UNIVERSITATEA TEHNICĂ A MOLDOVEI

Cu titlu de manuscris
CZU: 004.738.5.056.5(043.2)

AMEEN ALI

ASIGURAREA SECURITĂȚII REȚELELOR DE CALCULATOARE BAZATE PE TEHNOLOGII DE REȚEA DEFINITE SOFTWARE

Rezumatul tezei de doctor în Științe Inginerești

SPECIALITATEA 232.01 SISTEME DE CONDUCERE, CALCULATOARE ȘI REȚELE INFORMAȚIONALE

CHIȘINĂU, 2025

Teza de doctor a fost elaborată la Departamentul Informatică și Ingineria Sistemelor al Universității Tehnice a Moldovei.

Conducător științific:
PERJU Veaceslav, dr. hab., acad. AII

Membrii Comisiei de îndrumare:
GUȚULEAC Emilian, dr. hab., prof. univ.
ABABII Victor, dr, conf. univ.
SUDACEVSCHI Viorica, dr, conf. univ.

Comisia de Susținere Publică a Tezei de Doctorat:
LEAHU Alexei, dr., univ. prof., UTM, Președinte al CSP a TD.
IZVOREANU Bartolomeu, dr., conf. univ., UTM, Secretar științific.
PERJU Veaceslav, dr. hab., acad. AII, AMFA, membru.
CIORBA Dumitru, dr., conf. univ., UTM, referent oficial.
SUDACEVSCHI Viorica, dr., conf. univ., UTM, referent oficial.
OHRIMENCO Serghei, dr. hab., prof. univ., ASEM, referent oficial.
ZGUREANU Aureliu, dr., conf. univ., ASEM, referent oficial.

Susținerea tezei va avea loc pe data de **15.05.2025** la ora **14:00** în cadrul ședinței Comisiei de Susținere Publică a Tezei de Doctorat la Universitatea Tehnică a Moldovei, str. Studenților, 9/7, blocul de studii nr. 3, Facultatea Calculatoare, Informatică și Microelectronică, aula **3-208**, MD-2045, Chișinău, Republica Moldova.

Teza de doctor și Rezumatul pot fi consultate la Biblioteca Științifică a Universității Tehnice a Moldovei și pe pagina web ANACEC.

Rezumat a fost expediat pe data de **11.04.2025**.

Secretar științific al Comisiei de Susținere Publică a Tezei de Doctorat:
IZVOREANU Bartolomeu, dr., conf. univ.

Conducător științific:
PERJU Veaceslav, Dr. hab., Acad. AII

Autor:
AMEEN Ali, Ing., Mag.

CUPRINS

REPERE CONCEPTUALE ALE CERCETĂRII

Actualitatea și semnificația teoretică a cercetării reiese din necesitatea creării unei infrastructuri avansate a rețelelor de calculatoare pentru a face față provocărilor în continuă în domeniul securității cibernetice și cuprinde analiza, precizarea și definirea principiilor teoretice ale structurii clasice a rețelelor de calculatoare, structurii SDN, standardele de securitate cibernetică și conceptele esențiale ale algoritmilor VPN, RSA și Blockchain.

Importanța și relevanța problemei acordate constă în elaborarea unui nou set de algoritmi și topologii ale controlerelor SDN pentru sporirea nivelului de securitate al SDN și evaluarea teoretică a nivelului de securitate al rețelelor de calculatoare. Topologia SDN reprezintă o soluție în unele probleme, dar odată cu aceasta apar și noi provocări și de aici reiese importanța acestui studiu, destinat asigurării unui nivel mai înalt de securitate al structurilor SDN și rețelelor de calculatoare care utilizează topologii SDN.

Scopul principal al tezei este elaborarea soluțiilor noi pentru sporirea nivelului de securitate al Rețelei Definite Software printr-un set de algoritmi și topologii de controlere SDN cu scopul securizării datelor de schimb între noduri și de a elabora metodologia de evaluare a nivelului de securitate a rețelei de calculatoare.

Obiectivele cercetării:

1. Analiza metodelor și tehnologiilor existente pentru asigurarea securității rețelelor de calculatoare.
2. Elaborarea algoritmilor de asigurare a securității topologiilor SDN pentru protecția sporită împotriva atacurilor cibernetice.
3. Elaborarea topologiilor controlerelor SDN pentru asigurarea securității rețelelor de calculatoare.
4. Elaborarea noii metode de evaluare a securității rețelelor de calculatoare.
5. Evaluarea eficienței securității topologiilor de controlere SDN propuse pentru asigurarea securității rețelelor de calculatoare.

Ipoteza cercetării. O posibilă direcție în soluționarea problemei de cercetare poate fi elaborarea de noi algoritmi, eficienți pentru securizarea datelor de schimb între nodurile multiple din rețelele SDN, de noi tipuri de topologii ale controlerelor SDN pentru asigurarea securității rețelelor de calculatoare, și a bazei teoretice de evaluare a nivelului de securitate al rețelelor de calculatoare.

Metodele de cercetare aplicate: metode de criptografie, modelare și simulare, utilizarea rețelelor Petri pentru cercetarea fiabilității abordărilor propuse privind asigurarea securității, evaluarea riscurilor de securitate, analiza generală a datelor economice legate de costuri.

Noutatea științifică a rezultatelor obținute constă în elaborarea algoritmilor noi pentru asigurarea securității a topologiilor SDN – algoritmii Hydra, DOUBLE RSA și registrul distribuit al Blockchain; elaborarea de noi topologii de controlere – de tip Serial, Paralel și Hybrid; elaborarea metodei noi de evaluare a securității tehnologiei SDN, bazate pe utilizarea rețelelor Petri și parametri propuși - Fiabilitatea serviciului, Factorul de securitate, Factorul de risc, Parametrul Modificat de Evaluare a Riscului și Efectul de Cost.

Semnificația teoretică reprezintă algoritmii criptografici pentru asigurarea securității SDN, cum ar fi arhitectura Hydra, canalul securizat al algoritmului VPN, algoritmul Double RSA și algoritmul Distributed Ledger of Blockchain; noi topologii de controlere SDN pentru sporirea nivelului de securitate al rețelelor de calculatoare; nouă metodă de evaluare a nivelului de securitate al rețelelor de calculatoare, bazată pe utilizarea rețelelor Petri și a unui set de parametri.

Problemă științifică importantă soluționată constă în elaborarea unui nou set de algoritmi de asigurare a securității și de topologii controlerelor structurilor SDN pentru a spori nivelul de securitate al structurilor SDN și elaborarea teoriei de evaluare a nivelului de securitate al rețelelor de calculatoare.

Valoarea aplicativă a tezei a lucrării este determinată de arhitectura SDN dezvoltată pe baza unor noi algoritmi propuși pentru a face față problemei de centralizare și de protejare a conexiunii între controlere multiple, ceea ce are o mare contribuție pentru comunitatea SDN. De asemenea, oferă o imagine mai bună a nivelului de securitate al unei rețele prin evaluarea acesteia folosind instrumente matematice pe baza parametrilor propuși.

Rezultatele științifice înaintate pentru susținere:

1. Algoritmi de asigurare a securității rețelelor SDN: set de algoritmi integrate în arhitectură Hydra, canalul securizat al algoritmului VPN, algoritmul RSA dublu, registru distribuit al algoritmului Blockchain.
2. Topologiile controlerelor SDN pentru asigurarea securității rețelelor de calculatoare: de tip Serial, Paralel, Hibrid.
3. Metodă de evaluare a nivelului de securitate a rețelelor de calculatoare bazată pe utilizarea rețelelor Petri și setului de parametri propuși: Fiabilitatea Serviciului, Factorul de Apărare, Factorul de Risc, Factorul de Risc Modificat și Efectul de Cost.

Aprobarea rezultatelor. Rezultatele cercetării au fost publicate în 13 lucrări științifice, dintre care 8 de un singur autor, cu un volum total de peste 7 coli de autor, inclusiv 8 - în reviste de categoria B+, 4 - în reviste de categoria B, 1- în revista de categoria C, au fost raportate la 5 conferințe internaționale și la 1 conferință națională.

Conferințe la care au fost prezentate rapoarte: Conferința Tehnico-științifică a UTM, 2019; Conferința Internațională „Mediul Strategic de Securitate: Tendințe și Provocări SSETC-2019", 2021, Academia Militară a Forțelor Armate; Conferința internațională de comunicații electronice și calcul, 2020, UTM; Conferința științifică internațională "Evoluția științei militare în contextul noilor amenințări la adresa securității naționale și regionale", 2020, Academia Militară a Forțelor Armate; Conferința științifică internațională „Republica Moldova în contextul noii arhitecturi regionale de securitate", 2024, Academia Militară a Forțelor Armate.

Structura și volumul tezei. Teza este alcătuită din introducere, **3** capitole, concluzii generale și recomandări, bibliografie **130** titluri, textul principal din **153** pagini, care include **47** figuri, **23** tabele și **6** anexe. Volumul compartimentelor de baza este **105** pagini. Rezultatele obținute în cadrul tezei au fost publicate în **13** lucrări științifice.

Cuvinte-cheie: securitate, asigurare, rețea de calculatoare, SDN, algoritm, controler, blockchain, RSA dublu, rețele Petri.

CONȚINUTUL TEZEI

INTRODUCERE

Introducerea reflectă premisele teoretice și practice, care subliniază actualitatea și importanța problemei cercetate. Se formulează scopul și obiectivele cercetării, se descrie ipoteza cercetării, valoarea teoretică și practică a tezei.

1 ANALIZA METODELOR SI TEHNOLOGILOR EXISTENTE PENTRU ASIGURAREA SECURITATII RETELELOR DE CALCULATOARE

În Capitolul 1 este expusă o privire de ansamblu asupra stării actuale a rețelelor de calculatoare, acoperind structura și ierarhia acestora. Urmează descrierea rețelelor definite software (SDN), evidențiind structura, avantajele și provocările asociate de securitate. Este menționat potențialul SDN de integrare cu alte tehnologii, arătând importanța acestuia în abordarea amenințărilor de securitate. Proiectul Ethane [1], în care s-a propus separarea nivelelor de control și de date, este prezentat ca baza SDN.

Este efectuată comparația dintre structura rețelelor clasice și a rețelelor definite software. Există doi factori care denotă principalele diferențe dintre configurațiile de rețea tradiționale față de configurația SDN, și anume:

1. Funcționalitatea rețelei este suportată în principal de un aparat sau dispozitiv dedicat. În acest caz aparatul dedicat înseamnă unul sau mai multe comutatoare, routere și/sau controlere de livrare a aplicațiilor.

