POLITECHNIKA GDAŃSKA

Katedra Teleinformatyki
Tematy prac dyplomowych magisterskich dla kierunku INFORMATYKA
Rok akademicki 2022/2023

1. **Analiza oraz porównanie mechanizmów DPC oraz Poll Mode w odniesieniu do komunikacji karty sieciowej z systemem operacyjnym MAN**
2. **Analiza porównawcza rozszerzeń bezpieczeństwa standardu DNS**
3. **Analiza porównawcza rozwiązań zwiększających niezawodność systemów chmurowych**
4. **Analiza porównawcza wybranych podatności urządzeń podłączanych do Internetu wraz z propozycją dobrych praktyk w zakresie zabezpieczeń i minimalizacji ryzyka.**
5. **Analiza sprawiedliwości indywidualnej i systemowej w sieciach komputerowych**
6. **Arbitracja dostępu do chmury publicznej z wykorzystaniem wirtualnej domeny kolizyjnej**
7. **Badania skuteczności zgodnych motywacyjnie systemów reputacyjnych w wybranych środowiskach teleinformatycznych w warunkach zmowy grup podmiotów**
8. **Badania symulacyjne mechanizmów obrony mobilnych sieci bezprzewodowych o topologii wieloskokowej przed inteligentnymi atakami metodą podmiany klasy ruchu**
9. **Mechanizmy komunikacji sieciowej w środowisku Kubernetes**
10. **Mechanizmy monitorowania w środowisku OpenStack**
11. **Mechanizm budowy zaufania dla ochrony przed atakami metodą fałszywego VIPa w systemach teleinformatycznych wspierających różnicowanie jakości usług**
12. **Model symulacyjny mechanizmu reputacyjnego RISC2WIN dla dwuskokowej kooperatywnej komunikacji bezprzewodowej z różnicowaniem jakości usług**
13. **Ocena możliwości manipulacji w systemach reputacyjnych stosowanych w wybranych środowiskach teleinformatycznych**
14. **Optymalizacja rozmieszczania kontrolerów SDN w celu przeciwdziałania atakom skierowanym na węzły sieci**
15. **Projekt architektury i ocena wybranych charakterystyk wydajności sieci korporacyjnej**

Temat 1	**Analiza oraz porównanie mechanizmów DPC oraz Poll Mode w odniesieniu do komunikacji karty sieciowej z systemem operacyjnym MAN**
Temat w języku angielskim	Analysis and comparison of DPC and Poll Mode mechanism in relation to the communication of network adapter with the operating system
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest porównanie wydajności karty sieciowej przy wykorzystaniu mechanizmu DPC (Deffered Procedure Call) vs Poll Mode do komunikacji z systemem operacyjnym Windows.
Zadania	1. Analiza oraz opis mechanizmu DPC 2. Analiza oraz opis mechanizmu Poll Mode 3. Implementacja obejmująca zmianę mechanizmu komunikacji DPC na Poll Mode w sterowniku do karty sieciowej Intel 4. Konfiguracja i opis środowiska pod testy wydajnościowe - m.in ustawienia RSS (Recieve Side Scaling) 5. Porównanie wydajności karty sieciowej przy mechaniźmie DPS vs Poll Mode
Literatura	1. Brendan Gregg: Systems Performance, 2nd Edition, wydawnictwo Pearson, 2020. 928s. 2. Robert C. Martin: Clean Architecture, wydawnictwo Pearson, 2017. 423s. 3. Clint Huffman: Windows Performance Analysis Field Guide, wydawnictwo Syngress, 2014. 380s. 4. Microsoft: Introduction to DPC (https://docs.microsoft.com/en-us/windows-hardware/drivers/kernel/introduction-to-dpc-objects) 5. Microsoft: Poll overview (https://docs.microsoft.com/en-us/windows-hardware/drivers/ddi/poll/)
Proponowana liczba osób	1
Informacje dodatkowe	Badania mechanizmów DPC oraz Poll Mode zdefiniowanych przez firmę Microsoft winny zostać prowadzone na systemie Windows, zaś wydajność (przepustowość karty, wykorzystanie procesora, itd.) porównywana na kartach 40Gb/s (lub 100Gb/s)
Komentarz	
Studia	Informatyka stacjonarne II stopnia

