[2]*Assistant Professor Kumaon Institute of Technology (BTKIT) Dwarahat, Almora, Uttarakhand*
[3]*Assistant Professor Kumaon Institute of Technology (BTKIT) Dwarahat, Almora, Uttarakhand*

Abstract:- Recently VoIP applications have been popular due to the wide deployment of the wired/wireless Internet. Commercial VoIP services typically employ SIP and RTP for signaling and media transport protocols. Therefore, the VoIP service is vulnerable to a lot of threats because it uses the Internet where security is not guaranteed. For example, anomaly traffic cases such as hindering call connections, maliciously canceling calls, and deteriorating quality of voices have already been known. In this paper, we propose an anomaly traffic detection method for VoIP applications based on the flow monitoring traffic measurement architecture, called IETF IPFIX. Under IPFIX, we present algorithms to detect BYE DDoS and RTP flooding anomaly trafc by defining new IPFIX templates for monitoring SIP and RTP flows.

Keywords:- IPFIX, VoIP, anomaly, detection, algorithm

I. INTRODUCTION

Voice over IP (VoIP) delivers voice communication between users through IP networks. Except Skype which uses a proprietary protocol, most of VoIP services employ Session Initation Protocol (SIP) [1] and Real-time Transport Protocol (RTP) [2] for connecting call and communicating voice between users. Thereby VoIP are exposed to several security threats. For example, anomaly trafc such as in terfering calls or degrading voice quality have been already known. Although secure protocols for SIP and RTP exist, they have not been fully implemented and deployed. Therefore, we have to devise an anomaly trafc method for the current VoIP services. In this work, we aim at proposing a flow-based VoIP anomaly trafc detection method which uses the IETF IP Flow Information eXport (IPFIX) [3] standard.

We use the flow-based trafc monitoring standard called IPFIX because it could provide flexible templates useful for monitoring various protocols. In addition, flow-based trafc monitoring architecture could be easily utilized since routers are typically eqiupped with flow monitoring functions such as Cisco Net Flow.

Among several VoIP anomaly trafc, we consider only two representative anomalies called BYE Denial of Service (DoS) and RTP flooding. Malicious attacker can generate these anomalies through snifng normal VoIP trafc in wireless network. When these anomalies are sent to proxy server or users, they cause fatal problems such as force call termination and voice quality degradation. In this paper, we propose two VoIP-related anomaly trafc detection methods against BYE DoS and RTP flooding. We use SIP header information such as Called and message type, and RTP trafc statistics such as timestamp for detecting BYE DoS anomaly traffic. For RTP flooding detection, we utilize SSRC and sequence number values of the RTP header.There are several similar studies to detect anomaly traffic using NetFlow [4]. Aurora [5], flowscan [6] and nfsen [7] focus on monitoring trafc based on Net Flow, which provide trafc trend information or statistics. Peakflow[8] and NetQoS [9] could detect anomaly trafc based on NetFlow data. However, these are not suitable for finding VoIP related attacks. Especially, in [10], it is shown that INVITE and RTP flooding attacks could be detected using Hellinger Distance. However, this may not extended to support finding various VoIP attack trafc, because it uses the packet count information.
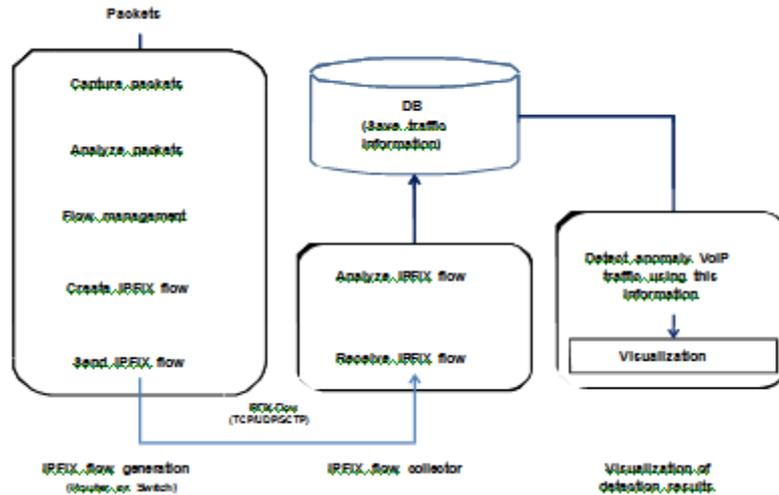
Figure 1: A flow-based anomaly traffic detection architecture

Figure 1 describes an architecture for detecting anomaVoIP trafc using the IPFIX protocol.