2. Majoritatea funcțiilor acestui aparat sunt implementate în hardware dedicat. În acest scop este folosit ASIC (circuit integrat specific aplicației). Organizațiile se confruntă din ce în ce mai mult cu limitările privind această abordare centrată pe hardware, cum ar fi configurația tradițională consumatoare de timp și predispusă la erori: sunt necesari mulți pași când un administrator IT trebuie să adauge sau să elimine un singur dispozitiv într-o rețea tradițională [2]. În primul rând, aici vor trebui configurate manual mai multe dispozitive (switch-uri, routere, firewall-uri). Următorul pas este utilizarea instrumentelor de management la nivel de dispozitiv pentru a actualiza numeroase setări de configurare, cum ar fi ACL-uri, VLAN-uri și calitatea serviciului. Această metodă de configurare îngreunează administratorii să aplice politici consecvente, ceea ce duce la potențiale încălcări de securitate și probleme de conformitate.

Prin alte cuvinte, configurațiile tradiționale creează provocări semnificative la îndeplinirea cerințelor rețelelor de calculatoare. Mediile cu mai mulți furnizori necesită un nivel ridicat de expertiză. Administratorul de rețea va trebui să aibă cunoștințe cuprinzătoare despre toate tipurile de dispozitive și furnizori pentru a configura și a seta cu succes rețeaua. Arhitecturile tradiționale complică segmentarea rețelei, în special odată cu sporire conectivității dispozitivelor precum sistemele de alarmă și camerele de securitate, pe lângă tablete, PC-uri și smartphonuri.

SDN simplifică acest lucru prin rețele virtuale, separate de infrastructura fizică. Combinația dintre nivel de rețea și programabilitatea rețelei asigură procesul de colectare a informațiilor in sistemele de detectare a intruziunilor (IDS) și sistemele de prevenire a intruziunilor (IPS) existente, urmate de analiza și reprogramarea centralizată a rețelei. Această abordare poate face SDN mai robust la atacurile rău intenționate decât rețelele tradiționale [3].

2 ELABORAREA ALGORITMILOR SI TOPOLOGILOR PENTRU ASIGURAREA SECURITATII RETELELOR DE CALCULATOARE

În Capitolul 2 se propun soluții noi pentru arhitectură SDN care reprezintă algoritmi cheie și metode, și care formează o arhitectură integrată pentru a îmbunătăți securitatea SDN.

Au fost determinate principale probleme în structura SDN care au servit baza acestei cercetări:

1. Centralizare: în timp ce centralizarea arhitecturii SDN este un avantaj-cheie față de

modelele clasice, aceasta reprezintă, de asemenea, o potențială amenințare prin crearea unui singur punct de eșec (SPOF).

2. API-ul est-vest: nu-i este acordată suficientă atenție și ar putea fi vulnerabil la unele atacuri cibernetice precum MITM, DDoS sau tipuri de atacuri DoS [4], [5], [6].

Algoritmi pentru asigurarea securității SDN bazate pe Criptografie.

1. Set de algoritmi integrați în arhitectură Hydra pentru a contracara atacurile de tip Denial of Service/Distributed Denial of Service (DoS/DDoS) [7], prin instalarea botnet-urilor [8], [9] pe computerele din rețea conectate la controlerul, care are instalat software-ul Hydra, pentru a constitui potențiali protectori și pentru a ataca IP-ul sursă al infractorului. Diagrama arhitecturii Hydra este prezentată în Figura 1.

2. Canal securizat al algoritmului VPN. O rețea privată virtuală (VPN) utilizează Internet Protocol Security (IPsec), creând canale de comunicații virtuale securizate. Poate fi integrat în arhitectură propusă. Un VPN este necesar pentru a asigura certitudinea că confidențialitatea datelor sensibile poate fi păstrată și transmisă în rețea, o rețea locală (LAN) sau funcțională, astfel încât numai utilizatorii autorizați să poată accesa datele sensibile [10]. Practic, cercetarea propune să se conecteze la fiecare două controlere, folosind canalul securizat al VPN, chiar dacă acestea se află în aceeași clădire. Diagrama algoritmului VPN este prezentată în Figura 2.

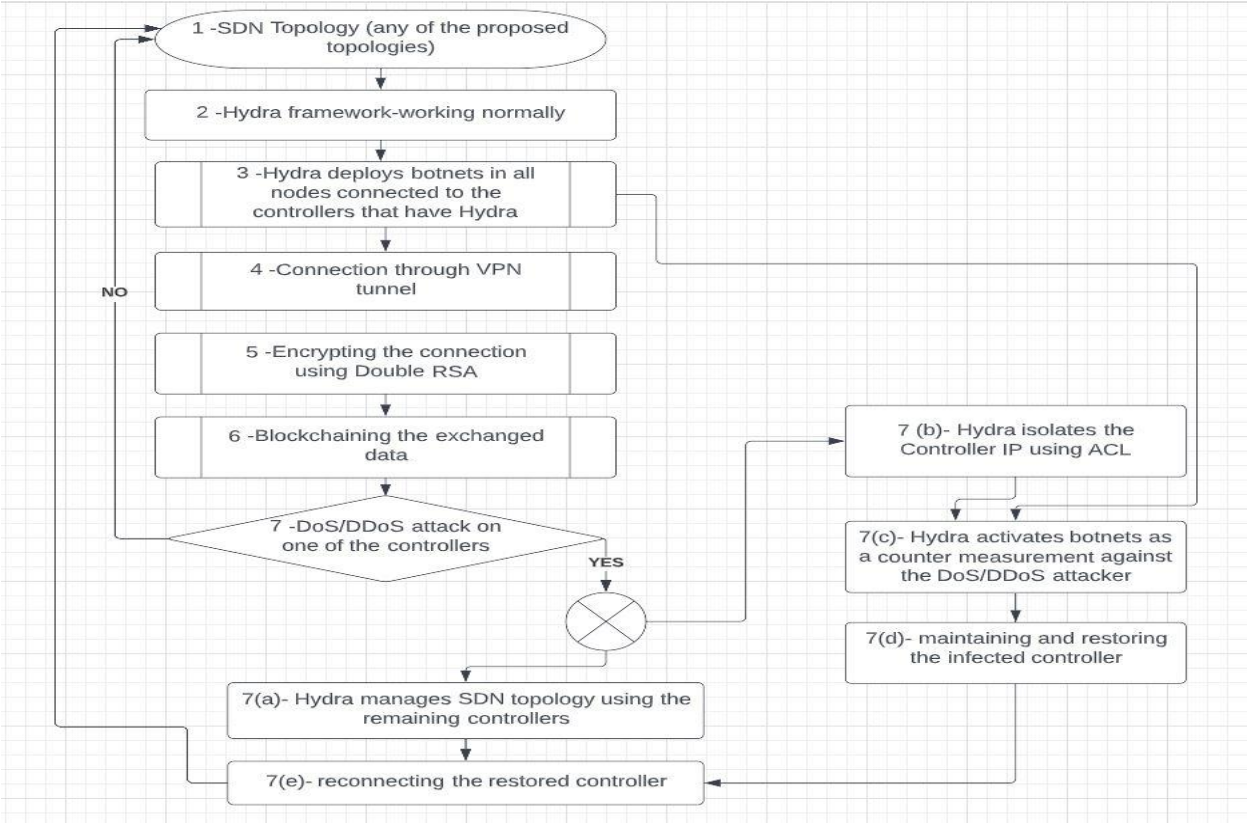

Figura 1. Diagrama arhitecturii Hydra.

3. Algoritmul RSA Dublu. Algoritmul acesta reprezintă RSA în care a fost adăugată o pereche suplimentară de chei pentru semnăturile digitale în canalul de criptare, ceea ce înseamnă că vor exista două perechi de chei, o pereche pentru fiecare procedură de criptare-decriptare; două canale de autentificare. Dacă se dovedește a fi adevărat că orice metodă de a sparge RSA poate conduce la un algoritm eficient pentru factorizarea întregului mare, este posibil să tragem concluzia că ruperea RSA și problema-factorului-întreg sunt cu același grad de dificultate [11]. Diagrama algoritmului RSA Dublu este prezentată în Figura 3.

4. Registru distribuit al algoritmului Blockchain. Acest algoritm este încorporat în arhitectură SDN pentru a securiza actualizările de configurare între mai multe controlere iar acesta este folosit într-un mod diferit de protocolul Marconi [12]. Diagrama algoritmului registrul distribuit Blockchain este prezentată în Figura 4.

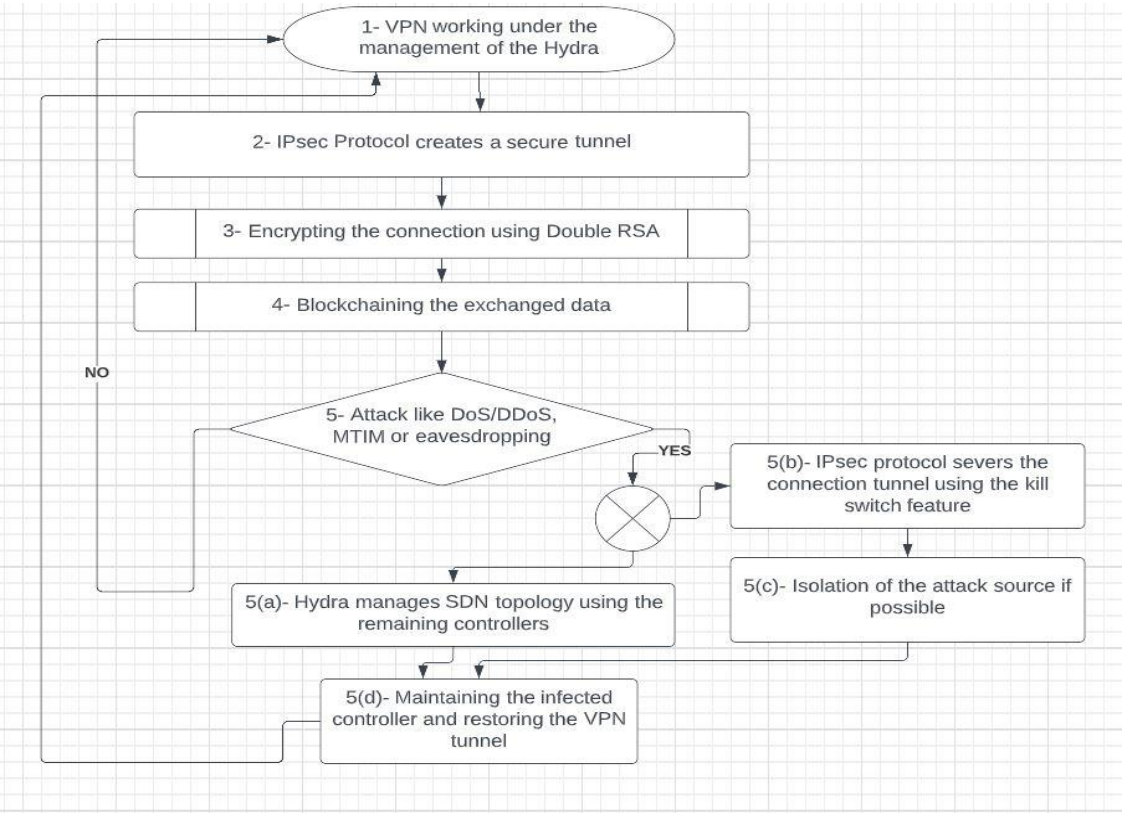

Figura 2. Diagrama algoritmului VPN.

