MINISTERUL EDUCAŢIEI ŞI CERCETĂRII AL REPUBLICII MOLDOVA
Universitatea Tehnică a Moldovei
Facultatea Electronică şi Telecomunicaţii
Departamentul Telecomunicaţii şi Sisteme Electronice

Admis la susţinere
Şefă departament TSE:
Tîrşu Valentina, conf. univ., dr.

_____

20 ianiarie 2025

Analiza securităţii comunicaţiilor în reţelele optice pasive (PON)

Teză de master

Student: **Tîrnovan Sorin**
gr. SISRC-231M

Conducător: **Şestacova Tatiana**
conf. univ., dr.

Chişinău, 2025

REZUMAT

Autorul: Tîrnovan Sorin gr. **SISRC-231M**

Tema: Analiza securității comunicațiilor în rețelele optice pasive (PON)

Structura lucrării: Lucrarea constă din pagini de titlu, aviz, rezumat, introducere, 3 capitole, concluzii și bibliografie.

Cuvinte cheie: rețele optice pasive, criptare AES, autentificare, securizarea datelor, transmisie de date.

Problematica studiului: Investigarea metodelor de securizare a comunicațiilor în rețelele optice pasive, cu accent pe utilizarea criptării și autentificării pentru a proteja integritatea și confidențialitatea datelor.

Scopul lucrării: Studierea și analiza soluțiilor moderne de securizare a comunicațiilor în rețelele optice pasive (PON), utilizând metode avansate de criptare, autentificare și protecție a datelor împotriva atacurilor cibernetice.

Obiectivele:

1. Prezentare generală a rețelei PON și analiza preliminară;
2. Studierea și analiza protocoalelor și tehnologiilor de securizare a datelor în rețelele PON;
3. Implementarea practică a unui sistem de criptare și decriptare a datelor transmise într-o rețea PON;
4. Investigarea influenței criptării asupra vitezei și latenței transmisiunilor în rețelele optice;
5. Oferirea de recomandări pentru îmbunătățirea securității comunicațiilor în rețelele optice pasive.

Metode aplicate:

În cadrul lucrării s-au utilizat metode analitice pentru analiza securității comunicațiilor, simulări pentru implementarea procesului de criptare și decriptare, precum și metode comparative pentru evaluarea eficienței diferitelor tehnologii de securizare.

Rezultatele obținute:

Lucrarea analizează diverse tehnologii de criptare și autentificare aplicabile rețelelor PON, precum AES (Advanced Encryption Standard) și hash-ul criptografic. Printr-o simulare practică s-a demonstrat procesul de criptare a unui mesaj de către un client și decriptarea acestuia de către un server, exemplificând modul de protejare a datelor într-un mediu optic pasiv. Studiul evidențiază influența metodelor de securizare asupra performanței rețelei și oferă soluții pentru optimizarea acestora. Sunt propuse recomandări specifice pentru îmbunătățirea securității rețelelor PON.

SUMMARY

Author: **Tîrnovan Sorin** gr. **SISRC-231M**

Topic: **Analysis of Communication Security in Passive Optical Networks (PON)**

Thesis structure: The paper consists of a title page, approval page, abstract, introduction, three chapters, conclusions, and bibliography.

Keywords: Passive Optical Networks (PON), AES encryption, authentication, data security, data transmission.

Research problem: The investigation focuses on methods for securing communications in Passive Optical Networks, emphasizing encryption and authentication techniques to protect data integrity and confidentiality.

Purpose of the Work: To study and analyze modern solutions for securing communications in Passive Optical Networks (PON), utilizing advanced methods of encryption, authentication, and data protection against cyber threats.

Objectives:

1. Network PON overview and preliminary analysis;
2. Studying the protocols and technologies for securing data in PON networks;
3. Practical implementation of a data encryption and decryption system for transmissions in a PON network;
4. Investigating the impact of encryption on the speed and latency of transmissions in optical networks;
5. Providing recommendations for improving communication security in passive optical networks.

Methods Used:

The study employs analytical methods for communication security analysis, simulations to implement the encryption and decryption processes, and comparative methods to evaluate the efficiency of different security technologies.

Results Obtained:

The paper explores various encryption and authentication technologies applicable to PONs, such as AES (Advanced Encryption Standard) and cryptographic hashing. A practical simulation demonstrates the encryption of a message by a client and its decryption by a server, showcasing data protection mechanisms in a passive optical environment. The study highlights the impact of security methods on network performance and proposes optimization solutions. Specific recommendations are made to enhance the security of PON.

