

**FACULTATEA DE AUTOMATICĂ ȘI CALCULATOARE**

**DEPARTAMENTUL CALCULATOARE**

**Realizarea unei aplicații destinate capturii și analizei**

**traficului dintr-o rețea de calculatoare**

LUCRARE DE LICENȚĂ

Absolvent:

Coordonator:

**Capitolul 2: Obiectivele Proiectului**

**2.1 Definirea temei**

Tema proiectului presupune crearea unei aplicații software care să permită capturarea și analiza traficului de rețea în timp real, furnizând statistici și informații utile pentru un administrator de rețea. Aplicația va folosi un framework pentru captarea pachetelor de rețea și va oferi opțiuni pentru filtrarea acestora, generarea de rapoarte și vizualizarea acestora într-o interfață web accesibilă de la distanță.

**Obiectivele principale ale proiectului sunt:**

* **Capturarea traficului de rețea:** Identificarea interfețelor de rețea disponibile pe dispozitivul gazdă și capturarea pachetelor de pe aceste interfețe.
* **Analiza traficului:** Procesarea pachetelor pentru identificarea protocoalelor de rețea (IPv4, IPv6, TCP, UDP, ICMP), împărțirea traficului pe fluxuri și generarea de statistici.
* **Stocarea datelor:** Salvarea informațiilor despre pachetele capturate (header-e, metadate) într-un format accesibil (CSV, XML, PCAP) pentru analiză ulterioară.
* **Vizualizarea datelor:** Oferirea unei interfețe grafice web pentru vizualizarea în timp real a statisticilor și compararea acestora cu datele istorice.

**2.2 Obiectivele specifice ale proiectului**

1. **Identificarea și selecția interfețelor de rețea:** Aplicația va trebui să permită administratorului să identifice interfețele de rețea disponibile (Ethernet, Wi-Fi, etc.) și să selecteze cele pe care dorește să le monitorizeze.
   * **Tehnici de implementare:** Utilizarea librăriei libpcap (sau JPcap pentru Java) pentru identificarea interfețelor de rețea.
   * **Provocări tehnice:** Gestionarea permisiunilor de acces la interfețele de rețea (administrator/root), gestionarea eroilor și a întreruperilor de conexiune.
2. **Captura și analiza pachetelor:** Sistemul va capta pachetele de pe interfețele selectate și le va analiza pentru a extrage informații utile.
   * **Tehnici de implementare:** Analiza pachetelor folosind protocoale de bază (TCP, UDP, ICMP, IPv4, IPv6).
   * **Provocări tehnice:** Identificarea fluxurilor de trafic (fiecare flux fiind definit prin IP sursă, port sursă, IP destinație, port destinație și protocol) și analiza eficientă a unui trafic de rețea voluminos.
3. **Stocarea datelor:** Pachetele capturate vor fi salvate în fișiere pentru o analiză ulterioară. Datele vor include metadatele fiecărui pachet (header-e).
   * **Tehnici de implementare:** Utilizarea formatului PCAP (format standardizat pentru capturarea pachetelor) sau CSV/XML pentru stocarea datelor.
   * **Provocări tehnice:** Crearea unei structuri eficiente pentru stocarea și recuperarea datelor din fișiere mari.
4. **Generarea și vizualizarea statisticilor:** În timp real, aplicația va crea statistici despre trafic, fluxuri, protocoale, utilizare a rețelei și altele.
   * **Tehnici de implementare:** Utilizarea unui server web (de exemplu, Flask pentru Python) pentru a transmite statistici într-o interfață web.
   * **Provocări tehnice:** Gestionarea volumului mare de date și furnizarea de informații în timp real cu o latență minimă.