II.   AN ANOMALY VOIP TRAFFIC DETECTION METHOD

2.1   Traffic monitoring architecture

This architectureconsists of IPFIX flow generator, IPFIX flow collector and flow visualizer. The IPFIX flow generator at the flow monitoring servers or within routers/switches creates and exports IPFIX flows periodically while monitoring IP packets.   The routers or switches in wired networks can be performed IPFIX flows generation. In addition, we can generate IPFIX flows through monitoring IP packets at wireless access routers or access points (AP). In the generator, the IP packets are captured, then analyzed in detail. Analyzed information of the packet is maintained by flow entries.   Periodically, the generator makes the IPFIX flows from the flow entries, then send them to the IPFIX flow collector using TCP, UDP or SCTP.

We define two IPFIX templates for monitoring SIP and RTP trafc, because the default IPFIX template is not useful for delivering VoIP-related information. The defined templates carry the interesting fields of SIP and RTP headers. For in- ance, we catch Call-ID and voice transmission information from SIP headers. From RTP header, we capture sequence number and SSRC (Synchronization SouRCe). The IPFIX
 flow collector receives IPFIX flows from the IPFIX genera- tor. The collector analyzes IPFIX flows and saves the results to database. Our anomaly VoIP trafc detection algo- rithm periodically runs whether anomaly VoIP trafc exist at the saved trafc measurement information in database or not.   Then, at the visualizer, we present results of detecting anomaly VoIP trafc.

2.2   AnomalyVoIPtrafficdetectionalgorithms

For detecting anomaly VoIP trafc using the IPFIX frame work, we propose two algorithms that couldetect BYE DoS and RTP flooding anomaly trafc.

2.2.1   BYE DoS anomaly traffic detection Figure 2 shows the method for detecting BYE DoS anomaly trafc. When we observe SIP and RTP packets, we extracts session information of IP address and port number from SIP INVITE and OK messeges. Then, we investigate media traf- fic information after observing the BYE message. If RTP trafc is observed after BYE message, it could be highly considered that this RTP trafc is a flooding anomaly.

2.2.2   RTP flooding anomaly traffic detection Figure 3 depicts a RTP flooding anomaly trafc detect- ing method that utilizes SSRC and sequence number of RTP consists of IPFIX flow generator, IPFIX flow collector and flow visualizer.

The IPFIX flow generator at the flow monitoring servers or within routers/switches creates and exports IPFIX flows periodically while monitoring IP packets.   The routers or switches in wired networks can be

performed IPFIX flows generation. In addition, we can generate IPFIX flows through monitoring IP packets at wireless access routers or access points (AP). In the generator, the IP packets are captured, then analyzed in detail. Analyzed information of the packet is maintained by flow entries. Periodically, the generator makes the IPFIX flows from the flow entries, then send them to the IPFIX flow collector using TCP, UDP or SCTP. We define two IPFIX templates for monitoring SIP and RTP trafc, because the default IPFIX template is not useful for delivering VoIP-related information. The defined templates carry the interesting fields of SIP and RTP headers. For instance, we catch Call-ID and voice transmission information from SIP headers. From RTP header, we capture sequence number and SSRC (Synchronization SouRCe). The IPFIX flow collector receives IPFIX flows from the IPFIX genera- tor. The collector analyzes IPFIX flows and saves the re- sults to database. Our anomaly VoIP trafc detection algo- rithm periodically runs whether anomaly VoIP trafc exist at the saved trafc measurement information in database or not. Then, at the visualizer, we present results of detecting anomaly VoIP trafc.

2.2 Anomaly VoIPtrafficdetectionalgorithms

For detecting anomaly VoIP trafc using the IPFIX frame work, we propose two algorithms that could detect BYE DoS and RTP flooding anomaly trafc.

2.2.1 BYE DoS anomaly traffic detection Figure 2 shows the method for detecting BYE DoS anomaly trafc. When we observe SIP and RTP packets, we extracts session information of IP address and port number from SIP INVITE and OK messeges. Then, we investigate media traffic information after observing the BYE message. If RTP trafc is observed after BYE message, it could be highly considered that this RTP trafc is a flooding anomaly.

