FAST PROCESSING OF APPLICATION-LAYER PROTOCOLS

Stanislav Bárta
Master Degree Programme (2), FIT BUT
E-mail: xbarta29@stud.fit.vutbr.cz

Supervised by: Libor Polčák
E-mail: ipolcak@fit.vutbr.cz

Abstract: This paper describes the design of the system for processing application-layer protocols in high-speed networks using the concept of Software Defined Monitoring. The proposed solution uses hardware acceleration network card performing pre-processing of network traffic based on the feedback from monitoring applications. The monitoring application modules process monitored application-layer protocols and generate reports describing main events in monitored flow. First packets of each flow are handed over to all application modules which decide how to deal with this flow. Following packets of unwanted flow are filtered in input filter. A flow is filtered in firmware of the network card if it is rejected by all of application modules.

Keywords: Lawful interception, Software Defined Monitoring, security, monitoring, high-speed networks, network traffic processing

1 ÚVOD

Trendem moderní doby je vývoj a výroba zařízení schopných připojit se k celosvětové počítačové síti internetu a komunikovat s ostatními připojenými zařízeními. S dalším rozvojem bude takovýchto zařízení přibývat. Připojení těchto zařízení k internetu má za následek výrazný nárust objemu dat přenášených sítí. Na vysokorychlostních sítích se tak přechází na technologie pracující s rychlostí 100Gb/s a v blízké budoucnosti bude docházet k dalšímu zvyšování.

Pro zabezpečení sítě a zařízení k ní připojených je s nárustem rychlosti potřeba vytvářet techniku schopnou efektivně zpracovávat velké množství dat. S aktuálně dostupnými prostředky není možné vytvořit univerzální čistě hardwarové nebo čistě softwarové řešení zvládající monitorovat aplikační protokoly na rychlostech 100Gb/s [2]. Je tedy potřeba hledat optimální řešení spolupráce softwaru s hardwarem. Tato práce se zabývá návrhem systému schopného zpracovávat aplikační protokoly ve vysokorychlostních sítích, který využívá spolupráce softwaru s hardwarem.

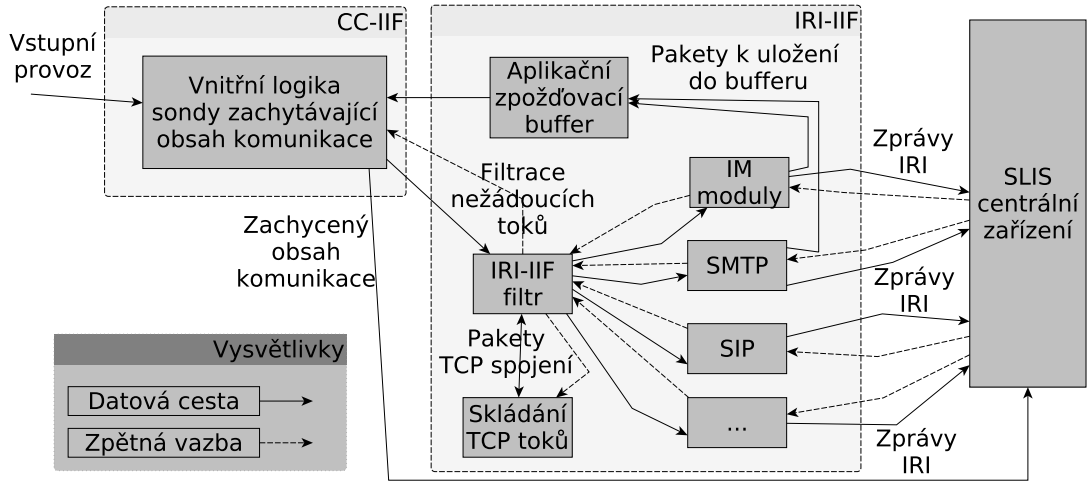
Ve vytvářeném systému je využito konceptu software defined monitoring (SDM) [2], který je možno použít k akceleraci zpracování dat. SDM vychází z některých myšlenek Software Defined Networking (SDN) navrhujících oddělení kontrolní a funkční části. V případě SDM jde o oddělení nízkoúrovňového předzpracování vstupních dat od řízení tohoto předzpracování. Samotné předzpracování je provedeno ve firmware akcelerační síťové karty a její řízení probíhá ze softwarové části systému. SDM umožňuje rozdělování paketů do softwarových kanálů, které je možno zpracovávat na různých jádrech procesoru. Současně lze zajistit předávání paketů jednoho toku vždy do stejného kanálu.