**2.3 Cerințele funcționale**

1. **Identificarea interfețelor de rețea disponibile pe dispozitivul gazdă.**
   * Implementarea unui mecanism de detectare a interfețelor de rețea disponibile.
   * Permisiuni adecvate pentru accesul la interfețele de rețea.
2. **Capturarea pachetelor de pe interfețele de rețea.**
   * Filtrarea traficului pe baza protocoalelor de interes (IPv4, IPv6, TCP, UDP, ICMP).
   * Suport pentru capturarea pe mai multe interfețe simultan.
3. **Analizarea pachetelor capturate.**
   * Analiza headere-lor pentru extragerea informațiilor relevante: adrese IP, porturi, protocoale.
   * Calcularea statisticilor pe fluxuri de trafic.
4. **Filtrarea și clasificarea traficului.**
   * Posibilitatea de a filtra pachetele pe baza unor criterii precum IP sursă/destinație, porturi sursă/destinație, tipul de trafic.
5. **Stocarea datelor.**
   * Salvarea în fișiere PCAP pentru analiza ulterioară.
   * Salvarea metadatelor pachetelor în formate ușor accesibile (CSV/XML).
6. **Vizualizarea de la distanță.**
   * Crearea unei interfețe web care să permită accesul la statistici și informații în timp real.

**2.4 Cerințele non-funcționale**

* **Performanța:** Aplicația trebuie să proceseze și să salveze datele într-un timp scurt, cu un impact minim asupra performanței rețelei.
* **Scalabilitate:** Sistemul trebuie să suporte monitorizarea mai multor interfețe de rețea și să poată scala pe măsură ce volumul de trafic crește.
* **Flexibilitate:** Aplicația trebuie să permită extinderea cu noi protocoale sau funcționalități.
* **Robustete:** Sistemul trebuie să gestioneze erorile și excepțiile, inclusiv întreruperile de rețea.
* **Persistența datelor:** Datele trebuie să fie stocate eficient și să poată fi recuperate oricând, chiar și după oprirea aplicației.

**Capitolul 3: Studiu Bibliografic**

**3.1 Introducere în capturarea și analiza traficului de rețea**

Capturarea și analiza traficului de rețea reprezintă procese fundamentale pentru gestionarea rețelelor de calculatoare, cu aplicații multiple în domenii precum securitatea cibernetică, optimizarea performanței, monitorizarea serviciilor și investigarea incidentelor. Traficul de rețea include toate datele care circulă între dispozitive conectate, iar analizarea acestuia presupune identificarea tipurilor de date, interpretarea scopului lor și evaluarea impactului lor asupra infrastructurii IT.

Începând cu anii 1990, când rețelele de calculatoare au devenit mai complexe, capturarea traficului de rețea a evoluat de la simple instrumente de diagnosticare până la platforme avansate capabile să ofere o vedere de ansamblu asupra performanței rețelei și să identifice vulnerabilități în timp real. Inițial, analiza traficului era utilizată doar pentru depanarea problemelor locale, dar creșterea utilizării internetului și apariția amenințărilor cibernetice complexe au transformat această activitate într-o necesitate pentru companiile de orice dimensiune.

Astăzi, analiza traficului de rețea se bazează pe instrumente avansate care folosesc tehnologii moderne precum inteligența artificială, procesarea în timp real și stocarea distribuită. Proiectul propus se încadrează în acest context, oferind o soluție care să răspundă cerințelor actuale de performanță și flexibilitate.

**3.2 Tipuri de protocoale monitorizate**

Întrucât traficul de rețea este format din pachete de date transmise conform unor reguli stabilite (protocoale), înțelegerea și analiza acestor protocoale sunt esențiale pentru a interpreta corect traficul capturat. Protocoalele oferă reguli standardizate pentru cum datele sunt transmise, fragmentate, reordonate și confirmate în rețea.

**IPv4 și IPv6: Protocoale pentru rutare**

1. **IPv4 (Internet Protocol version 4):**
   * Este cel mai utilizat protocol de rutare a traficului pe internet.
   * Funcționează folosind adrese IP pe 32 de biți, ceea ce limitează numărul de adrese disponibile.
   * Header-ul IPv4 include informații precum adresa IP sursă și destinație, timpul de viață al pachetului (TTL) și fragmentarea pachetelor.
   * Exemplu de utilizare: Transferul unei pagini web către utilizatorul final.
2. **IPv6 (Internet Protocol version 6):**
   * A fost introdus pentru a rezolva limitările IPv4, extinzând spațiul de adresare la 128 de biți.
   * Adaugă îmbunătățiri semnificative în ceea ce privește securitatea (IPSec) și eficiența rutării.
   * Este preferat în rețelele moderne datorită integrării sale cu IoT (Internet of Things).