Temat 2	**Analiza porównawcza rozszerzeń bezpieczeństwa standardu DNS**
Temat w języku angielskim	A comparative analysis of security extensions of the DNS standard
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest wykonanie analizy porównawczej rozszerzeń bezpieczeństwa systemu DNS obejmującej funkcjonalność, wpływ na wydajność i łatwość wdrożenia. Część eksperymentalna powinna obejmować praktyczne przykłady wdrożenia zależnego od zastosowania.
Zadania	1. Przegląd rozszerzeń bezpieczeństwa systemu DNS. 2. Praktyczne wdrożenie poszczególnych rozszerzeń. 3. Wielokryterialna analiza porównawcza. 4. Wnioski
Literatura	Dokumenty RFC dotyczące usługi DNS: RFC1034, RFC1035 z aktualizacjami Dokumenty RFC dotyczące DNSEC: RFC4033, RFC4034, RFC4035 z aktualizacjami Dokumenty RFC dotyczące DoT DNS over TLS: RFC7875, RFC8310 Dokumenty RFC dotyczące DoH DNS over HTTPS: RFC8484 Dokumentacja propozycji rozszerzeń DoQ i DoH3 dostawców Cloudflare i NextDNS.
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka stacjonarne II stopnia

Temat 3	**Analiza porównawcza rozwiązań zwiększających niezawodność systemów chmurowych**
Temat w języku angielskim	Comparative analysis of mechanisms improving resilience of cloud-based systems
Opiekun pracy	dr hab. inż. Jacek Rak
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest przeprowadzenie możliwie szerokiego przeglądu mechanizmów podnoszenia niezawodności systemów chmurowych wraz z analizą zagrożeń, jak i przeprowadzenie badań ukierunkowanych na opracowanie zbioru „dobrych praktyk”.
Zadania	• przegląd literatury odnośnie istniejących metod podnoszenia niezawodności systemów chmurowych • konfiguracja i ocena właściwości wybranych rozwiązań • opracowanie zbioru „dobrych praktyk” na podstawie uzyskanych wyników
Literatura	· Colman-Meixner, C., Develder, Ch., Tornatore, M., Mukherjee, B.: A survey on Resiliency Techniques in Cloud Computing Infrastructures and Applications, IEEE Communications Surveys & Tutorials, 18(3), 2244-2281 (2016) · R. de Souza Couto, S. Secci, M. Mitre Campista, L. Costa: Network Design Requirements for Disaster Resilience in IaaS Clouds, IEEE Communications Magazine, 52-58, October 2014 · przegląd literatury odnośnie istniejących metod podnoszenia niezawodności systemów chmurowych · konfiguracja i ocena właściwości wybranych rozwiązań opracowanie zbioru „dobrych praktyk” na podstawie uzyskanych wyników
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

Temat 4	**Analiza porównawcza wybranych podatności urządzeń podłączanych do Internetu wraz z propozycją dobrych praktyk w zakresie zabezpieczeń i minimalizacji ryzyka.**
Temat w języku angielskim	Comparative analysis of selected vulnerabilities in Internet facing devices with recommendation of best practices in terms of hardening and risk mitigation.
Opiekun pracy	dr inż. Wojciech Gumiński
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest wykonanie możliwie szerokiego przeglądu podatności urządzeń podłączanych do Internetu wraz z analizą zagrożeń i opisem dobrych praktyk minimalizujących ryzyka.
Zadania	1. Przegląd stanu wiedzy. 2. Omówienie metod wykrywania urządzeń podłączonych do Internetu oraz skanowania pasywnego i aktywnego pod kątem identyfikacji podatności. 3. Porównanie najpopularniejszych podatności oraz możliwości wykorzystania ich przez atakujących. 4. Propozycja dobrych praktyk w zakresie zabezpieczeń i minimalizacji ryzyka. 5. Praktyczny przykład wdrożenia proponowanych zabezpieczeń. 6. Wnioski.
Literatura	Mutemwa and F. Mouton, "Cyber security threats and mitigation techniques for multifunctional devices," 2018 Conference on Information Communications Technology and Society (ICTAS), 2018, pp. 1-6, doi: 10.1109/ICTAS.2018.8368745. Albataineh and I. Alsmadi, "IoT and the Risk of Internet Exposure: Risk Assessment Using Shodan Queries," 2019 IEEE 20th International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), 2019, pp. 1-5, doi: 10.1109/WoWMoM.2019.8792986. Dokumentacja projektu OWASP TOP 10 https://owasp.org/www-project-top-ten/ Dokumentacja platformy Shodan Dokumentacja oprogramowania nmap
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka niestacjonarne II stopnia

