ANALYSIS AND DETECTION OF MULTIMEDIA TYPES IN RTP TRAFFIC

Martin Kmeť
Master Degree Programme (2), FIT BUT
E-mail: xkmetm01@stud.fit.vutbr.cz

Supervised by: Petr Matoušek
E-mail: matousp@fit.vutbr.cz

Abstract: This paper is focused on the detection of the audio vocoder used to code voice transferred via RTP traffic. This aspect of an RTP stream is difficult to detect but it is very important for knowing the characteristics of the stream.

Keywords: EEICT, RTP, VoIP, multimedia, network

1 ÚVOD

Protokol RTP, bol navrhnutý na prenos rôznych druhov dát s potrebou prenosu v reálnom čase. Aktuálne sa však prevažne používa pri prenose multimediálnych dát napríklad pre streaming videa, videokonferencie alebo VoIP. VoIP je v dnešnej dobe čím ďalej, tým viac obľúbené najmä vo firemných infraštruktúrach, kde nahrádza klasické telefónne linky, ktoré sú drahé pre rozširovanie a vyžadujú samostatné rozvody. Zvýšeniu kvality prenášaného hlasu a bezpečnosti však bráni obtiažna detekcia protokolu RTP. Problém s bezpečnosťou súvisí najmä s obtiažnou detekciou RTP prenosu, a teda problematickým otváraním portov na firewalle. Problému s detekciou sa venuje práca [1]. Problém so zložitejším zabezpečením kvality súvisí s detekciou kodeku neseného RTP streamom. Typ neseného kodeku totiž určuje, aký veľký dátový tok hovor vyžaduje. S pomocou tejto informácie je možné vyhradiť požadovanú časť prenosového pásma, a teda zabezpečiť kvalitu aj vo vysoko vyťaženej sieti.

Cieľom tejto práce je vyvinúť metódu automatizovanej a spoľahlivej detekcie kodeku, ktorá by doplňovala metódu detekcie RTP prenosu bez použitia informácií nesenými signalizačnými protokolmi. Táto je využiteľná pre využitie vo firewalloch, zbieraní štatistík alebo spätnej rekonštrukcie odchytenej komunikácie.

2 DETEKCIA KODEKU

2.1 MOŽNOSTI DETEKCIE KODEKU

Aplikácie komunikujúce pomocou protokolu RTP sa o použití kodeku dohodnú pomocou niektorého zo signalizačných protokolov. Bohužiaľ, tento môže ísť cez sieť inou cestou ako RTP tok prenášajúci samostatné multimediálne dáta. Kodek je pomocou signalizačného protokolu dohodnutý pred začiatkom komunikácie, a teda v prípade, že sa detekcia začala až v priebehu započatého prenosu, tieto informácie nebudú k dispozícii. Problém ale môže nastať aj v prípade preťaženia detekčného mechanizmu, v prípade vynechania tejto jedinej správy tak isto nebudú už tieto dáta dostupné.

Druhá možnosť, ktorá netrpí vyššie uvedenými problémami je založená na použití len na základe informácií dostupných so samotného protokolu RTP a dátach nim nesených. Táto možnosť umožňuje detekciu z malej vzorky odchytených dát, ktoré boli zaznamenané v ľubovolnej fáze prebiehajúcej komunikácie. Možnostiam realizácie tejto metódy sa budeme ďalej venovať.

2.2 DETEKCIA KLASIFIKÁTOROM

Táto možnosť detekcie je založená na použití štandardnej schémy klasifikátora. Možnosť tejto formy detekcie skúmali aj na Ankara University v tureckej Ankare [4]. Klasifikátor je založený na steganografickej báze. Tento klasifikátor teda neskúma špecifické opakujúce sa vzory, ale štatistiku bitového streamu ako celku. Tieto štatistiky by mali byť u jedného streamu nemenné, a teda by sa pri zmene bitratu, ani pri poprehadzovaní poradia nemali výsledky meniť. Táto metóda teda funguje aj na poškodených streamoch s poprehadzovanými paketmi, bez potreby opätovného preskladania.