CUPRINS

INTRODUCERE

În era digitalizării rapide și a creșterii exponențiale a cererii de comunicații de mare viteză, rețelele optice pasive PON *(engl. Passive Optical Networks*) au devenit un pilon central în infrastructurile de telecomunicații. Aceste rețele, utilizate pentru a furniza servicii de internet de mare viteză, televiziune și telefonie, se bazează pe o arhitectură eficientă din punct de vedere al costurilor și al consumului energetic, fapt care le-a făcut extrem de populare în întreaga lume. Rețelele PON permit transmisia datelor prin intermediul fibrei optice, utilizând componente pasive care reduc necesitatea echipamentelor active și cresc fiabilitatea rețelei.

Cu toate acestea, pe măsură ce tehnologia PON devine esențială în infrastructuri critice, cum ar fi cele financiare, guvernamentale și industriale, securitatea comunicațiilor devine un subiect de o importanță majoră. Din cauza arhitecturii lor pasive, care presupune partajarea unei singure fibre opticeîntre mai mulți utilizatori, rețelele PON sunt vulnerabile la interceptarea semnalelor și alte tipuri de atacuri cibernetice. Astfel, asigurarea confidențialității, integrității și disponibilității datelor transmise prin aceste rețele este o provocare care necesită soluții tehnologice inovatoare.

Această lucrare își propune să analizeze securitatea comunicațiilor în rețelele optice pasive (PON), oferind o privire de ansamblu asupra vulnerabilităților existente, precum și a soluțiilor tehnologice disponibile pentru a proteja aceste rețele împotriva amenințărilor. Obiectivele principale ale lucrării sunt de a identifica cele mai frecvente riscuri de securitate asociate rețelelor PON și de a analiza măsurile eficiente care pot fi implementate pentru a le contracara.

Relevanța lucrării este dată de creșterea continuă a numărului de utilizatori și de nevoia stringentă de securitate în contextul actual al atacurilor cibernetice tot mai sofisticate. În plus, pe măsură ce rețelelePON sunt implementate la scară largă în rețelele publice și private, protejarea comunicațiilor devine o provocare pentru a menține funcționalitatea infrastructurilor critice și pentru a preveni scurgerile de date.

Prin urmare, ***scopul*** tezei de master este studierea și analiza soluțiilor moderne de securizare a comunicațiilor în rețelele optice pasive (PON), utilizând metode avansate de criptare, autentificare și protecție a datelor împotriva atacurilor cibernetice.

Pentru a atinge acest scop, este necesar să se rezolve următoarele ***obiective***:

1. Analiza principiilor de funcționare a rețelelor optice pasive PON;.
2. Studierea protocoalelor și tehnologiilor de securizare a datelor în rețelele PON.
3. Implementarea practică a unui sistem de criptare și decriptare a datelor transmise într-o rețea PON.
4. Investigarea influenței criptării asupra vitezei și latenței transmisiunilor în rețelele optice.
5. Oferirea de recomandări pentru îmbunătățirea securității comunicațiilor în rețelele optice pasive.

Prin această cercetare, lucrarea va contribui la o înțelegere mai aprofundată a vulnerabilităților și soluțiilor de protecție pentru rețelele PON, oferind perspective practice și recomandări pentru creșterea rezilienței acestora în fața riscurilor cibernetice actuale.

BIBLIOGRAFIE

1. TÎRȘU, V., CRISTEA E. Baze de date : Ghid metodic pentru lucrările de laborator. Chișinău: Ed. "Tehnica-UTM", 2024, 112 pag. ISBN 978-9975-64-392-4. Disponibil: https://library.utm.md/items/?biblionumber=2628876
2. SAVA, L., VORTOLOMEI, D. Organizarea şi analiza activităţii economice în domeniul telecomunicaţiilor. Note de curs, Chişinău, Editura UTM, 2022, ISBN: 978-9975-45-805-4.
3. NISTIRIUC, P., MIROVSKI, V., CHIHAI, A., ȚURCANU, D., SAVA, L., TÎRȘU, V. Variable Optical Attenuator. In: The 14th International Workshop on Electromagnetic Compatibility (CEM 2024), 18-20 September, 2024, p.30-31, Sibiu, România. https://www.researchgate.net/publication/384635429_Variable_Optical_Attenuator
4. "What is a Passive Optical Network (PON)?" Disponibil: https://www.viavisolutions.com/ru-ru/node/81005 (Postat pe 6 aprilie 2020)
5. "Înțelegeți tehnologia GPON" [09.10.2022] . Disponibil:https://www.cisco.com/c/zh_cn/support/docs/switches/catalyst-pon- series/216230-understand-gpon-technology.html
6. NISTIRIUC, P., ȚURCANU, D., CHIHAI, A., SAVA, L., GRIȚCO, R. Restructurable Optical Attenuator. In: The 14th International Workshop on Electromagnetic Compatibility (CEM 2024), 18-20 September, 2024, p.29, Sibiu, România. https://www.researchgate.net/publication/384635426_Restructurable_Optical_Attenuator
7. Tomas Horvath, Petr Munster,Vaclav Oujezsky Ning-Hai BaoPassive "Optical NetworksProgress" [accesat 2020]. Disponibil: https://www.mdpi.com/2079-9292/9/
8. "Simulation and Performance Analysis of Passive Optical Networks (PONs)" Disponibil:https://www.researchgate.net/publication/333046922_Simulation_and_Performance_Analysis_of_Passive_Optical_Networks_PONs
9. XG-PON Network Scenarios Source: (International Telecommunication Union, 2016). Disponibil: https://www.researchgate.net/figure/G-PON-Network-Scenarios-Source-International-Telecommunication-Union-2016_fig1_344465943
10. "Development of Multicast Service Standardization Regulation for the XG-PON OLT Equipment". Disponibil:https://www.researchgate.net/publication/344465943_Development_of_Multicast_Service_Standardization_Regulation_for_the_XG-PON_OLT_Equipment (septembrie 2020)
11. What is WDM-PON? Disponibil: https://www.fibermall.com/blog/what-is-wdm-pon.htm