Temat 5	**Analiza sprawiedliwości indywidualnej i systemowej w sieciach komputerowych**
Temat w języku angielskim	Analysis of individual and system fairness in computer networks
Opiekun pracy	dr inż. Krzysztof Nowicki
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest ocena użyteczności miar sprawiedliwości przydziału zasobów, w szczególności do oceny sprawiedliwości indywidualnej
Zadania	1. Zapoznanie z problemami zapewniania sprawiedliwości w sieciach komputerowych, w szczególności miarami sprawiedliwości 2. Wybór mechanizmów zapewniania sprawiedliwości w sieciach 3. Przegląd dostępnych środowisk symulacyjnych 4. Wybór środowiska symulacyjnego 5. Zaprojektowanie i implementacja mechanizmów sprawiedliwości w środowisku symulacyjnym i ocena ich jakości pod kątem sprawiedliwości indywidualnej i systemowej
Literatura	1. Shi H., Prasad V., Onur E., Niemegeers I.G.M.M.: Fairness in Wireless Networks - Issues, Measures and Challenges, *IEEE Communications Surveys and Tutorials*, pp. 5-24, 2013, PDF. 2. Antkiewicz J., Sznyter B.: Projekt i implementacja symulatora sieci pierścieniowej, praca inżynierska WETI PG 2018 3. Nowicki K., Malinowski A., Sikorski M..: More Just Measure of Fairness for Sharing Network Resources, W: 23rd International Conference on Computer Networks (CN), 2016, Springer 4. Mazur I., Rak J., Nowicki K.: Minimising the Churn Out of the Service by Using a Fairness Mechanism// Computer Networks/ : Springer, 2020, s.117-137 5. Mazur I., Rak J., Nowicki K.: Ensuring the QoE-Related Fairness to Reduce the User Abandonment Ratio// SENSORS -Vol. 21,iss. 21 (2021), s.7050 Zasoby Internetu
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka stacjonarne II stopnia

Temat 6	**Arbitracja dostępu do chmury publicznej z wykorzystaniem wirtualnej domeny kolizyjnej**
Temat w języku angielskim	**Arbitrated access to a public cloud through a virtual collision domain**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Recenzent	
Cel pracy	Dla ograniczania skutków ataków EDoS na systemy chmurowe mechanizmy admisji wymagają rozróżniania uczciwych i nieuczciwych wywołań klienckich przy pomocy testów Turinga lub protokołów wyzwania i odpowiedzi. Wymaga to kalibracji a priori stopnia trudności testu/wyzwania i faworyzuje klientów dysponujących szybkim sprzętem obliczeniowym. Celem projektu jest stworzenie alternatywnego mechanizmu admisji zmuszającego klientów do rozegrania odpowiednio zaprojektowanej gry w wojnę na wyniszczenie.
Zadania	1. Opis i analiza wpływu metod ochrony przed atakiem EDoS na przykładzie wybranego środowiska chmurowego. 2. Opracowanie mechanizmu wirtualnej domeny kolizyjnej i projekt powiązania uporczywości wywołań klienckich z wielkością żądanych zasobów chmury. 3. Ocena sprawiedliwości dostępu i odporności na ataki EDoS.
Literatura	1. K. Bhushan, B.B. Gupta, *Network flow analysis for detection and mitigation of Fraudulent Resource Consumption (FRC) attacks in multimedia cloud computing*, Multimed Tools Appl, 2019 2. F. Z. Chowdhury, L. B. M. Kiah, M. M. Ahsan, *Economic Denial of Sustainability (EDoS) Mitigation Approaches in Cloud: Analysis and Open Challenges*, Proc. ICECOS 2017 3. M.A.S. Monge, J.M. Vidal, G.M. Pérez, *Detection of economic denial of sustainability (EDoS) threats in self-organizing networks*, Computer Communications 145, 2019. 4. J. Konorski, *Ad Hoc WLAN with Selfish, Secretive, and Short-Sighted Stations*, ISABEL 2009.
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