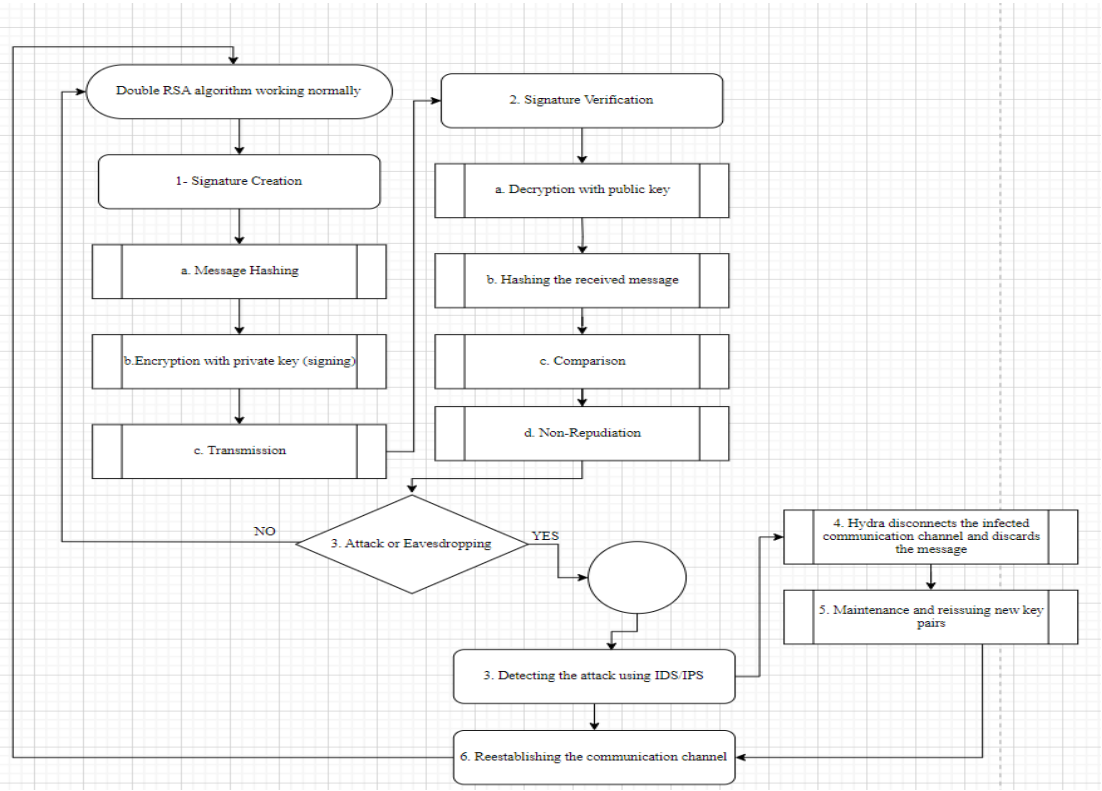

Figura 3. Diagrama algoritmului RSA Dublu.

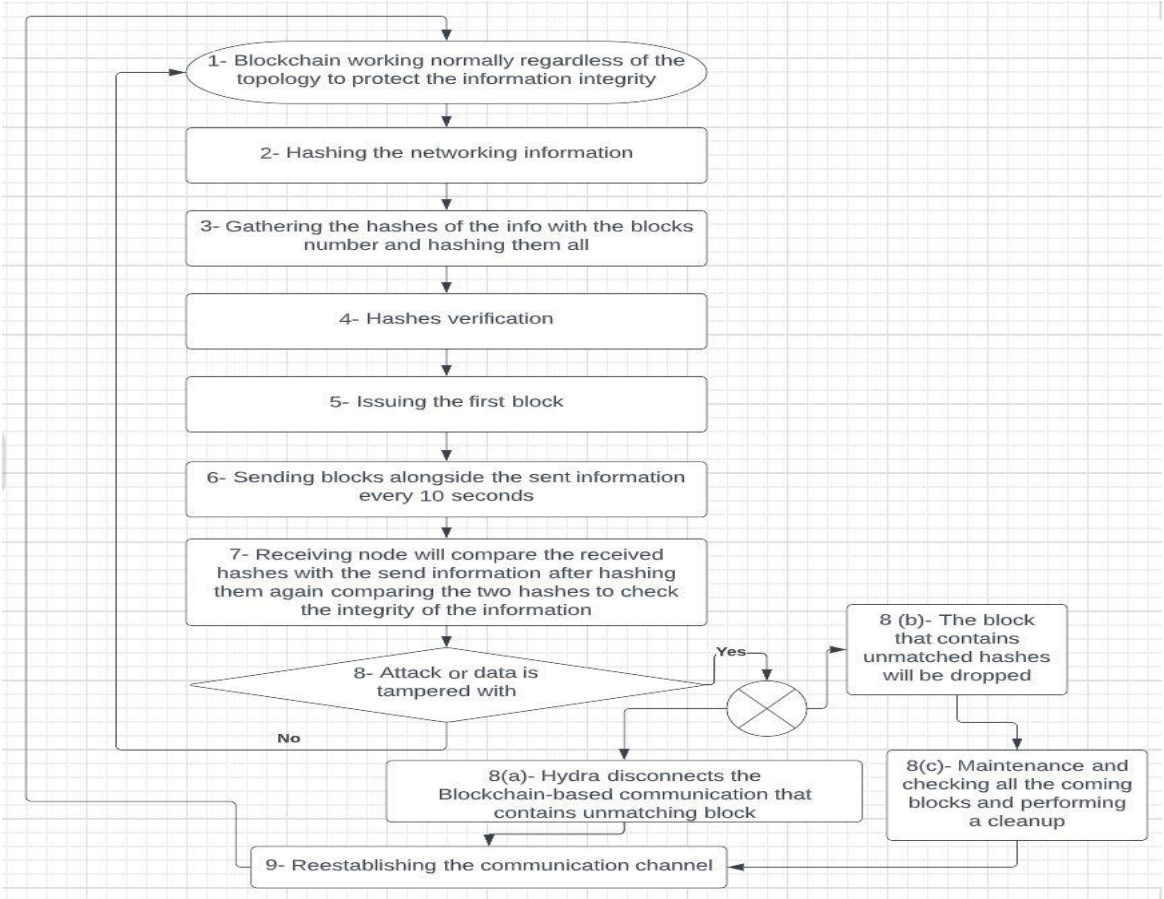

Figura 4. Diagrama algoritmului registrul distribuit Blockchain.

Topologiile propuse pentru asigurarea securității SDN-ului.

În această cercetare se propun diverse topologii privind abordarea problemei centralizării, oferind un avantaj față de structurile de rețea tradiționale. În timp ce o rețea definită software (SDN) simplifică gestionarea și aplicarea politicilor, singurul său controler poate fi un singur punct de eșec (SPOF) dacă este atacat. Topologiile propuse, care pot activa sau nu arhitectură Hydra, ajută la atenuarea centralizării prin varierea numărului de controlere și a interacțiunilor acestora. Deși unele dintre aceste topologii sunt parțial utilizate în alte cercetări, diferența principală constă în interacțiunea dintre controlere.

1. Topologia serială. Cercetarea conturează o topologie serială cu un controler principal și două copii de rezervă pentru a asigura continuitatea rețelei în timpul atacurilor. Controlerul principal actualizează copiile de rezervă la fiecare 10 secunde; întârzierile indică un potențial atac DDoS, determinând preluarea de către backup. Ca parte a arhitectură Hydra, controlorii implementează rețele bot pentru contramăsuri împotriva atacatorilor. Topologia serială este prezentată în Figura 5.

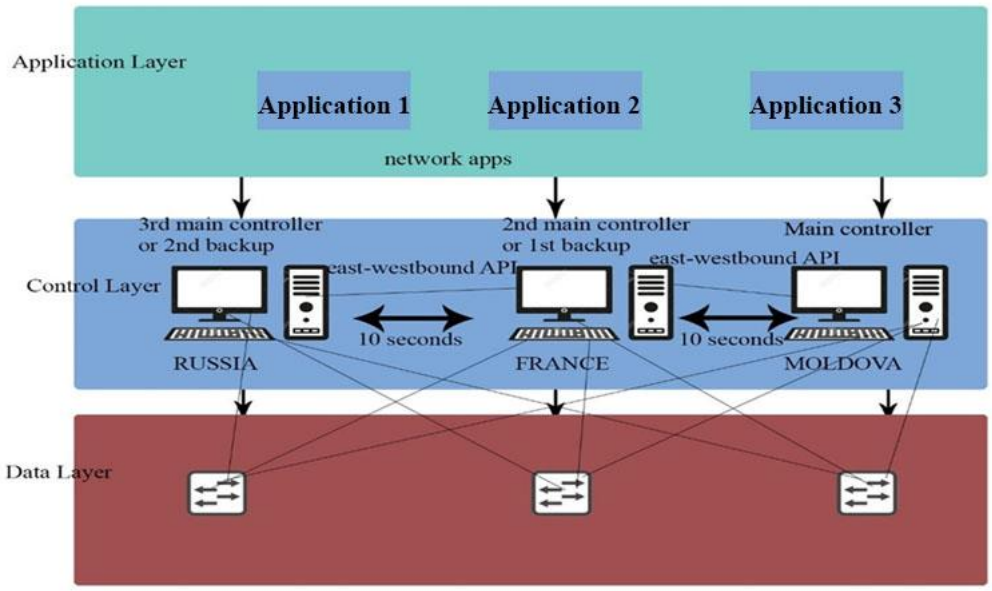

Figura 5. Topologia serială.

2. **Topologia paralelă.** În această topologie funcționează trei controlere ca o unitate unificată, procesând informațiile în mod sincron și acordând prioritate segmentelor de rețea din apropiere fără o ierarhie strictă. Ei trimit actualizări la fiecare 10 secunde, iar într-un atac DoS/DDoS, controlorii îl pot izola pe cel infectat, îi pot distribui încărcătura sau îi pot contraataca pentru a menține integritatea rețelei. Topologia paralelă este prezentată în Figura 6.