Pri použití klasifikátora natrénovanom na normalizované štatistiky trénovacej množiny dát na testovaciu množinu dát, dostali výsledky potvrdzujúce vysokú úspešnosť. Jej ďalšou výhodou je, že bude fungovať aj pri poškodených častiach streamu bez zníženia presnosti. Táto metóda má však aj veľké nevýhody. Jednou z nich je potreba neurónovú sieť natrénovať pomocou veľkého množstva testovacích dát so známymi kodekmi predtým, ako ich bude schopná klasifikovať. Ďalším, väčším problémom tejto metódy je pomerne veľká výpočetná náročnosť. Oproti nasledujúcej metóde, ktorá je značne jednoduchšia, bude beh analýzy výrazne dlhší, a jej hardwarové urýchľovanie náročnejšie. Toto môže byť problém pri potrebe behu aplikácie v reálnom čase pri analýze dát prúdiacich sieťou.

2.3 DETEKCIA POMOCOU CHARAKTERISTICKÝCH ZNAKOV

Táto metóda je založená na filtrovaní jednotlivých možných kodekov na základe ich charakteristických znakov a je predmetom výskumu, ktorým sa zaoberá táto práca.

Jedným z týchto znakov je mapovanie použitého kodeku na položku `payload type` v hlavičke každého RTP paketu. Samotný použitý kodek a mapovanie jednotlivých kodekov na číslo v položke `payload type` sa síce dohaduje na začiatku komunikácie pomocou niektorého zo signalizačných protokolov, ale existuje množina staticky mapovaných kodekov, ktoré sa vždy mapujú na číslo registrované u IETF v RFC dokumentoch. Ako ukázal prieskum vykonaný v [1]. Všetky pozorované aplikácie statické mapovanie dodržiavajú, a teda môžeme predpokladať jeho správnosť a prehlásiť takto určený kodek za úspešne detekovaný. Okrem staticky mapovaných kodekov sa však používa aj dynamické mapovanie v rozsahu 96 – 127. V prípade výskytu takéhoto čísla v položke `payload type`, môže stream obsahovať ktorýkoľvek dynamicky mapovaný kodek.

Ďalšími významnými informáciami nesenými v RTP hlavičke je časové razítko uložené v položke `timestamp`. Toto musí vychádzať z reálnej hodnoty založenej na vzorkovacej frekvencii, a teda rozdiel medzi dvoma po sebe idúcimi paketmi spolu s dĺžkou dát nesených jednotlivými paketmi vytvára ďalší špecifický rys pre jednotlivé kodeky. Na prieskum týchto hodnôt bola vytvorená vzorka dát, ktorá bola odchytená z komunikácie niektorých softwarových telefónov ako aj za použitia profesionálneho sieťového testeru od firmy Ixia (viac informácií dostupných na http://www.ixiacom.com/).

V rámci práce bol vykonaný prieskum a spísaný prehľad používaných kodekov. Vzorky boli preskúmané detekčným nástrojom vytvoreným k práci [1], ktorý bol ďalej upravený a doplnený. Výsledky sú uvedené v tabuľke 1. Z týchto výsledkov je viditeľné, že pomer medzi hodnotami rozdielu časového razítka a dĺžky paketu sú u dynamicky mapovaných kodekov naozaj individuálne, a teda nám pomôžu identifikovať jednoznačne kodek a dokonca aj variantu kódeku. U staticky mapovaných kodekov nám zase táto metóda pomôže zvýšiť presnosť.

Metóda môže byť ďalej spresnená prieskumom opakujúcich sa hodnôt pri niektorých kodekoch ako napríklad Speex alebo GSM. Ďalej môže byť spresnená prieskumom hlavičiek u kodekov, ktoré ho vkladajú na začiatok dátovej časti každého paketu ako napríklad G723.1 alebo AMR, v ktorej sa nachádza aj identifikácia varianty kodeku.