**TCP și UDP: Protocoale de transport**

1. **TCP (Transmission Control Protocol):**
   * Este protocolul preferat pentru transferurile fiabile de date, precum e-mailurile, transferurile de fișiere (FTP) și navigarea pe web.
   * Mecanismul său de confirmare și retransmisie asigură că toate datele sunt livrate în mod corect.
   * Dezavantaj: Consumă mai multă lățime de bandă și introduce o latență mai mare comparativ cu UDP.
2. **UDP (User Datagram Protocol):**
   * Folosit pentru aplicații care necesită viteză mai mare și toleranță la pierderi (streaming video, jocuri online).
   * Nu oferă mecanisme de confirmare sau retransmisie, ceea ce îl face mai eficient, dar mai puțin fiabil.

**ICMP: Protocol pentru diagnosticare**

1. **ICMP (Internet Control Message Protocol):**
   * Este utilizat pentru trimiterea mesajelor de eroare și diagnosticare.
   * Exemple: Comenzile ping și traceroute folosesc ICMP pentru a măsura timpul de răspuns al unei destinații sau traseul urmat de un pachet.

**QoS și DSCP: Prioritizarea traficului**

1. **DSCP (Differentiated Services Code Point):**
   * Este un mecanism utilizat pentru a clasifica și prioritiza pachetele în funcție de importanța lor (de exemplu, pachetele audio/video pot avea prioritate față de alte tipuri de trafic).

**3.3 Tehnologii și framework-uri pentru capturarea traficului**

Capturarea pachetelor este posibilă datorită unor framework-uri care permit aplicațiilor să acceseze interfețele de rețea la nivel de kernel. Cele mai utilizate tehnologii includ:

**libpcap/WinPcap**

* Descriere: Biblioteca de bază utilizată pentru capturarea pachetelor. libpcap este disponibilă pe Unix/Linux, în timp ce WinPcap este varianta sa pentru Windows.
* Funcționalități:
  + Oferă acces la nivel scăzut la interfețele de rețea.
  + Permite capturarea pachetelor și aplicarea de filtre.
* Exemplu de utilizare: Wireshark folosește libpcap pentru capturarea traficului.

**NFQueue și Netfilter**

* Descriere: Tehnologii specifice Linux care permit manipularea pachetelor de rețea direct din kernel.
* Aplicații: Firewall-uri și sisteme de prevenire a intruziunilor.

**Apache Kafka**

* Descriere: O platformă distribuită pentru procesarea în timp real a datelor.
* Exemplu: Utilizarea Apache Kafka pentru stocarea și analiza fluxurilor mari de trafic în timp real.

**3.4 Soluții existente pentru captură și analiză**

În acest subcapitol, vom analiza câteva dintre cele mai populare soluții existente pentru capturarea și analiza traficului de rețea, incluzând atât instrumente open-source, cât și soluții comerciale. În acest caz, vom discuta despre **Wireshark**, **tcpdump**, **Zeek (Bro)**, **SolarWinds Network Performance Monitor (NPM)** și **NetworkMiner**. Acestea oferă diferite abordări în funcție de cerințele rețelelor și scopurile utilizatorilor.

**1) Wireshark**

**Descriere:** Wireshark este unul dintre cele mai populare și utilizate instrumente pentru analiza și capturarea pachetelor de rețea. Este un **tool open-source** care permite capturarea pachetelor de date de pe interfețele de rețea și analiza lor detaliată, inclusiv decodificarea protocoalelor de rețea. Wireshark este folosit de administratorii de rețea, cercetătorii în securitate și dezvoltatorii de aplicații pentru a înțelege comportamentele rețelelor și pentru a rezolva probleme de performanță sau securitate.