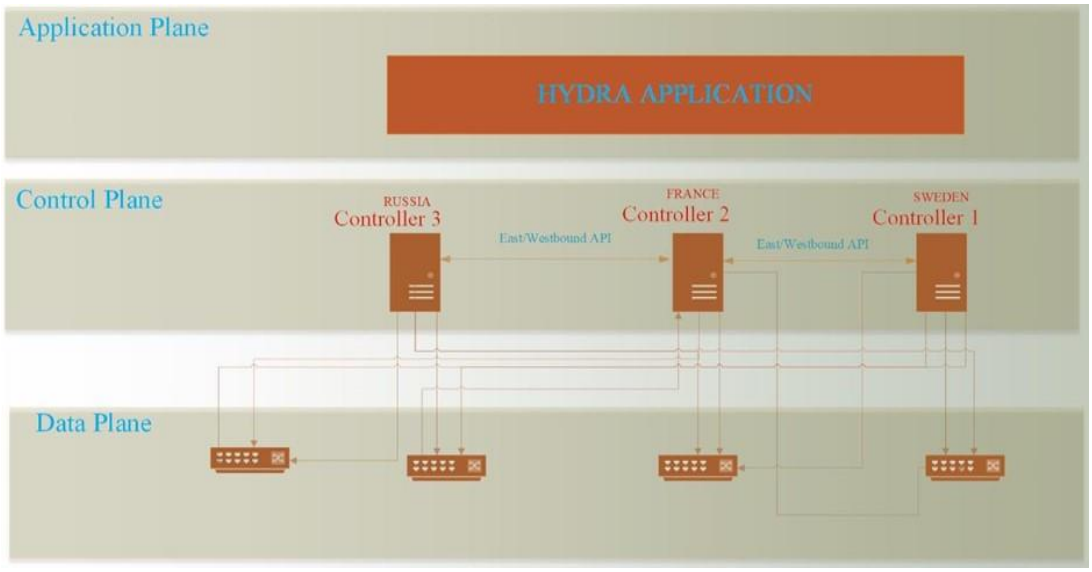

Figura 6. Topologia paralelă.

3. **Topologia hibridă.** Această topologie combină modelele anterioare cu șase controlere: trei controlere primare în paralel, fiecare asociat cu o copie de rezervă care se activează în caz de defecțiune. Actualizările sunt trimise la fiecare 10 secunde, iar backup-urile mențin conexiunile cu principalele lor și alte backup-uri. Pe când topologia standard se bazează

pe un singur controler, limitându-i capacitatea de a gestiona amenințările în creștere și de a implementa algoritmi multicontroler. Topologia hibridă este prezentată în Figura 7.

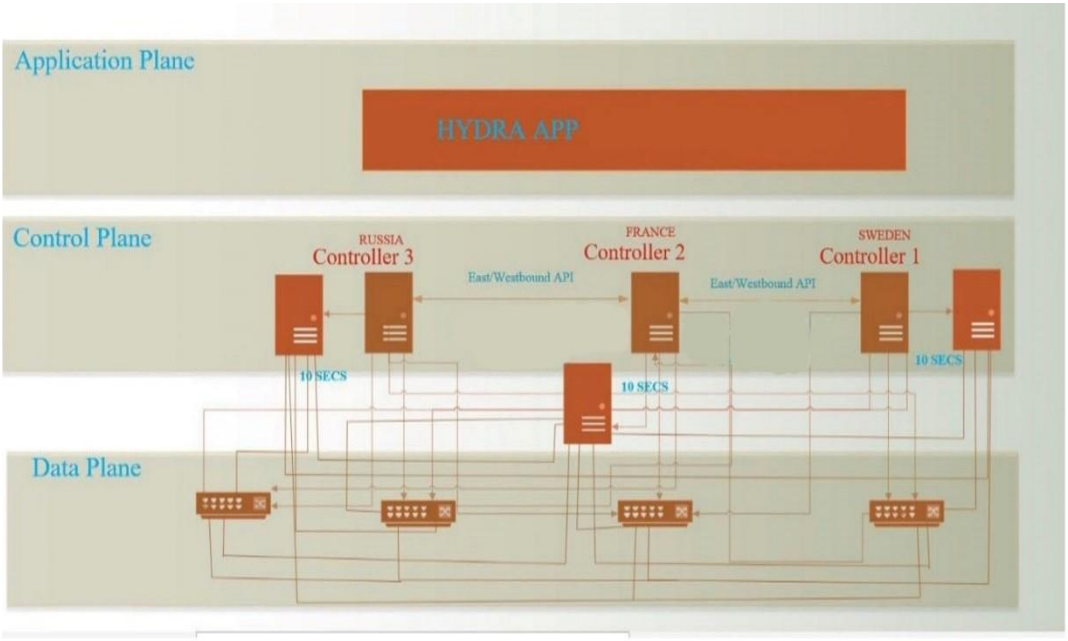

Figura 7. Topologia hibridă.

4. Topologia standard. Această topologie de rețea de bază, definită software, se bazează pe un singur controler pentru a gestiona comutatoarele și computerele, riscând eșec în timpul cererii mari sau a unui atac DoS/DDoS. Fără o copie de rezervă, un astfel de atac ar putea compromite controlerul, amenințând securitatea și recuperarea rețelei. În Figura 4 este prezentată topologia standard. Autorul tezei a publicat un articol referitor la un sondaj pentru a oferi o informația generală privind SDN și principalele sale avantaje, precum și dezavantaje [13], [14].

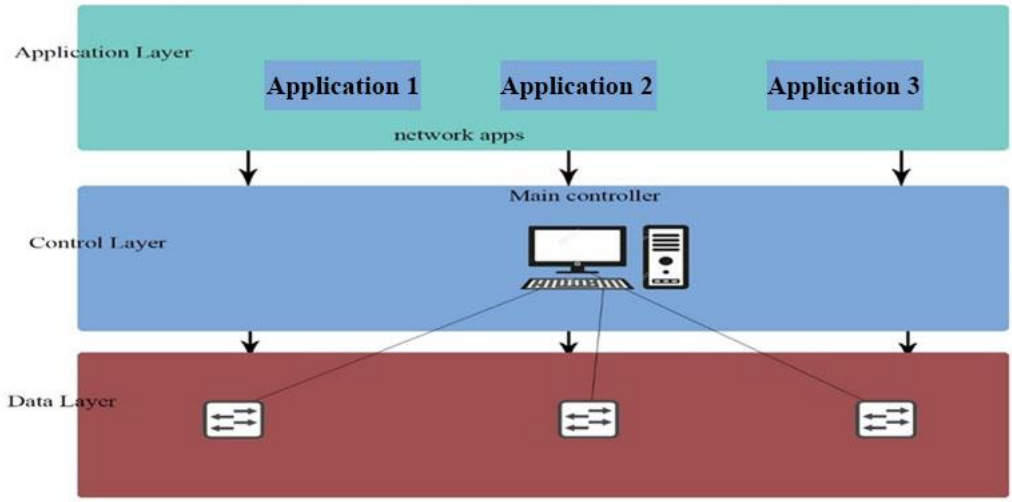

Figura 8. Topologia standard.

3 EVALUAREA EFICIENȚEI TOPOLOGILOR PROPUSE PENTRU ASIGURAREA SECURITĂȚII REȚELELOR DE CALCULATOARE

Capitolul 3 este dedicat evaluării topologiilor controlerelor propuse pentru asigurarea securității rețelei de calculatoare. A fost elaborată noua metodă de evaluare a nivelului de securitate a rețelelor de calculatoare bazată pe utilizarea Rețelelor Petri și setului de parametri propuși. A fost efectuată modelarea topologiilor SDN propuse prin rețele Petri. S-a executat simularea topologiilor folosind modulul Generalized Stochastic Petri Nets. A fost determinată eficiența topologiilor folosind un set de parametri.

Noua metodă de evaluare a nivelului de securitate a rețelelor de calculatoare bazată pe Rețele Petri și un set de parametri.

Metoda propusă constă din 3 etape. **În prima etapă**, pentru topologia controlerului SDN supus investigației, se elaborează un model Petri Nets. În a **doua etapă**, se efectuează simularea modelului elaborat folosind modulul Generalized Stochastic Petri Nets (GSPN) de 6 parametri (P, T, F, W, M_0, λ), unde $P= \{P_1, P_2 \dots P_m\}$ este un set finit de locuri, și obținerea datelor numerice referitoare la locuri și tokene. În a **treia etapă**, în baza datelor obținute prin simulare se va calcula setul de parametri, cum ar fi fiabilitatea serviciului, factorul de apărare, factorul de risc, riscul de securitate modificat și efectul de cost, care vor reflecta nivelul de securitate al topologiei SDN. Se va face analiza si interpretarea rezultatelor obținute.

Descrierea setului propus de parametri pentru evaluarea nivelului de securitate a rețelei de calculatoare urmează.

1. ***Fiabilitatea Serviciului.*** Fiabilitatea Serviciului (Reliability of Service *RoS*) este asemănătoare cu Calitatea Serviciului (Quality of Service QoS), care este definiția performanței serviciului oricărui sistem, cum ar fi o rețea de calculatoare sau un cloud computing etc. SDN-ul are multe caracteristici pozitive, care au atras atenția cercetătorilor pentru a îmbunătăți QoS a diverselor aplicații de rețea contemporane [15]. Dar *RoS* este puțin diferită și are o specificație mai detaliată, adaptată necesităților SDN. Se propune de a evalua *RoS* în mod următor:

$$RoS = 1 - TANR / TANR_O. \quad (1)$$

Unde *TANR* este numărul mediu total de solicitări de rețea ale topologiilor propuse, care este suma tuturor mediilor după împărțirea lor la numărul acestor medii, semnificând solicitările pe server și nivelul de apariție a riscului. $TANR_O$ este numărul mediu total sau intensitatea cererilor în controlerul topologiei standard.

2. ***Factorul de apărare.*** Factorul de apărare *DF* poate fi utilizat pentru a determina puterea și fezabilitatea de securitate a rețelei împotriva atacurilor DoS/DDoS. În ceea ce privește rețelele Petri, solicitările vor fi reprezentate de câte token-uri în anumite locuri care, la rândul lor, reprezintă noduri specifice din rețeaua definită de software, iar acele noduri specifice de interes sunt controlerele SDN. În ecuația (4), locurile reprezentând controlerele SDN sunt notate cu *K*, unde $K \in P$, *P* este întregul grup de locuri din modelul Petri Nets (PN), care la rândul său este un tuplu de 5 obiecte, $PN = \{P, T, I, O, M_0\}$[16], unde *P* este mulțimea finită de locuri, *T* este o mulțime finită de tranziții, *I* este funcția de intrare, *O* este funcția de ieșire și M_0 este marcarea inițială și:

$$K = \sum_{i=1}^{i=n} Ki,\ K_i \in \{1 - n\}. \tag{2}$$

$$Z = \sum_{i=1}^{i=n} Zi,\quad Z_i \in \{0 - \infty\}. \tag{3}$$

$$DF = [\sum_{i=1}^{i=n} Ki] / [\sum_{i=1}^{i=n} Zi] = \sum_{i=1}^{i=n} [\frac{Ki}{Zi}]. \tag{4}$$

Unde *K* este numărul locurilor care reprezintă controlerele dintr-un anumit model, $K_i = (K_1, K_2 \ldots K_n)$ și *Z* este valoarea jetoanelor din acele locuri K_i, $Z_i = (0 \ldots \infty)$.

Parametrul Factorului de Apărare depinde în principal de evaluarea puterii controlerelor rețelei definite de software și asta înseamnă disponibilitatea lor pentru a descuraja orice tip de atac DoS/DDoS. Prin urmare, putem constata, că cu cât avem mai multe controlere, cu atât capacitatea rețelei este mai bună de a descuraja aceste atacuri.