Koncept SDM je využit pro filtrování zachycených síťových dat, které je prováděno na úrovni toků. První pakety z každého toku musí být předávány do software, který rozhodne, jak s daným tokem nakládat. Samotná filtrace je prováděna ve firmware, který je konfigurován softwarovým řadičem, s kterým komunikují uživatelské aplikace. Do firmwaru jsou nastavovány blokující pravidla pouze pro dlouhotrvající toky a to na základě vnitřní heuristiky řadiče. Tento princip byl zvolen z důvodu efektivity, protože aktualizace tabulky je s každým nově přidaným pravidlem časově náročnější.

2 RYCHLÉ ZPRACOVÁNÍ APLIKAČNÍCH PROTOKOLŮ

Hlavní myšlenkou zpracování aplikačních protokolů ve vysokorychlostních sítích je včasné filtrování všech toků, které není potřeba sledovat. Tato filtrace probíhá ve firmware akcelerační síťové karty a filtrací dlouhotrvajících toků lze síťový provoz zredukovat až o přibližně 85% paketů [2]. Další nutností je pracovat s pakety tak, aby nebylo potřeba vytvářet jeho zbytečné kopie a celý proces zpracování proběhl v ideálním případě bez kopií paměti [3]. Ne vždy je však možno pracovat bez jediné kopie. Příkladem je skládání TCP toků, které se musí vypořádat se zpožděnými nebo přeházenými pakety a některé pakety tak musí být bufferovány.

Funkcionalita vytvářeného software je součástí systému pro zákonné odposlechy [1], v rámci kterého tvoří funkční blok dynamické identity uživatele (IRI-IIF [1]). Z bloku zajišťujícího zachytávání obsahu komunikace (CC-IIF [1]) jsou získávána vstupní data k dalšímu zpracování a vyhodnocené informace jsou předávány ve formě zpráv IRI [1] do centrálního zařízení systému pro zákonné odposlechy nazvaného SLIS. Umístění vytvářeného bloku v rámci systému vyobrazuje obrázek 1.



Obrázek 1: Umístění vytvářeného bloku IRI-IIF v rámci systému pro zákonné odposlechy.

CC-IIF je funkčním blokem, který zpracovává vstupní síťový provoz a je tvořen firmwarem akcelerační síťové karty a softwarovou částí, které využívá a řídí firmwarovou část. Jedná se o využití konceptu SDM. Hlavním účelem CC-IIF je odposlech obsahu komunikace na základě vystavených odposlechů. V navrženém řešení slouží také jako zdroj dat pro komponentu IRI-IIF a za účelem úspory výpočetního výkonu jsou z CC-IIF do IRI-IIF předávány již jednou zjištěné informace z nízkoúrovňového předzpracování. Jedná se o pozice začátku IP hlavičky, transportní hlavičky a aplikačních data ve zpracovávaném paketu. Dále je předávána vypočítaná hash toku pro vyhledávání v tabulkách uložených v IRI-IIF. Na základě požadavků z IRI-IIF je v CC-IIF prováděna filtrace vstupních paketů.

IRI-IIF je hlavním blokem vyvíjeným v rámci této práce, který analyzuje síťový provoz a to na úrovni aplikačních protokolů. V aplikačních protokolech se snaží vyhledat identifikátory, podle kterých je možno identifikovat komunikujícího uživatele. Blok je tvořen komponentami IRI-IIF filtr, skládání TCP toků, aplikační moduly a aplikační zpožďovací buffer.

IRI-IIF filtr slouží jako vstupní bod bloku IRI-IIF. Přijímá pakety z CC-IIF a přeposílá je aplikačním modulům, které o ně mají zájem. Pro toky, o které nemá žádný modul zájem, jsou do CC-IIF zasílána blokující pravidla, na základě kterých jsou tyto toky odfiltrovány. Pakety TCP toků jsou předávány do komponenty skládání TCP toků, která provádí jejich řazení a pakety v pořadí vrací zpět do filtru, aby mohly být předány odpovídajícím aplikačním modulům.