**Funcționalități:**

* **Capturarea live a pachetelor:** Wireshark poate captura pachete de pe orice interfață de rețea disponibilă pe sistem.
* **Analiză detaliată a pachetelor:** Permite analiza fiecărui pachet capturat în detaliu, oferind informații despre header, protocoale și datele transmise.
* **Filtrare avansată:** Oferă un limbaj de filtrare puternic care permite selecția precisă a pachetelor de interes.
* **Decodare a protocoalelor:** Wireshark poate decoda sute de protocoale de rețea (IP, TCP, UDP, HTTP, DNS, și multe altele).
* **Analiză vizuală:** Grafice și statistici vizuale pentru a analiza traficul în funcție de diverse criterii (ex: volume de trafic pe fiecare protocol).
* **Exportul datelor:** Permite exportarea datelor capturate în formate precum **PCAP**, **CSV**, și **XML** pentru analize ulterioare.

**Avantaje:**

* **Open-source și gratuit.**
* Suport pentru un număr mare de protocoale și formate.
* Interfață grafică prietenoasă, ușor de utilizat.
* Comunitate activă și actualizări frecvente.
* Permite salvarea și analiza ulterioară a datelor capturate (întotdeauna poți analiza aceleași capturi multiple ori).

**Dezavantaje:**

* Poate consuma multe resurse, mai ales pe rețele mari.
* Este mai puțin eficient în capturarea traficului în timp real pentru rețele mari sau cu lățime de bandă mare.
* Interfața grafică poate deveni copleșitoare pentru începători din cauza complexității opțiunilor.

**Cazuri de utilizare:** Wireshark este ideal pentru depanarea rețelelor, analiza traficului de aplicație și diagnosticul de performanță. Este folosit frecvent pentru a înțelege comportamentele de rețea, pentru a detecta atacuri sau anomalii și pentru a analiza aplicațiile care rulează pe rețea.

**2) tcpdump**

**Descriere:** tcpdump este un alt instrument de capturare a pachetelor de rețea, dar spre deosebire de Wireshark, tcpdump funcționează din linia de comandă. Este un instrument extrem de rapid și eficient pentru capturarea pachetelor în rețelele de calculatoare, iar datorită simplității și eficienței sale, este folosit adesea pe servere și în scenarii automate sau de scripting.

**Funcționalități:**

* **Captura de pachete:** Poate capta pachete de pe orice interfață de rețea, inclusiv Wi-Fi.
* **Filtrare BPF (Berkeley Packet Filter):** Permite utilizatorilor să aplice filtre extrem de precise pentru a capta doar pachetele care îi interesează (de exemplu, toate pachetele dintr-o anumită adresă IP sau port).
* **Exportul datelor:** Pachetele capturate pot fi salvate în fișiere **PCAP** pentru analize ulterioare cu instrumente ca Wireshark.
* **Analiză de bază:** Poate decoda și analiza protocoale precum **IP, TCP, UDP, ICMP** și altele, dar cu mai puțină detaliere față de Wireshark.

**Avantaje:**

* **Rapid și eficient:** Este un instrument ușor de utilizat în medii de producție unde performanța este critică.
* **Consum redus de resurse:** Deoarece rulează în linie de comandă, consumă mult mai puține resurse comparativ cu Wireshark.
* **Ideal pentru scripting:** Poate fi folosit într-un mod complet automatizat și integrat în scripturi pentru capturi de pachete programate.
* **Flexibilitate:** Permite capturarea și filtrarea precisă a pachetelor, cu un control detaliat asupra ceea ce se captează.

**Dezavantaje:**

* **Lipsa interfeței grafice:** Nu are interfață grafică, ceea ce poate face analiza datelor mai dificilă pentru cei care nu sunt familiarizați cu linia de comandă.
* **Capacități limitate de analiză vizuală:** Deși poate analiza protocoale de rețea, nu oferă aceleași funcționalități vizuale avansate ca Wireshark.

**Cazuri de utilizare:** tcpdump este folosit frecvent pentru capturi rapide de pachete, diagnosticul problemelor de rețea și analize automate. Este de asemenea popular pe servere sau în medii în care resursele sunt limitate sau când se dorește integrarea sa într-un sistem automatizat de monitorizare.