Asta înseamnă cu cât mai multe controlere, cu atât este mai bună și mai mare valoarea DF și asta explică de ce ecuația *DF* are locurile care reprezintă controlerele în poziția numărătorului deoarece numărul de controlere este proporțional cu valoarea *DF*. În timp ce, pe de altă parte, putem vedea că cu cât sunt mai multe tokene care reprezintă cererile, cu atât rețeaua devine mai slabă și asta înseamnă că vom obține mai puțină valoare a lui *DF*.

Deci, valoarea *DF* și numărul de tokene sau cereri sunt invers proporționale și de aceea ar trebui puse în poziția numitorului. În plus, merită să menționăm că, dacă am inversat *DF*-ul, adică dacă token-urile/cererile sunt împărțite la locuri/controlere, atunci vom obține câte cereri pe server [17].

3. ***Factorul de Risc.*** Parametrul Factor de Risc *RF* poate fi utilizat pentru a determina porțiunea slabă a rețelei. Valorile Numărului Mediu Total (intensitatea distribuției) cererilor (*TANR*) pot fi interpretate ca Factor de Risc. Deoarece trebuie să găsim puterea și capacitatea de apărare a controlerelor de rețea pentru a descuraja atacurile DoS/DDoS și cu cât avem mai multe tokene/cereri, cu atât controlerele vor fi mai ocupate și mai slabe și astfel nu vom determina

capacitatea necesară de apărare sau nivelul de fiabilitate al rețelei, ci mai degrabă punctul slab. Parametrul dat poate fi estimat ca:

$$RF = 1/DF. \quad (5)$$

Unde *DF* este valoarea Factorului de Apărare a topologiei estimate. Parametrul *RF* va fi în continuare opusul valorii lui *TANR*. Deci, locurile/controlerele ar trebui să se afle la numărător, iar tokenurile/cererile la numitor și aceasta este o altă dovadă logică a motivului pentru care a fost elaborată formula respectivă.

4. *Parametrul Modificat de Evaluare a Riscului.* Pentru a evalua nivelul de securitate al rețelelor de calculatoare, este posibil de a folosi legea de evaluare a riscurilor, dar pentru a o face potrivită pentru SDN. Atunci este posibilă modificarea legii de evaluare a riscurilor și după modificare, se va numi în această cercetare ca parametrul Evaluarea Riscului Modificat (*RM*). Pe baza legii modificate de evaluare a riscurilor de securitate putem evalua nivelul de protecție al rețelelor de calculatoare, care prevede [18]:

$$R = P_0 * V. \quad (6)$$

Unde *R* este valoarea riscului de securitate care arată probabilitatea că o amenințare va acționa cu succes asupra unei vulnerabilități și severitatea rezultatelor acelui atac, P_0 reprezintă probabilitatea inițială de apariție a vulnerabilității și *V* reprezintă valoarea sau costul.

Prin alte cuvinte, folosind această formulă putem estima cât de mult arhitectura propusă va reduce riscul de securitate unei rețele de calculatoare, asigurând astfel securitatea acesteia. Deoarece un server este partea cea mai importantă și are cel mai mare nod de valoare din mediul de rețea, în care ne vom instala software-ul controlerului, atunci putem spune că are cea mai mare valoare a impactului. Serverele au valoarea *V*=100 ca impact asupra activului, deoarece este valoarea impactului serverului asupra stratului de socket securizat (SSL), care este același strat în care funcționează protocolul OpenFlow.

Probabilitatea de vulnerabilitate P_0 = 0,025 este estimată pe baza comenzilor pierdute din cauza atacului de tip denial of service de la serverul web. Putem obține o nouă valoare a probabilității P_n, care va fi afectată de *DF* matematic, în mod următor:

$$P_n = P_0 / DF. \quad (7)$$

Cu cât factorul de apărare este mai mare, cu atât este mai bine, fiind opusul probabilității de vulnerabilitate. Asta înseamnă că ar trebui să fie invers proporționale din punct de vedere matematic, așa cum este logic și de aceea este poziționat astfel în formula de estimare a probabilității de vulnerabilitate. Este posibil constatat, că arhitectura propusă și formula derivată din modelarea acesteia vor reduce probabilitatea apariției atacurilor (cum ar fi atacurile

DoS/DDoS) și pentru asta propunem o versiune modificată a parametrului de evaluare a riscurilor de securitate, care va fi astfel:

$$RM = P_n * V. \quad (8)$$

5. ***Parametrul efectul de cost.*** Pentru a evalua influența costurilor la utilizarea topologiilor de controler propuse în scopul asigurării securității SDN, au fost folosite datele privind prețurile switch-urilor, calculatoarelor și controlerelor [19], [20]. Anterior au fost descrise structurile de bază ale topologiilor controlerelor - Serial, Paralel, Hybrid și Ordinary. Să estimăm costul acestor topologii, avînd la bază topologia standard, care include 1 controler, 3 comutatoare și 6 calculatoare. Atât topologiile seriale, cât și cele paralele vor avea 3 controlere, 3 comutatoare și 6 calculatoare, iar topologia hibridă va conține 6 controlere, 3 comutatoare și 6 calculatoare.

În acest caz, costul total *TC* al topologiei de rețea standard poate fi estimat astfel:

$$TC_O = CC+3SC+6NC. \quad (9)$$

Unde *CC*, *SC* și *NC* reprezintă costul controlerului, comutatorului și, respectiv, computerului de rețea. Costul total al topologiilor seriale și paralele va fi estimat prin formula:

$$TC_{S,P} = 3CC+3SC+6NC. \quad (10)$$

Costul total al topologiei hibride va fi:

$$TC_H = 6CC+3SC+6NC. \quad (11)$$

Vom stabili relațiile dintre costurile controlerului, comutatorului și computerului, după cum urmează:

$$CC = aSC = bNC. \quad (12)$$

Unde parametrii $a = \{a_{min} \div a_{max}\}$ și $b = \{b_{min} \div b_{max}\}$.

După aplicarea acestor valori în ecuațiile (9) ÷ (11) costurile topologiilor vor fi descrise astfel:

$$TC_O = CC+3SC+6NC = CC\,(1+3/a+6/b). \quad (13)$$

$$TC_{S,P} = 3CC+3SC+6NC = 3CC\,(1+1/a+2/b). \quad (14)$$

$$TC_H = 6CC+3SC+6NC = CC\,(6+3/a+6/b). \quad (15)$$

Eficacitatea diferenței de cost la utilizarea topologiilor propuse poate fi exprimată prin următoarele formule:

$$Y1 = TC_{S,P}/TC_O = 3(2a+b+ab)/(6a+3b+ab). \quad (16)$$

$$Y2 = TC_H/TC_O = 3(2a+b+2ab)/(6a+3b+ab). \quad (17)$$

$$Y3 = TC_H/TC_{S,P} = (2a+b+2ab)/(2a+b+ab). \quad (18)$$

Simularea topologiilor controlerelor propuse folosind modulul Rețelelor Petri Stochastic Generalizat.

Folosind modulul GSPN din software-ul PIPE, s-au obținut rezultatele privind numărul mediu de tokene (intensitatea distribuției sau câte tokene există în fiecare loc pe unitatea de timp) în locurile care reprezintă controlerele SDN. Rezultatele sunt afișate în Figura 9.

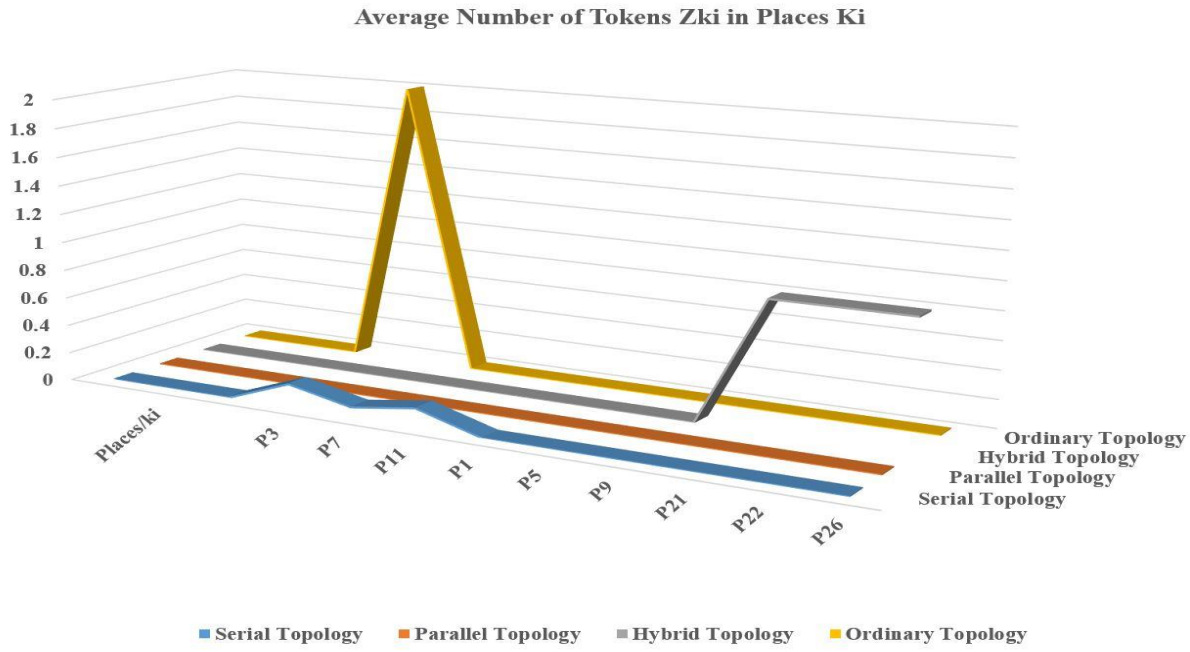

Figura 9. Numărul mediu de tokene în locurile care reprezintă controlerele SDN.

Din datele din Figura 9 se poate concluziona, că cea mai mică cantitate de tokene/cereri pe unitatea de timp se referă la controlorii topologiei paralele, ceea ce înseamnă că acestea vor fi disponibile pentru a trata cele mai multe cereri în timp și asta ar însemna că vor fi mai capabili să contracareze atacurile DoS/DDoS. Prin urmare, se poate spune că cea mai bună topologie dintre toate topologiile propuse ar fi topologia paralela, și cea mai slabă ar fi topologia standard datorită numărului sau cantității mari de tokene și dependenței sale de un singur controler care ar putea fi un punct de eșec.

Determinarea eficienței topologiilor propuse folosind un set de parametri.

Eficiența topologiilor controlorilor elaborați va fi determinată utilizând parametrii fiabilitatea serviciului (*RoS*), factorul de apărare (*DF*), factorul de risc (*RF*), riscul de securitate modificat (*RM*) și efectul de cost (*Y*) descriși mai sus. În Figura 10 sunt prezentate valorile parametrilor topologiilor.