Temat 7	**Badania skuteczności zgodnych motywacyjnie systemów reputacyjnych w wybranych środowiskach teleinformatycznych w warunkach zmowy grup podmiotów**
Temat w języku angielskim	**Investigation of the effectiveness of incentive compatible reputation systems in selected computer communication settings under collusion of groups of entities**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest przebadanie zasad i protokołów współpracy autonomicznych agentów racjonalnych zapewniających prawdomówność raportowania o zaobserwowanych zachowaniach innych agentów.
Zadania	1. Specyfikacja protokołów współpracy agentów. 2. Budowa modelu symulacyjnego w środowisku sieci bezprzewodowych oraz społecznościowych 3. Ocena wpływu rzeczywistych parametrów środowiska na skuteczność wybranych protokołów współpracy agentów.
Literatura	1. Jurca R., B. Faltings, *An incentive compatible reputation mechanism*, Proc. 2nd AAMAS, 2003 2. Jurca R., B. Faltings, *Collusion-resistant, incentive-compatible feedback payments*, Proc. 8th ACM Conf. on Electronic Commerce, 2007 3. Miller N., P. Resnick, R. Zeckhauser, *Eliciting informative feedback: the peer-prediction method*, *Management Science* vol. 51, 2005 4. J. Konorski, *Reputacja i zaufanie w systemach teleinformatycznych z podmiotami anonimowymi - podejście dynamiczne*, Przegląd Telekomunikacyjny, t. LXXXIX, 2016
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

Temat 8	**Badania symulacyjne mechanizmów obrony mobilnych sieci bezprzewodowych o topologii wieloskokowej przed inteligentnymi atakami metodą podmiany klasy ruchu**
Temat w języku angielskim	**Simulation study of defense mechanisms against intelligent traffic remapping attacks in multi-hop mobile wireless networks**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest zbadanie, czy ataki na poziomie podwarstwy MAC mogą mieć zasięg większy niż najbliższe sąsiedztwo węzła atakującego oraz symulacyjna ocena efektów takich ataków i skuteczności wybranych mechanizmów obronnych w warunkach mobilności węzłów sieci.
Zadania	1. Zapoznanie się z metodami wsparcia QoS w sieciach bezprzewodowych o topologii wieloskokowej oraz sposobami ich wykorzystanie przez węzły atakujące 2. Opracowanie symulacyjnego modelu ataku wykorzystującego mechanizm EDCA 3. Opracowanie symulacyjnego modelu sieci z atakami na wiele przepływów pakietowych 4. Symulacja wybranych strategii ataków i ocena skuteczności obronnej mechanizmów sterowania ruchem
Literatura	1. J. Konorski, S. Szott, Discouraging traffic remapping attacks in local ad hoc networks, IEEE Trans Wireless Communications, 2014, 3752-3767. 2. R. Haywood, S. Mukherjee, X.-H. Peng, Investigation of H.264 Video Streaming over an IEEE 802.11e EDCA Wireless Testbed, IEEE International Conf. on Communications, 2009. 3. S. Szott, M. Natkaniec, A. R. Pach, Improving QoS and security in wireless ad hoc networks by mitigating the impact of selfish behaviors: a game-theoretic approach, Security and Communication Networks 6 (2013) 509-522. 4. Inne materiały źródłowe dostępne u opiekuna
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