**3) Zeek (fost Bro)**

**Descriere: Zeek**, cunoscut anterior sub denumirea de **Bro**, este un sistem open-source pentru monitorizarea și analiza rețelelor. Spre deosebire de Wireshark și tcpdump, Zeek este un **framework de securitate și monitorizare** a rețelelor care se concentrează pe analiza și detecția evenimentelor din rețea la nivel înalt. Este folosit pentru a examina și detecta activitățile de rețea, pentru a identifica comportamente anormale sau potențial dăunătoare și pentru a genera loguri detaliate ale activităților de rețea.

**Funcționalități:**

* **Monitorizarea rețelei la nivel de aplicație:** Zeek analizează fluxurile de rețea și detectează anomalii la nivelul aplicațiilor.
* **Detectarea evenimentelor de securitate:** Zeek poate fi configurat să detecteze diverse tipuri de atacuri, cum ar fi scanările de porturi, atacurile DDoS, injectarea de comenzi SQL, etc.
* **Scripturi personalizate:** Oferă un limbaj propriu de scripting, **Zeek scripting language**, care permite utilizatorilor să creeze reguli personalizate pentru a analiza evenimente și protocoale specifice.
* **Loguri detaliate:** Generează loguri detaliate care pot fi folosite pentru analiza ulterioară sau pentru investigarea incidentelor de securitate.
* **Suport pentru protocoale diverse:** Analizează o gamă largă de protocoale (HTTP, DNS, FTP, SSH, SMTP etc.) și poate integra datele cu alte soluții de securitate (de exemplu, SIEM).

**Avantaje:**

* **Puternic în securitate:** Zeek este un instrument de securitate avansat, excelent pentru detectarea atacurilor și monitorizarea comportamentului rețelelor.
* **Extensibilitate:** Posibilitatea de a crea scripturi personalizate pentru a analiza protocoale specifice sau pentru a implementa politici de securitate.
* **Loguri detaliate:** Oferă o gamă largă de loguri pentru a urmări activitățile din rețea și pentru a răspunde la incidente de securitate.
* **Scalabilitate:** Zeek poate fi scalat pentru a monitoriza rețele mari și complexe, fiind potrivit pentru organizații mari și centre de date.

**Dezavantaje:**

* **Complexitatea configurării:** Zeek necesită o configurare inițială și un învățământ detaliat pentru a fi utilizat eficient.
* **Consum mare de resurse:** Monitorizarea rețelelor mari poate consuma resurse semnificative, fiind necesare hardware puternice pentru a procesa traficul în timp real.
* **Curba de învățare:** Zeek poate fi mai dificil de utilizat pentru cei care nu au experiență în scripting sau administrarea rețelelor.

**Cazuri de utilizare:** Zeek este utilizat adesea în medii de securitate avansată, cum ar fi centrele de securitate a rețelelor, pentru a detecta comportamente anormale, pentru a implementa reguli personalizate de monitorizare și pentru a răspunde la incidente de securitate în timp real.

**4) SolarWinds Network Performance Monitor (NPM)**

**Descriere:** SolarWinds Network Performance Monitor (NPM) este o soluție comercială de monitorizare a rețelei, care include și funcționalități pentru capturarea și analiza traficului de rețea. Este o soluție completă destinată organizațiilor mari și medii, care doresc o platformă centralizată pentru a monitoriza performanța rețelelor, dispozitivelor și aplicațiilor.

**Funcționalități:**

* + **Monitorizare continuă:** SolarWinds NPM monitorizează rețeaua în timp real, identificând întreruperile și problemele de performanță.
  + **Captură și analiză a traficului:** Permite monitorizarea fluxurilor de trafic pe baza protocolului, a adresei IP și a porturilor.
  + **Vizualizare a performanței rețelei:** Grafice și hărți detaliate ale rețelei pentru a vizualiza performanța în timp real.
  + **Alertare și rapoarte:** Sistem de alerte în timp real și rapoarte detaliate care ajută administratorii să identifice rapid problemele.
  + **Analiză a aplicațiilor:** SolarWinds NPM poate urmări traficul aplicațiilor pentru a determina performanța acestora și impactul asupra rețelei.
  + **Configurare ușoară:** Configurare și implementare rapidă printr-o interfață web intuitivă.
  + **Scalabilitate:** Suportă rețele mari, scalându-se ușor în funcție de nevoile organizației.