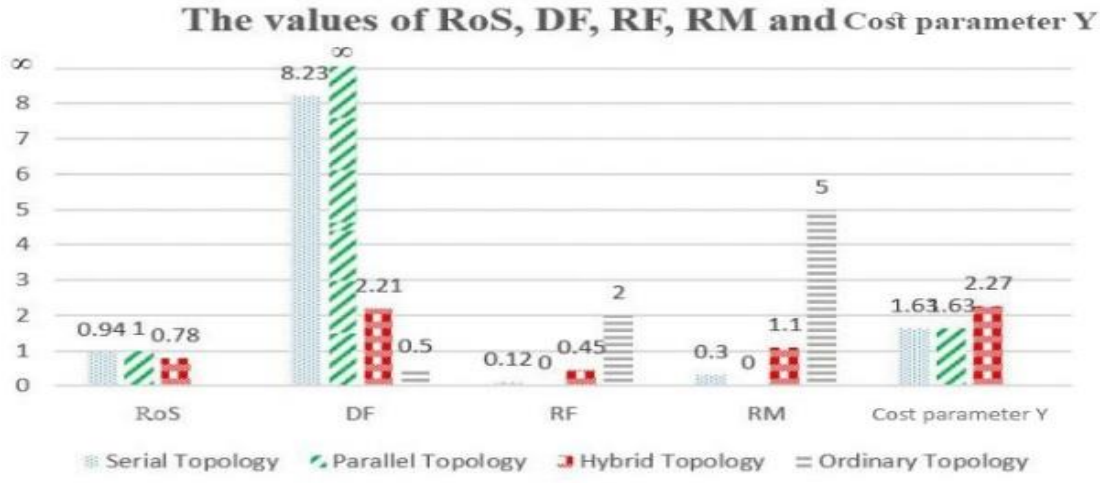

Figura 10. Valorile parametrilor topologiilor propuși.

Din datele prezentate în Figura 10 se poate deduce că topologia Paralelă este cea mai bună din punct de vedere al tuturor parametrilor de estimare a securității, după care vine topologia Serială, și topologia Hibridă este ultima.

Circumstanțele de utilizare ale acestor parametri diferă unele de altele. Atunci când este necesar să se măsoare performanța de protecție a datelor, este rezonabil să se aplice parametrul *RoS*. Parametrul dat al topologiei seriale este de 0,94 în comparație parametrul *RoS* al topologiei standard care conține numai un controler. Topologia paralelă asigură o îmbunătățire de 100% în comparație cu topologia standard, iar topologia hibridă s-a dovedit a fi mai bună decât topologia standard, precum și în ceea ce privește *RoS* prin 0,78. Cu alte cuvinte, se poate spune că cea mai bună topologie dintre toate topologiile propuse în ceea ce privește *RoS*, este topologia paralelă.

Atunci când este necesitate de a determina capacitatea de apărare și rezistența rețelei împotriva atacurilor DoS/DDoS, este aplicabil parametrul *DF*. Pentru topologia paralelă Factorul de Apărare are valoarea foarte mare, apropiată de ∞, deoarece numărul de tokene care reprezintă cereri de rețea în controlerele sale este foarte mic și apropiat de 0. Asta înseamnă că valoarea Factorului de Apărare a acestei topologii este aproape de optimal, ceea ce înseamnă că topologia paralelă este cea mai fiabilă împotriva atacurilor DoS/DDoS. Topologia hibridă are o valoare de 2,21, iar topologia standard are cea mai mică valoare, care este 0,50, ceea ce

înseamnă că topologia cu un singur controler este cea mai slabă structură împotriva atacurilor DoS/DDoS.

Dacă este necesar de a determina nivelul de rezistență a rețelei, este posibil de a utiliza parametrul *RF*, care este invers proporțional cu *DF*. Se poate concluziona că topologia serială are valoarea parametrului de 0,12, valoarea factorului de risc al topologiei paralele este 0, deoarece este aproape optimă și asta înseamnă că această structură are un risc scăzut, topologia hibridă are un factor de risc de 0,45 și topologia standard are cea mai mare valoare de 2.0, ceea ce se referă la riscul mare care apare în timpul utilizării acestei topologii.

În cazul în care a este necesitate de a determina slăbiciunea mediului SDN, atunci este rezonabil de a utiliza parametrul *RM*. Acest parametru reprezintă nivelul asigurării securității topologiilor propuse și a reducerii riscului în comparație cu topologia standard în ceea ce privește evaluarea riscurilor pentru rețelele de calculatoare în general.

Datele arată, că topologia serială are o valoare a parametrului de risc modificat *RM* de 0,3, iar topologia paralelă are o valoare 0, și prin urmare, este cea mai bună topologie dintre toate topologiile elaborate. Valoarea *RM* a topologiei hibride este 1.1, iar topologia cu un singur controler are o valoare de 5.0. Această arată sporirea nivelului de securitate al topologiilor propuse față de topologia standard.

Determinarea efectului de cost al utilizării topologiilor propuse pentru a asigura securitatea paradigmei SDN în comparație cu topologia standard (cu un singur controler) arată, că utilizarea topologiilor seriale și paralele ar putea crește în preț de 1,63 ori. În cazul folosirii topologiei hibride cheltuielile ar putea crește de 2,27 ori mai mult.

Pentru a arăta o eficiență mai detaliată a topologiilor controlerelor SDN propuse, au fost calculate relațiile parametrilor de evaluare a securității noilor topologii în comparație cu topologia standard, după cum urmează. Relația *DF* a topologiilor propuse cu topologia standard $R_{DF} = DF_{pr}/DF_O$, relația *RF* a topologiei standard cu topologiile propuse $R_{RF} = RF_O/ RF_{pr}$, relația RM a topologiei standard cu topologiile propuse $R_{RM} = RM_O/RM_{pr}$. Rezultatele calculelor sunt prezentate în Tabelul 1.

Tabelul 1. Valorile parametrilor topologiilor propuse în comparație cu topologia standard

No.	***Topology***	***RoS***	R_{DF}	R_{RF}	R_{RM}	***Y***
1	Serial Topology	0.94	16.46	16.66	16.66	1.63
2	Parallel Topology	1.0	∞	∞	∞	1.63
3	Hybrid Topology	0.78	4.42	4.44	4.54	2.27

Din Tabelul 1 se poate deduce că topologia serială se caracterizează prin parametrul *RoS* egal cu 0,94, parametrii R_{DF}, R_{RF} și R_{RM} mai mari de 16,46 ori, și mai parametrul *Y* mai mare cu 1,63 ori în comparație cu topologia standard. Topologia paralelă are un *RoS* egal cu 1,0, un parametrii $R_{DF,}$ R_{RF} și R_{RM} apropiați cu ∞, și parametrul *Y* egal cu 1,63 în comparație cu topologia standard. În timp ce topologia hibridă are un *RoS* egal cu 0,78, coeficienții R_{DF} și R_{RF} ă de 4,42 ori, coeficientul R_{RM} egal cu 4,54 și parametrul *Y* egal cu 2,27 în comparație cu topologia standard.

Așa dar, datele arată, că topologia paralelă poate fi caracterizată ca topologia cu cea mai mare valoare de protecție în comparație cu celelalte topologii. În ceea ce privește costul topologiilor propuse, s-a ajuns la concluzia că topologiile Serială și Paralelă necesită creșterea costului de 1,63 ori, iar topologia hibridă - de 2,27 ori față de topologia standard.

Rezultatele matematice obținute sunt preponderent teoretice și se consideră, în mod general acceptat, că împărțirea la zero nu este permisă. Cu toate acestea, având în vedere rezultatele obținute prin simularea software PIPE, a fost imperativ să se efectueze o astfel de operație matematică. Acest fapt demonstrează că topologia paralelă este extrem de fiabilă și aproape optimă.

CONCLUZII GENERALE ȘI RECOMANDĂRI

CONCLUZII GENERALE

Principalele rezultate științifice obținute în cadrul cercetării sunt următoarele.

1. În teză a fost argumentat că rețea definită software este o soluție potențială pentru abordarea amenințărilor cibernetice. A fost evaluată eficiența securității unora dintre cele mai importante tehnici, cercetări și metode legate de SDN, care denotă importanța SDN-ului în tehnologie și capacitatea de a fi încorporat cu alte tehnologii pentru a le îmbunătăți și flexibilitatea SDN-ului de a accepta alte tehnologii în paradigma sa pentru a obține mai multe îmbunătățiri [21].

Această analiză a permis formularea problemelor observate în structura de mediu SDN, cum ar fi centralizarea, în ciuda faptului că controlerele SDN oferă capacitatea de a gestiona mediul de rețea dintr-un singur punct, dar care, de asemenea, ar putea fi considerat un punct vulnerabil dacă este periclitat și utilizat ca un punct unic de defecțiune.

2. Au fost propuși noi algoritmi criptografici integrați în tehnologiile de asigurare a securității SDN. Set de algoritmi constă în principal din arhitectură Hydra și integrat în acesta canalul securizat al algoritmului VPN, algoritmul RSA Dublu și registru distribuit al algoritmului Blockchain. Acești algoritmi funcționează împreună și interacționează pentru a forma comportamentul de tip HIDRA al arhitecturii și pentru a preîntâmpina atacurile Man In The Middle (MITM) și atacurile Denial of Service/ Distributed Denial of Service (DoS/DDoS) [22].

3. Au fost propuse trei tipuri de topologii de controlere SDN: serială, paralelă și hibridă pentru sporirea nivelului de securitate al rețelelor prin adăugarea mai multor controlere care interacționează într-un mod specific, pentru a aborda problema SPOF (Single Point Of Failure) [23], [24], [25].

4. Este propusă noua metodă pentru evaluarea nivelului de securitate a rețelelor de calculatoare, bazată pe utilizarea Rețelelor Petri și a unui set de parametri precum Fiabilitatea Serviciului (*RoS*), Factorul de Apărare (*DF*), Factorul de Risc (*RF*), Factorul de Risc Modificat (*RM*) și Efectul de Cost (*Y*) [26].

5. S-a stabilit că atunci, când este necesară evaluarea performanței de protecție a datelor este posibilă aplicarea parametrului *RoS*. Când este nevoie a determina capacitatea de securitate și puterea rețelei împotriva atacurilor DoS/DDoS, atunci poate fi utilizat parametrul *DF*, iar dacă trebuie determinată vulnerabilitatea rețelei, poate fi utilizat parametrul *RF*. În cazul în care trebuie determinată vulnerabilitatea mediului SDN pe baza rețelelor de calculatoare, se poate utiliza parametrul *RM* [27].

6. A fost realizată modelarea și simularea topologiilor SDN de tip serială, paralelă și hibridă, folosind rețele Petri și Petri Stochastice Generalizate (GSPN). S-a demonstrat că cea mai mică cantitate de tokene/cereri pe unitate de timp se referă la controlerele topologiei paralele, ceea ce înseamnă că acestea vor fi disponibile pentru tratarea cererilor de cele mai multe ori și vor fi mai capabili să preîntâmpine atacurile DoS/DDoS. Prin urmare, putem conchide că cea mai adecvată topologie dintre toate topologiile propuse este topologia paralelă [28], [29].