12. Iulian Alecu, Costel Ciuchi, Toma Cîmpeanu, et al. Ghid de securitate cibernetică. CentrulNațional de Răspuns la Incidente de Securitate Cibernetică (CERT-RO), 2021. Disponibil: https://anssi.ro/wp-content/uploads/2021/03/Ghid-de-Securitate-Cibernetica.pdf
13. ȚURCANU, D., ȚURCANU, T., NISTIRIUC, A., ANDRONIC, S., CHIHAI, A., NISTIRIUC, P., BAXAN, L., NISTIRIUC, P., ALEXEI, A. Application of external synchronization for increasing noise stability in homodyne reception of optical signals. In: The 22nd International Crimean Conference "Microwave & Telecommunication Technology", 2012, pp. 298-299. https://ieeexplore.ieee.org/abstract/document/6335988
14. Simulation and Performance Analysis of Passive Optical Networks (PONs) Disponibil: https://iceeng.journals.ekb.eg/article_30358_f2afcf44c4b58869e4c8c7b35affd8c4.pdf
15. „40 Channel AWG Module Rack Mount“ Disponibil:https://www.htfwdm.com/optical-network-products/optical-multiplexers/dwdm-mux-demux/40-channel-awg-module-rack-mount.html
16. Conf. dr. Praoveanu Iosif. Securitatea sistemelor informatice - pilon de bază al siguranței.Conferința Telecom, 2018. Disponibil: http://repository.utm.md/bitstream/handle/5014/2813/Conf_Telecom_2018_pg_356_359.pdf
17. "Înțelegeți tehnologia GPON" [09.10.2022]. Disponibil: https://www.cisco.com/c/zh_cn/support/docs/switches/catalyst-pon-series/216230-understand-gpon-technology.html (Postat pe 6 decembrie 2023)
18. "Enhanced Security in Passive Optical Networks using WDM PON". Disponibil: https://www.ijert.org/research/enhanced-security-in-passive-optical-networks-using-wdm-pon-IJERTV3IS041395.pdf (Postat pe 15 aprilie 2023)
19. "Tehnici de criptare. Tendinţe actuale în securitatea informaţiei" Disponibil: https://intelligence.sri.ro/tehnici-de-criptare-tendinte-actuale-securitatea-informatiei (Postat pe 10 iunie 2022)
20. "Tehnologie GPON: Cum funcționează rețeaua FTTH cu fibră optică?" Disponibil: https://itigic.com/ro/gpon-technology-how-does-fiber-optic-ftth-network-work/ (Postat pe 15 iunie 2021)
21. "Evaluarea securităţii fizice pentru reţele şi sisteme de comunicaţii" Disponibil: https://www.agir.ro/buletine/862.pdf (Postat pe 10 martie 2023)
22. "SISTEME DE SECURITATE A REȚELELOR" Disponibil: http://repository.utm.md/bitstream/handle/5014/8598/Conf_TehStiint_UTM_StudMastDoct_2020_Vol_I_pg185-186.pdf?sequence=1 (Postat pe 3 aprilie 2020)

23. "Criptarea RSA vs AES: Explicarea diferențelor dintre chei" Disponibil: https://www.ssldragon.com/ro/blog/rsa-aes-encryption/?utm_source=chatgpt.com
24. "Security in Passive Optical Network via Wavelength Hopping and Codes Cycling Techniques" Disponibil: https://link.springer.com/chapter/10.1007/1-84628-352-3_8 (Postat pe 23 martie 2006)
25. "A Comparison of Passive Optical Network Security" Disponibil: https://www.spiedigitallibrary.org/conference-proceedings-of-spie/7344/1/A-comparison-of-passive-optical-network-security/10.1117/12.818997.full (Postat pe 13 aprilie 2009).