**Avantaje:**

* + Suport excelent pentru rețele complexe și mari.
  + Ușor de utilizat, cu o interfață grafică prietenoasă.
  + Integrare cu soluții de management ale rețelei și de securitate.
  + Capabilități de monitorizare a aplicațiilor și a performanței rețelei.

**Dezavantaje:**

* + Este o soluție costisitoare, potrivită pentru organizații mari.
  + Poate fi mai puțin flexibil în comparație cu soluțiile open-source personalizabile.
  + Necesită licențiere anuală, ceea ce adaugă costuri suplimentare pe termen lung.

**5) NetworkMiner**

**Descriere:** NetworkMiner este un instrument de analiză forensică a traficului de rețea, special conceput pentru a extrage informații utile din pachetele de rețea capturate. Spre deosebire de Wireshark, NetworkMiner se concentrează pe recuperarea și prezentarea datelor importante din capturile de pachete, cum ar fi fișierele transferate, utilizatorii autentificați și sesiunile de rețea.

**Funcționalități:**

* + **Analiză forensică:** NetworkMiner este folosit pentru a reconstruirea sesiunilor de rețea și extragerea datelor transmise (fișiere, parole, etc.).
  + **Detectarea sesiunilor și utilizatorilor:** Poate extrage date din sesiunile HTTP, FTP, POP3, IMAP, SMB și multe altele.
  + **Decodificarea și analiza protocoalelor:** Permite decodificarea completă a protocoalelor și analizarea fișierelor transferate.
  + **Captura offline:** Poate analiza fișierele de captură deja realizate (PCAP) pentru a extrage informațiile relevante.
  + **Interfață grafică ușor de utilizat:** Interfață intuitivă care permite o analiză detaliată a traficului capturat.

**Avantaje:**

* + Ideal pentru analiza incidentelor de securitate și investigații forensice.
  + Permite extragerea detaliilor sensibile din traficul de rețea, cum ar fi parolele și fișierele transmise.
  + Ușor de utilizat pentru cei care nu sunt experți în analiza pachetelor.

**Dezavantaje:**

* + Nu este la fel de complet în ceea ce privește analiza în timp real.
  + Suportă mai puține protocoale comparativ cu Wireshark sau tcpdump.
  + Poate fi mai limitat pentru analize de performanță în rețele mari.

**3.5 Compararea soluțiilor existente**

Un tabel comparativ între soluțiile existente.

**3.6 Limitările soluțiilor existente**

* **Wireshark**: Nu este ideal pentru rețele mari sau pentru capturarea traficului în timp real din cauza consumului mare de resurse.
* **tcpdump**: Deși eficient și rapid, nu oferă capabilități avansate de analiză vizuală.
* **Zeek**: Necesită un hardware puternic și o configurare detaliată, ceea ce îl face dificil de implementat fără experiență.
* **SolarWinds NPM**: Costisitor și mai puțin personalizabil în comparație cu soluțiile open-source.
* **NetworkMiner**: Limitează analiza în timp real și nu poate decoda toate protocoalele.

**3.7 Concluzii asupra soluțiilor existente**

Analiza traficului de rețea este într-o continuă schimbare, iar tehnologiile emergente, precum **inteligenta artificială** și **machine learning-ul**, vor juca un rol tot mai important. Aceste tehnologii vor putea ajuta la detectarea automată a anomaliilor și a atacurilor sofisticate în timp real. Totodată, **tehnologiile 5G** și **internetul obiectelor (IoT)** vor genera noi provocări, deoarece vor aduce o creștere semnificativă a volumului și diversității traficului de rețea.

În concluzie, capturarea și analiza traficului de rețea reprezintă un domeniu esențial pentru menținerea securității și performanței rețelelor moderne. Soluțiile existente variază în funcție de complexitatea și scopul utilizării, iar alegerea celor mai potrivite instrumente depinde de cerințele fiecărei rețele în parte.

A logo of a company

Description automatically generated