2.2.2 RTP flooding anomaly traffic detection

Figure 3 depicts a RTP flooding anomaly trafc detecting method that utilizes SSRC and sequence number of RTP header. First, we check SSRC in a flow because it should be the same with the SSRC value within the same RTP session. If SSRC has been changed at the RTP flow, it should be anomaly trafc. Second, we use sequence number information because it is possible to inject irrelevant RTP packets through snifng RTP sessions. In our method, we compare the first and last sequence numbers with the maximum and minimum sequence numbers in a RTP flow.
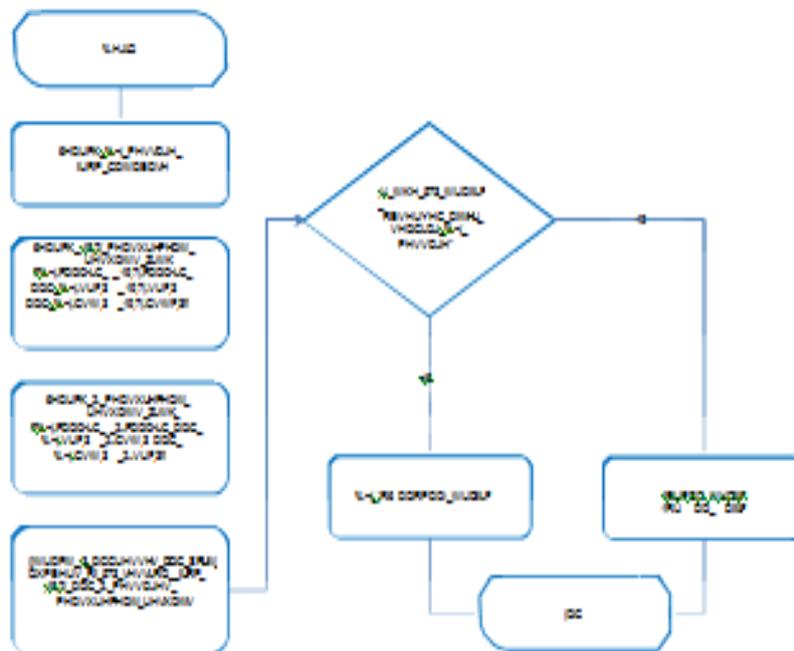

Figure 2: An algorithm to detect BYE DoS anomaly traffic
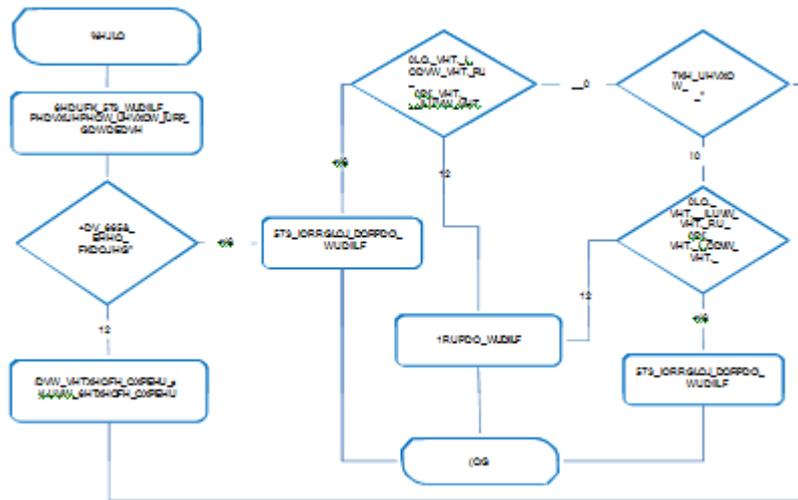
Figure 3: An algorithm to detect RTP flooding anomaly traffic

III. CONCLUSION

In this paper, we propose an anomaly VoIP trafc detection method using the IPFIX protocol. For monitoring VoIP flows, we defined two IPFIX templates which provide information of SIP and RTP header. Based on the flowmonitoring trafc measurement architecture, we present two VoIP anomaly trafc detection algorithms against SIP BYE DoS attack and RTP flooding. For the future work, we will look for VoIP anomalies influenced commercial VoIP services, then proposed these anomalies detection algorithms. Using IPFIX, [11] has already tried monitoring trafc at 1/10Gbps links with low packet loss rate. Therefore, our proposed system will be useful for monitoring VoIP trafc at these links.

REFERENCES

[1] ITU-T: Recommendation E.800: Terms and definitions related to quality of service and network performance including dependability, 2008
[2] ITU-T: Recommendation G.1010: End-user multimedia QoS categories, 2001
[3] ITU-T: Recommendation P.11: Telephone transmission quality, 1993
[4] ITU-T: Recommendation P.800.1: Mean Opinion Score (MOS) terminology, 2006