7. S-a stabilit că topologiile serială și paralelă se caracterizează printr-un cost mai mare de 1,63 ori, iar costul topologiei hibride - de 2,27 ori mai mare în comparație cu topologia standard [30].

Noutatea științifică a cercetării constă în elaborarea de noi algoritmi pentru asigurarea securității SDN-ului, care sunt Hydra, Double RSA și registrul distribuit Blockchain; elaborarea de noi topologii de controlere: seriale, paralele și hibride; elaborarea unei noi metode de evaluare a securității rețelelor de calculatoare bazată pe rețelele Petri și cinci parametri: fiabilitatea serviciului, factorul de apărare, factorul de risc, parametrul modificat de evaluării a riscului și efectul de cost al topologiilor controlorilor SDN propuse.

Valoarea aplicativă a lucrării constă în determinarea arhitecturii dezvoltate, care are o mare importanță în comportamentul SDN prin implementarea de noi topologii SDN pentru a face față problemei centralizării și protejării conexiunii dintre mai multe controlere SDN. De asemenea, oferă o vizualizare mai bună a nivelului de securitate al unei anumite rețele prin evaluarea acesteia, folosind diverse instrumente matematice care se bazează pe parametrii propuși.

RECOMANDĂRI

Cercetarea ar putea fi extinsă mai profund în diferite direcții, cum ar fi:

1. Posibilitatea de utilizare pe larg a parametrilor propuși, capacitatea de evaluare a nivelului de securitate a datelor, a structurii de rețea definită software.

2. Securizarea TLS/SSL împotriva DoS. După cum se știe, controlerul comunică cu switch-urile prin stratul de transport, folosind protocoale precum protocolul openflow.

3. Utilizarea rețelelor neuronale și a inteligenței artificiale pentru a crea un algoritm analitic privind detectarea anomaliilor pe baza statisticilor, iar acest algoritm ar putea fi construit pe o arhitectură care este integrat cu controlerul.

4. Utilizarea extragerii de date pentru a evalua greșelile, problemele, atacurile,

problemele de rețea, erorile de cod și greșelile umane; toate statisticile combinate cu articolul anterior al AI pentru a crea o rețea de calculatoare autosuficientă și auto securizată care utilizează structura SDN.

5. Adăugarea mai multor controlere în topologiile propuse ar putea fi considerată o îmbunătățire, mai ales dacă ar exista mai multe simulări, folosind abordări diferite pentru a obține rezultate mai bune.

REFERINȚE BIBLIOGRAFICE

1. CASADO, M, et. al. Ethane: taking control of the enterprise, In: *ACM SIGCOMM Computer Communication Review*, 2007, 37(4), pp. 1–12.
2. IP knowledge. (2013). traditional VS SDN [whitepaper].
3. SCOTT-HAYWARD, S, O'CALLAGHAN, G, SEZER, S. SDN Security: A Survey. In: *IEEE SDN for Future Networks and Services (SDN4FNS)*, 2013, Centre for Secure Information Technology (CSIT), (10), pp. 1-7.
4. AYESHA, I. SDN controllers' security issues: MS thesis. *University of Jyväskylä* - Finland, 2017.
5. MALIK, A, AHSAN, A, SHAHADAT, M, TSOU, J. Man-in-the-middle-attack: Understanding in simple words. In: *International Journal of Data and Network Science*, 2019, 3, pp. 77-92.
6. PRASAD, K, REDDY, A, RAO, K. DoS and DDoS Attacks: Defense, Detection and Trace Back Mechanisms – A Survey. In: *Global journal of computer science and technology: E Network, Web and Security*, 2014, 14 (7), pp. 15-32.
7. BAWANY, N, SHAMSI, J, SALAH, K. DDoS Attack Detection and Mitigation Using SDN: Methods, Practices, and Solutions. In: *Journal of Cryptology*, 2017, 42, pp. 425-441.
8. OSAGIE, M, ENAGBONMA, O, INYANG, A. the historical perspective of botnet tools. In: *Current Journal of Applied Science and Technology*, 2019, 32 (6), pp. 1-8.
9. CCTV-based botnet used for DDoS attacks. [Online]. [Accessed: 04.07.2017]. Available: https://www.ddosattacks.net/a-massive-botnet-of-cctv-cameras-involved-inferocious-ddos-attacks .
10. IQBAL, M, RIADI, I. Analysis of Security Virtual Private Network (VPN) Using OpenVPN. In: *International Journal of Cyber-Security and Digital Forensics*, 2019, 8 (1), pp. 58-65.
11. TAN, W, et. al. Analysis of RSA based on Quantitating key security strength. In: *Procedia Engineering*, 2011, 15, pp. 1340-1344.
12. How blockchain will manage networks. [Online]. 2019, [accessed: 26.08.2019] available: https://www.networkworld.com/article/3356496/how-blockchain-will-manage-networks.html.
13. **AMEEN, A.** Software - Defined Networks. A General Survey and Analysis, In: *Journal of Engineering Science*, 2018, 25 (3), pp. 61-73.

14. **AMEEN, A.** The Using of SDN Technologies for Security Insurance of Computer Networks, In: proc. of *Technical-Scientific Conference of TUM*, 2019, Technical University of Moldova, 1, pp.1-4.
15. KARAKUS, M, DURRESI, A. Quality of Service (QoS) in Software Defined Networking SDN: A Survey. In: *Journal of Network and Computer Applications*, 2017, 80, pp. 200-218.
16. ALMUTAIRI, L, SHETTY, S. Generalized Stochastic Petri Net Model Based Security Risk Assessment of Software Defined Networks. In: *IEEE Military Communications Conference*, 2017, pp. 545-550.
17. PERJU, V, **AMEEN, A.** State Security Assurance through the Creation of High-Protected Computer Networks, In proc. of *International Conference "Security Strategic Environment: Trends and Challenges SSETC-2019"*, 2021, Armed Forces Military Academy, pp. 101-109.
18. WHITMAN, M, MATTORD, H. Principles of Information Security (book). USA, 2011. 658 p. ISBN-13: 978-1-111-13821-9.
19. Dell Poweredge Servers Special Deals and Offers. [Online]. 2022, [Cited: 02.06.2022] available: https://www.dell.com/en-uk/work/shop/deals/enterprise-deals.
20. Cisco Switch Catalyst 1000. [Online]. 2022, [Cited: 02.06.2022] available: https://www.router-switch.com/cisco-catalyst-1000-switches-price.html.
21. **AMEEN, A.** Leveraging Blockchain Technology to Assure Security of SDN, In: proc. of *International conference on Electronics Communications and computing*, 2020, pp. 1-12.
22. **AMEEN, A.** Making Cyber Space Networks a Safer Work Environment After Covid-19 Using Software-Defined Networks' Technologies, In: proc. of *International scientific conference-evolution of military science in the context of new threats to national and regional security*, 2020, Armed Forces Military Academy, volume 1, pp. 246-260.
23. **AMEEN, A.** Assuring the SDN security by modeling and comparing SDN proposed topologies using Petri Nets. In: *Journal of Engineering Science*, 2021, 28(4), pp. 93-105.
24. **AMEEN, A.** MODELING PROPOSED SDN PARALLEL TOPOLOGY AND EVALUATION OF ITS RELIABILITY. In: *Polish Journal of Science*, 2023, (66), pp. 47-56.
25. **AMEEN, A.** modeling proposed hybrid software-defined network controllers' topology by using Petri Nets system. In: *Studia Universitatis Moldaviae*, 2021, 2(142), pp. 40-50.

26. PERJU, V, Mastac, I, **AMEEN, A.** Modern Military Command and Control Systems and their Security Ensuring based on the SDN technology. In: *Polish Journal of Science*, 2023, (69), pp. 45-51.
27. PERJU, V, **AMEEN, A.** Security Assurance of State-of-the-Art Military Command-and-Control Systems Using the SDN-Based Technologies. In: Proc. of *International Scientific Conference "Republic of Moldova in the context of the new regional security architecture"*, 2022, Armed Forces Military Academy, 1, pp. 169-182.
28. **AMEEN, A**, Guţuleac, E. Petri Nets Modeling for SDN topologies. In: *Journal of Engineering Science*, 2021, 28(2), pp.79-90.
29. **AMEEN, A.** Evaluation of the Computer Networks Security Level Based on Petri Nets & a Set of Parameters. In: *Polish Journal of Science*, 2023, (68), pp. 82-91.
30. PERJU, V, **AMEEN, A.** ASSESSING THE SECURITY OF MILITARY COMPUTER NETWORKS BASED ON THE PETRI NETS MODELING AND A SET OF PARAMETERS. In: Proc. of *International Scientific Conference "The Republic of Moldova in the context of the new regional security architecture"*, 2024, Armed Forces Military Academy (to be published).

LISTA LUCRĂRILOR PUBLICATE

1. AMEEN, A. Software - Defined Networks. A General Survey and Analysis, In: *Journal of Engineering Science*, 2018, 25 (3), pp. 61-73. DOI: https://doi.org/10.5281/zenodo.2557306.
2. AMEEN, A. The Using of SDN Technologies for Security Insurance of Computer Networks, In: proc. of *Technical-Scientific Conference of TUM*, 2019, Technical University of Moldova, 1, pp.1-4. https://ibn.idsi.md/en/vizualizare_articol/84710n.
3. PERJU, V, AMEEN, A. State Security Assurance through the Creation of High-Protected Computer Networks, In proc. Of *the International Conference "Security Strategic Environment: Trends and Challenges SSETC-2019"*, 2021, Armed Forces Military Academy, pp. 101-109.
4. AMEEN, A. Leveraging Blockchain Technology to Assure Security of SDN, In: proc. of *International conference on Electronics Communications and computing*, 2020, Technical University of Moldova, pp. 1-12. DOI: https://doi.org/10.5281/zenodo.4288305.
5. AMEEN, A, GUŢULEAC, E. Petri Nets Modeling for SDN topologies. In: *Journal of Engineering Science*, 2021, 28(2), pp.79-90.
   DOI: https://doi.org/10.52326/jes.utm.2021.28(2).06.
6. AMEEN, A. modeling proposed hybrid software-defined network controllers' topology by using Petri Nets system. In: *Studia Universitatis Moldaviae*, 2021, 2(142), pp. 40-50. DOI: https://doi.org/10.5281/zenodo.5094689.
7. AMEEN, A. Making Cyber Space Networks a Safer Work Environment After Covid-19 Using Software-Defined Networks' Technologies, In: proc. of *International Scientific Conference-Evolution of Military Science in the Context of New Threats to National and Regional Security*, 2020, Armed Forces Military Academy, volume 1, pp. 246-260.
   https://ibn.idsi.md/vizualizare_articol/162231.
8. AMEEN, A. MODELING PROPOSED SDN PARALLEL TOPOLOGY AND EVALUATION OF ITS RELIABILITY. In: *Polish Journal of Science*, 2023, (66), pp. 47-56. https://doi.org/10.5281/zenodo.8337094.
9. AMEEN, A. Assuring the SDN security by modeling and comparing SDN proposed topologies using Petri Nets. In: *Journal of Engineering Science*, 2021, 28(4), pp. 93-105. https://doi.org/10.52326/jes.utm.2021.28(4).08.
10. PERJU, V, Mastac, Ion, AMEEN, A. Modern Military Command and Control Systems and their Security Ensuring based on the SDN Technology. In: *Polish Journal of Science*, 2023, (69), pp. 45-51. DOI: https://doi.org/10.5281/zenodo.10400324.
11. AMEEN, A. Evaluation of the Computer Networks Security Level Based on Petri Nets & a Set of Parameters. In: *Polish Journal of Science*, 2023, (68), pp. 82-91.