Skládání TCP toků řadí pakety v rámci každého toku a pakety, které jsou v pořadí vrací zpět do filtru odkud jsou přeposlány do aplikačních modulů. Pakety mimo pořadí musí být uloženy do bufferu.

Aplikační moduly parsují aplikační protokoly a vytvářejí zprávy IRI [1]. Každý modul je tvořen rychlou a pamalou částí. Rychlá část má na starosti rozhodnutí o využití toku v daném modulu a informování komponenty filtru o tom, zda má nebo nemá o daný tok zájem. Pomalá část se stará o parsování dat aplikačního protokolu a vytváření zpráv IRI [1] na základě zjištěných informací. Do pomalé části jsou předány pouze pakety z toků, které byly v rychlé části identifikovány jako toky protokolu zpracovávaného v modulu.

SLIS centrální zařízení mimo jiné přijímá zpravý IRI od aplikačních modulů a pomocí zpětné vazby je informuje, zda je nebo není vystaven odposlech na identifikátory obsažené ve zprávě IRI.

Aplikační zpožďovací buffer (ADB) slouží k uložení prvních paketů toku, dokud není daný tok ukládán v CC-IIF. Do ADB jsou uloženy pouze pakety toku, který bude odposloucháván. Zpětnou vazbou ze SLIS je oznámeno, zda je tok sledován nebo ne a na základně této informace je s pakety naloženo. Nesledované toky jsou z bufferu ihned odstraněny. Pakety sledovaného toku jsou v ADB ponechány a vyjmuty jsou ve chvíli, kdy je nakonfigurován odposlech obsahu komunikace v CC-IIF.

Výsledný návrh systému pro rychlé zpracování aplikačních protokolů počítá s využitím více procesů, kdy každý proces bude využívat jedno jádro procesoru a bude zpracovávat část toků. K rozdělování toků mezi procesy bude využito SDM firmwaru, který umí rozdělovat pakety do více softwarových kanálů. Každé jádro bude vykonávat stejnou činnost pouze nad rozdílnými daty.

3 ZÁVĚR

Zpracování paketů bude probíhat v hlavním vlákně bez nutnosti využívat mechanismů meziprocesové komunikace. Zpracování paketů v jediném vlákně zajistí redukci kopií paměti a odstraní nutnost komunikace řešící zpětnou vazbu a předávání paketů. Té bude dosaženo pomocí návratových hodnot volaných funkcí. Dále je možno s využitím konceptu SDM a filtrování všech dlouhotrvajících toků nevyužitelných při odposlechu dosáhnout výrazné redukce zpracovávaných dat a to až o přibližně 85% paketů celého síťového provozu [2]. Tuto filtraci bude provádět firmware akcelerační síťové karty a do softwarové části se dostane jen zlomek síťového provozu. Díky tomu by mělo být možno zpracovávat aplikační protokoly ve vysokorychlostích sítích.

PODĚKOVÁNÍ

Tento příspěvek vznikl za podpory grantu MV a výzkumného záměru Moderní prostředky pro boj s kybernetickou kriminalitou na Internetu nové generace: VG20102015022 a projektu Výzkum pokročilých metod ICT a jejich aplikace: FIT-S-14-2299.

REFERENCE

[1] European Telecommunications Standards Institut. *ETSI TR 102 528: Lawful Interception (LI); Interception domain Architecture for IP networks*. 2006, version 1.1.1.

[2] Kekely, L. *Hardwarová akcelerace aplikací pro monitorování a bezpečnost vysokorychlostních sítí*. Diplomová práce. Brno: FIT VUT v Brně, 2013.

[3] Mudigonda J., Vin Harrick M., Yavatkar R. *Overcoming the memory wall in packet processing: hammers or ladders?*. In: Proceedings of the 2005 ACM symposium on Architecture for networking and communications systems (ANCS '05). New York, NY, USA: ACM, 2005.