Táto metóda je narozdiel od klasifikátora založená na pomerne jednoduchom rozhodovaní na základe konečného automatu, a preto bude rýchlejšia a ľahko akcelerovateľná pomocou hardvéru. Metóda je

Codec	Payload type	Δ time	Data len	Codec	Payload type	Δ time	Data len
AMR-WB	dyn	320	62	G.726-32	dyn	80/240	40/120
AMR-12k	dyn	160	33	G.726-40	dyn	80/240	50/150
GSM	3	160	33	G.729	18	160	20
G.722	9	160	160	G.729a	18	160	20
G.722.1	dyn	160	60	G.729b	18	160	20*
G.723.1-5k	4	320	20	PCMA	8	160	160
G.723.1-6k	4	240	24	PCMU	0	160	160
G.726-16	dyn	80/240	20/60	Speex16	dyn	320	52
G.726-24	dyn	80/240	30/90	Speex8	dyn	160	20

* – skrátené v prípade detekcie ticha

Tabuľka 1: Prehľad zistených, charakteristických znakov kodekov

aj jednoducho paralelizovateľná pomocou spracovania paketov vo viacerých vláknach.

3 ZÁVER

V tejto práci sú stručne popísané metódy detekcie kodekov nesených RTP streamom. Zameriava sa hlavne na porovnanie skúmanej metódy pomocou vyhodnocovania špecifických znakov jednotlivých kodekov proti metóde využívajúcej klasifikátor. Aj keď táto metóda nie je tak univerzálna ako klasifikátor, nepotrebuje rozsiahlu trénovaciu množinu dát. Je taktiež jednoduchšie implementovateľná, a teda aj rýchlejšia na spracovanie. Medzi nevýhody patrí neschopnosť spracovávať poškodené dáta, ktoré by ale cez sieť nemali byť doručené vôbec, vďaka kontrolným mechanizmom protokolov nižších vrstiev. Ďalej je to znížená presnosť v prípade výskytu kodekov s rovnakými znakmi. Toto negatívum však nie je podstatné z dôvodu pomerne nízkeho množstva reálne používaných kodekov vo VoIP. Preto môžeme túto metódu prehlásiť za lepšiu pre reálne nasadenie.

Metóda bola úspešne implementovaná v jazyku Python za použitia RTP detekčného nástroja popisovanom v [1]. Jej testovanie bolo úspešné na laboratórnych vzorkách dát, ktoré vznikli odchytom komunikácie viacerých softvérových telefónov, videokonferenčného softvéru a jednotky Tandberg. Ďalej bola využitá testovacia vzorka vytvorená sieťovým testerom Ixia. Implementácia využíva detekciu na základe informácií uvedených v tabuľke 1 a je pripravená na implementáciu spresnenia pomocou detekcie hlavičiek kodekov a opakujúcich sa vzorov.

POĎAKOVANIE

Tento príspevok vznikol za podpory projektu MV VG20102015022, Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace a projektu FIT-S-14-2299, Výzkum pokročilých metod ICT a jejich aplikace.

LITERATÚRA

[1] Kmeť, M.: Nástroj pro sledování RTP streamů. Bakalářská práce, FIT VUT v Brně, Brno, 2012.

[2] Schulzrinne, H.; Casner, S.: RTP Profile for Audio and Video Conferences with Minimal Control, RFC 3551. Technická zpráva, Júl 2003.

[3] Schulzrinne, H.; Casner, S.; Frederick, R.; aj.: RTP: A Transport Protocol for Real-Time Applications, RFC 3550. Technická zpráva, Júl 2003.

[4] Yargicoglu, A. U.; Ilk, H. G.: Speech Coder Identification Using Chaotic Features Based on Steganalyzer Models. In Communications, Žilina: Žilinská univerzita v Žiline, 2012, ISSN 1335-4205.