DOI: https://doi.org/10.5281/zenodo.10132797.

12. PERJU, V, AMEEN, A. Security Assurance of State-of-the-Art Military Command-and-Control Systems Using the SDN-Based Technologies. In: Proc. of *International Scientific Conference "Republic of Moldova in the context of the new regional security architecture"*, 2023, Armed Forces Military Academy, 1, pp. 169-182.
13. PERJU, V, AMEEN, A. ASSESSING THE SECURITY OF MILITARY COMPUTER NETWORKS BASED ON THE PETRI NETS MODELING AND A SET OF PARAMETERS. In: Proc. of *International Scientific Conference "The Republic of Moldova in the context of the new regional security architecture"*, 2024, Armed Forces Military Academy, (to be published).

ANNOTATION

To the PhD thesis **"Security assurance of the computer networks based on software defined network technologies"** submitted by Mr. Ali AMEEN for fulfillment of the requirements for the PhD in Engineering Sciences, specialty 232.01– Control system, computers and information networks. The dissertation was prepared at the Technical University of Moldova.

The structure of the thesis. The thesis contains Introduction, 3 chapters, general conclusions and recommendations, bibliography of 130 titles. The main text contains 117 pages, includes 47 figures, 23 tables, and 6 annexes. The obtained results of the thesis were published in 13 scientific papers.

Keywords: Software-Defined Networks (SDN), OpenFlow, security, controller, Hydra, virtual private network (VPN), Rivest-Shamir-Adleman (RSA), Blockchain.

Research problem: assuring the security of SDN-based computer networks.

Aim of research is to outline the current security state of the computer networks and to suggest new solutions to patch up different security aspects.

The objectives of thesis include analysis of existing methods and technologies for security assurance of computer networks, elaboration of algorithms and topologies for increasing the security assuring level of computer networks and efficiency evaluation of the proposed topologies for computer network security assuring.

Scientific novelty and originality of the obtained results are reflected in a new framework that assures the security of SDN and uses different techniques combined together to deal with the single point of failure in the SDN architecture, adds a defense mechanism by injecting the attacking source with botnets. And the usage of Petri Nets modeling technique to figure out the best outcome of the proposed topologies and to get different performance parameters that are translated to equations based on that modeling of those specific topologies to determine the one with the best performance in terms of cost saving and deterrence to cyber-threats like DoS/DDoS attacks.

Important scientific solved problem consists in elaboration of a new suite of algorithms and SDN controllers' topologies to increase the security level of SDN and elaboration of the theoretical assessment of computer networks' security level.

Theoretical significance can be described by defining the main problems in security assurance of the computer networks, by specifying the main issues in the SDN paradigm that need to be patched, the theoritization of the essential concepts of the proposed algorithms and topologies.

Applicative value of the work is determined by the developed framework, which has a big contribution for the SDN community by proposing new SDN topologies to deal with the centralization issue and by protecting the connection between multiple SDN controllers. Also, provides a better view for the security level of a specific network by measuring it using various mathematical tools that are based on proposed parameters.

Implementation of results. The obtained results were used in Dekart Company's investigations regarding the new approaches in information security.

ADNOTARE

La teza de doctor **„Asigurarea securitatii retelelor de calculatoare bazate pe tehnologii de rețea definite software”** prezentată de dl Ali AMEEN pentru conferirea titlului științific de doctor în Științe Inginerești la specialitatea 232.01– Sisteme de conducere, calculatoare şi reţele informaţionale. Teza a fost elaborată la Universitatea Tehnică a Moldovei.

Structura tezei. Teza conține Introducere, 3 capitole, concluzii generale și recomandări, bibliografia din 130 de titluri. Textul de bază constituie 117 de pagini, include 47 figuri, 23 tabele și 6 anexe. Rezultatele obținute ale tezei au fost publicate în 13 lucrări științifice.

Cuvinte cheie: Rețele definite prin software (SDN), OpenFlow, controller SDN, Hydra, rețea privată virtuală (VPN), Rivest-Shamir-Adleman (RSA), Blockchain.

Problemă de cercetare: creșterea nivelului de securitate a rețelelor de calculatoare folosind tehnologii bazate pe SDN.

Scopul cercetării este de a sublinia starea actuală de securitate a rețelelor de calculatoare și de a sugera noi soluții pentru a remedia diferite aspecte de securitate.

Obiectivele tezei includ analiza metodelor și tehnologiilor existente pentru asigurarea securității rețelelor de calculatoare, elaborarea algoritmilor și topologiilor pentru creșterea nivelului asigurării securității rețelelor de calculatoare și evaluarea eficienței topologiilor propuse pentru asigurarea securității rețelelor de calculatoare.

Noutatea științifică și originalitatea rezultatelor obținute sunt reflectate într-un cadru nou care asigură securitatea SDN și folosește diferite tehnici combinate pentru a face față punctului unic de eșec în arhitectura SDN, prevede un mecanism de apărare prin injectarea sursei de atac cu botnetele și utilizarea tehnicii de modelare a rețelelor Petri pentru a determina eficacitatea topologiilor propuse și a obține parametri de performanță, utilizați în ecuații bazate pe modelarea topologiilor specifice în ceea ce privește economisirea costurilor și descurajarea amenințărilor cibernetice precum atacurile DoS/DDoS.

Problema științifică importantă rezolvată constă în elaborarea unui nou set de algoritmi și topologii de controlere SDN pentru creșterea nivelului de securitate al SDN și elaborarea metodologiei de evaluare a nivelului de securitate al rețelelor de calculatoare.

Semnificația teoretică reflectă definirea principalelor probleme în asigurarea securității rețelelor de calculatoare, precizarea principalelor probleme din paradigma SDN care trebuie remediate, teoretizarea conceptelor esențiale ale algoritmilor și topologiilor propuse.

Valoarea aplicativă a lucrării este determinată de cadrul dezvoltat, care reprezintă o contribuție importantă pentru comunitatea SDN prin propunerea a câteva noi topologii SDN pentru a trata problema centralizării și protejarea conexiunii dintre mai multe controlere SDN. De asemenea, oferă o vizualizare mai bună a nivelului de securitate al unei anumite rețele prin măsurarea acesteia folosind diverse instrumente matematice care se bazează pe parametri propuși.

Implementarea rezultatelor. Rezultatele obținute au fost utilizate în investigațiile companiei Dekart privind noile abordări în domeniul securității informațiilor.

АННОТАЦИЯ

К докторской диссертации **«Обеспечение безопасности компьютерных сетей на основе программно-определяемых сетевых технологий»** представленной г-ном Али АМЕЕН на соискание ученой степени доктора наук в области Инженерных наук по специальности 232.01 – Системы управления, вычислительная техника и информационные сети. Диссертация была подготовлена в Техническом университете Молдовы.

Структура диссертации: Диссертация содержит введение, 3 главы, общие выводы и рекомендации, библиографию из 130 наименований. Основной текст составляет 117 страниц, включает 47 рисунков, 23 таблиц, и 6 приложений. Полученные результаты диссертации опубликованы в 13 научных работах.

Ключевые слова: программно-определяемые сети (SDN), OpenFlow, контроллер SDN, Hydra, виртуальная частная сеть (VPN), Rivest-Shamir-Adleman (RSA), криптовалюта, блокчейн.

Проблема исследовании: повышение уровня безопасности компьютерных сетей с использованием технологий на базе SDN.

Цель исследования: определить текущее состояние безопасности компьютерных сетей и предложить новые решения для исправления различных аспектов безопасности.

Задачи диссертации включают в себя анализ существующих методов и технологий обеспечения безопасности компьютерных сетей, разработка алгоритмов и топологий для обеспечения безопасности компьютерных сетей и определение параметров оценки эффективности предлагаемых топологий обеспечения безопасности компьютерных сетей.

Научная новизна и оригинальность полученных результатов отражены в новой структуре, которая обеспечивает безопасность SDN и использует различные методы, объединенные вместе, чтобы справиться с единственной точкой отказа в архитектуре SDN, добавляет защитный механизм, вводя атакующий источник с ботнетами, использование метода моделирования сетей Петри для определения наилучшего результата предлагаемых топологий и получения различных параметров производительности, которые используются в уравнениях, основанных на этом моделировании этих конкретных топологий, чтобы определить производительность с учетом экономии затрат и сдерживания киберугроз, таких как DoS/DDoS-атаки.

Важной научной решенной проблемой является разработка нового набора алгоритмов и топологий контроллеров SDN для повышения уровня безопасности SDN и разработка теоретической оценки уровня безопасности компьютерных сетей.

Теоретическая значимость может быть описана путем определения основных проблем в обеспечении безопасности компьютерных сетей, указания основных проблем в парадигме SDN, которые необходимо устранить, теоретизирования основных концепций предлагаемых алгоритмов и топологий.

Практическая ценность работы определяется разработанной структурой, которая представляет собой важный вклад в сообщество SDN, предлагая несколько новых топологий SDN для решения проблемы централизации и защиты соединения между контроллерами SDN. Также обеспечивается лучшая визуализация уровня безопасности конкретной сети путем измерения его с помощью различных математических инструментов, основанных на предлагаемых параметрах.

Внедрение результатов. Полученные результаты были использованы в исследованиях компании Dekart относительно новых подходов к информационной безопасности.

AMEEN ALI

AMEEN Ali

ASIGURAREA SECURITĂȚII REȚELELOR DE CALCULATOARE BAZATE PE TEHNOLOGII DE REȚEA DEFINITE SOFTWARE

Rezumatul tezei de doctor în științe inginerești

SPECIALITATEA 232.01 SISTEME DE CONDUCERE, CALCULATOARE ȘI REȚELE INFORMAȚIONALE

Bun de tipar	Formatul hârtiei 60x84 1/8
Hârtie ofset. Tipar RISO	Tirajul
Coli de tipar 8,0	Comanda

_

MD-2004, Chișinău, bd. Ștefan cel Mare și Sfânt, 168, UTM
MD-2045, Chișinău, str. Studenților, 9/9, Editura „Tehnica-UTM”