Temat 9	**Mechanizmy komunikacji sieciowej w środowisku Kubernetes**
Temat w języku angielskim	Networking mechanisms in Kubernetes cluster
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Recenzent	
Cel pracy	Środowisko klastra Kubernetes oferuje możliwość orkiestracji kontenerów zlokalizowanych na szeregu węzłów fizycznych. Wiąże się z tym konieczność utrzymania komunikacji sieciowej pomiędzy utworzonymi kontenerami (a także innymi typami zasobów, jak np. pody i usługi) oraz pomiędzy kontenerami a elementami zlokalizowanymi na zewnątrz klastra Kubernetes. Celem pracy jest dokonanie przeglądu architektury i funkcjonalności mechanizmów sieciowych oferowanych przez środowisko Kubernetes oraz wskazanie ich zalet i wad we właściwych dla powyższego środowiska scenariuszach wykorzystania.
Zadania	• Przegląd i analiza scenariuszy komunikacji sieciowej w środowisku klastra Kubernetes. • Przegląd i analiza architektury i funkcjonalności mechanizmów komunikacji sieciowej klastra Kubernetes. • Przygotowanie i przetestowanie działania powyższych mechanizmów w środowisku laboratoryjnym (np. w postaci demonstratora).
Literatura	• Dokumentacja środowiska Kubernetes • James Strong, Vallery Lancey, Networking and Kubernetes, O'Reilly Media, Inc., 2021
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

Temat 10	**Mechanizmy monitorowania w środowisku OpenStack**
Temat w języku angielskim	Monitoring solutions for OpenStack environment
Opiekun pracy	dr inż. Krzysztof Gierłowski
Konsultant pracy	
Recenzent	
Cel pracy	Środowisko OpenStack stanowi kompleksowe rozwiązanie pozwalające na uruchomienie, utrzymanie i praktyczne wykorzystanie środowiska chmurowego oferującego zróżnicowane zasoby wirtualne. Ponieważ jednym z kluczowych zadań niezbędnych w tym procesie jest szeroko pojęte monitorowanie elementów utworzonego systemu (infrastruktury, procesów utrzymaniowych, udostępnianych zasobów, itp.) OpenStack oferuje rozwiązania przeznaczone do tego celu. Celem pracy jest dokonanie analizy potrzeb i scenariuszy dotyczących monitorowania, obecnych w nowoczesnych systemach chmurowych oraz porównanie ich z funkcjonalnością i rozwiązaniami oferowanymi przez elementy systemu OpenStack.
Zadania	• Przegląd i analiza potrzeb dotyczących monitorowania elementów systemu chmurowego oraz popularnych sposobów realizacji związanych z nim zadań. • Przegląd i analiza elementów systemu OpenStack związanych z procesem szeroko pojętego monitorowania. • Przygotowanie i przetestowanie działania mechanizmów monitorowania systemu OpenStack w środowisku laboratoryjnym (np. w postaci demonstratora).
Literatura	• Dokumentacja systemu OpenStack. • Omar Khedher, Chandan Dutta Chowdhury, Mastering OpenStack, Packt Publishing, 2017
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

POLITECHNIKA GDAŃSKA

Temat 11	**Mechanizm budowy zaufania dla ochrony przed atakami metodą fałszywego VIPa w systemach teleinformatycznych wspierających różnicowanie jakości usług**
Temat w języku angielskim	**A trust building mechanism to defend against Fake VIP attacks in computer communication systems supporting QoS differentiation**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Recenzent	
Cel pracy	W systemach teleinformatycznych wspierających różnicowanie jakości usług (QoS) atak metodą fałszywego VIPa jest odmianą niewykrywalnej uzurpacji uprawnień. W obliczu żądania usług mogącego być częścią takiego ataku agent IDS ma do wyboru uruchomienie kosztownej procedury weryfikacji sygnatury ataku (np. DPI - *deep packet inspection*), bądź okazanie zaufania i przydział żądanego poziomu QoS. IDS dąży do jednoczesnego ograniczenia kosztu DPI oraz częstości przydziału nienależnie wysokiego poziomu QoS, zaś atakujący intruz - do możliwie częstego przydziału nienależnie wysokiego poziomu QoS. Celem pracy jest eksperymentalne zbadanie skuteczności mechanizmu zaufania w IDS dyktującego decyzje o uruchomieniu DPI dla kolejnych żądań usług.
Zadania	1. Opis mechanizmu ataku metodą fałszywego VIPa w różnych środowiskach sieciowych 2. Analiza możliwych mechanizmów obronnych oraz ich penetracji przez racjonalnego intruza ze zdolnością uczenia się 3. Sformułowanie modelu agenta IDS, intruza i systemu komunikacyjnego oraz pozyskanie zbiorów danych wejściowych do eksperymentów 4. Analiza skuteczności systemu budowy zaufania w warunkach stabilnej generacji żądań usług i pracy systemu komunikacyjnego.
Literatura	1. Y. L. Sun, Y. Liu, *Security of online reputation systems: The evolution of attacks and defenses*, IEEE Signal Proc. Mag., vol. 29, 2012 2. Po-Ching Lin et al., *Using String Matching for Deep Packet Inspection*, Computer, vol. 41, 2008 3. Patcha, Jung-Min Park, *A Game Theoretic Formulation for Intrusion Detection in Mobile Ad Hoc Networks*, Int. J. of Network Security, vol. 2, 2006. 4. T. Grandison and M. Sloman, *A survey of trust in internet applications*, IEEE Comm. Surveys & Tutorials, vol. 3, 2000. 5. P. L. Bartlett, *Online Prediction*. 2015, stat.berkeley.edu/~bartlett/papers/b-ol-16.pdf 6 Y. Freund et al., *Efficient Algorithms for Learning to Play Repeated Games Against Computationally Bounded Adversaries*, Proc. 36th Annual Symp. Foundations of Computer Science, 1995.
Proponowana liczba osób	1

Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

Temat 12	**Model symulacyjny mechanizmu reputacyjnego RISC2WIN dla dwuskokowej kooperatywnej komunikacji bezprzewodowej z różnicowaniem jakości usług**
Temat w języku angielskim	**Simulation model of the RISC2WIN reputation mechanism for two-hop wireless cooperative communications with QoS differentiation**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest opracowanie i implementacja modelu symulacyjnego mechanizmu budowania reputacji jako gwaranta uczciwego różnicowania jakości usług (QoS) przez stację pośredniczącą w dwuskokowej sieci bezprzewodowej.
Zadania	1. Wybór narzędzia symulacyjnego 2. Specyfikacja i implementacja mechanizmu w wybranym narzędziu symulacyjnym 3. Symulacja gry strategicznej pomiędzy stacją pośredniczącą i końcową 4. Wykonanie demonstratora zasilanego sztucznym źródłem ruchu webowego i VoIP
Literatura	1. S. Szott and J. Konorski, "Selfish attacks in two-hop IEEE 802.11 relay networks: impact and countermeasures," IEEE Wireless Comm. Letters, DOI: 10.1109/LWC.2018.2809726. 2. A. Garcia-Saavedra, B. Rengarajan, P. Serrano, D. Camps-Mur, and X. Costa-Pérez, "SOLOR: self-optimizing WLANs with legacy-compatible opportunistic relays," IEEE/ACM Trans. on Networking, vol. 23, no. 4, pp. 1202-1215, Aug. 2015. 3. B. Jedari, F. Xia and Z. Ning, "A Survey on Human-Centric Communications in Non-Cooperative Wireless Relay Networks," IEEE Communications Surveys & Tutorials, vol. 20, no. 2, pp. 914-944, 2018. 4. A. Malik, J. Qadir, B. Ahmad, K.-L. Alvin Yau, and U. Ullah, "QoS in IEEE 802.11-based wireless networks: a contemporary review," Journal of Network and Computer Applications, vol. 55, pp. 24-46, 2015. 5. inne materiały źródłowe dostępne u opiekuna
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

POLITECHNIKA GDAŃSKA

Temat 13	**Ocena możliwości manipulacji w systemach reputacyjnych stosowanych w wybranych środowiskach teleinformatycznych**
Temat w języku angielskim	**Feasibility study of reputation system manipulation in selected computer communication settings**
Opiekun pracy	dr hab. inż. Jerzy Konorski
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest przebadanie zasad i protokołów współpracy autonomicznych agentów racjonalnych opartych na generowaniu danych reputacyjnych ze szczególnym uwzględnieniem możliwości odwrócenia hierarchii uczciwości agentów.
Zadania	1. Specyfikacja protokołów zbierania przetwarzania danych reputacyjnych. 2. Budowa modelu symulacyjnego agentów o zróżnicowanym stopniu uczciwości w wybranym środowisku teleinformatycznym 3. Ocena wpływu rzeczywistych parametrów środowiska na skuteczność manipulacji w systemie reputacyjnym
Literatura	1. Y. L. Sun, Y. Liu, *Security of online reputation systems: The evolution of attacks and defenses*, IEEE Signal Proc. Mag., vol. 29, 2012 2. Miller N., P. Resnick, R. Zeckhauser, *Eliciting informative feedback: the peer-prediction method*, *Management Science* vol. 51, 2005 3. J. Konorski, *Reputacja i zaufanie w systemach teleinformatycznych z podmiotami anonimowymi - podejście dynamiczne*, Przegląd Telekomunikacyjny, t. LXXXIX, 2016
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia

POLITECHNIKA GDAŃSKA

Temat 14	**Optymalizacja rozmieszczania kontrolerów SDN w celu przeciwdziałania atakom skierowanym na węzły sieci**
Temat w języku angielskim	**Optimization of SDN controllers' placement against node-targeted attacks**
Opiekun pracy	prof. dr hab. inż. Michał Pióro
Konsultant pracy	
Recenzent	
Cel pracy	W sieciach definiowanych programowo (SDN – *software defined networks*) utrata dostępu do kontrolera (*controller node*) przez węzeł sieci (*switching node*) powoduje znaczną degradację jego funkcjonalności. Dlatego też minimalizacja liczby węzłów, które tracą taki dostęp w wyniku celowego ataku na wybrany przez atakującego podzbiór węzłów (w tym kontrolerów) jest istotnym problemem, przed którym stają operatorzy sieci. Jednym z najważniejszych środków rozwiązywania tego problemu jest optymalizacja rozmieszczania w sieci założonej liczby kontrolerów dla zadanej (przewidywanej) klasy ataków. Celem pracy będzie weryfikacja następującej hipotezy badawczej: właściwe rozmieszczenie kontrolerów SDN pozwala znacznie osłabić skutki ataków ukierunkowanych na węzły sieci.
Zadania	Realizacja pracy dyplomowej będzie polegała na opracowaniu modelu optymalizacyjnego pozwalającego na znajdowanie rozmieszczeń kontrolerów SDN minimalizujących skutki ataków z zadanej klasy. Model taki oparty będzie na sformułowaniach odpowiedniego problemu w języku programowania całkowitoliczbowego oraz na jego rozwiazywaniu za pomocą pakietu optymalizacyjnego CPLEX.
Literatura	[1] Mariusz Mycek, Michal Pióro, Artur Tomaszewski, Amaro de Sousa: Optimizing primary and backup controllers' placement resilient to node-targeted attacks, 17th International Conference on Network and Service Management (CNSM), 2021. [2] Eusebi Calle, David Martínez, Mariusz Mycek, Michał Pióro: Resilient backup controller placement in distributed SDN under critical targeted attacks, International Journal of Critical Infrastructure Protection, vol. 33, 2021.
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	Bardzo ciekawa tematyka dla osób zainteresowanych optymalizacją sieci teleinformatycznych za pomocą metod programowania liniowego i całkowitoliczbowego. Możliwe jest wykonywanie pracy opisanej powyżej w zespole dwuosobowym.
Studia	Informatyka stacjonarne II stopnia

Temat 15	**Projekt architektury i ocena wybranych charakterystyk wydajności sieci korporacyjnej**
Temat w języku angielskim	Architecture design and verification of selected characteristics of performance of a corporate network
Opiekun pracy	dr hab. inż. Jacek Rak
Konsultant pracy	
Recenzent	
Cel pracy	Celem pracy jest zaprojektowanie architektury sieci korporacyjnej oraz poddanie szerszej analizie wybranych aspektów jej wydajności.
Zadania	1. Przegląd literatury odnośnie metod projektowania sieci korporacyjnych ze szczególnym uwzględnieniem aspektów wydajności 2. Opracowanie rozwiązania własnego / modyfikacji metody referencyjnej 3. Ocena właściwości rozwiązania własnego
Literatura	Artykuły z bazy IEEE Xplore, np. 1) N. Vinogradov and A. Savchenko, "Impact of Network Control System Performance on Efficiency of Large Corporate Network," 2019 3rd International Conference on Advanced Information and Communications Technologies (AICT), 2019, pp. 195-199, doi: 10.1109/AIACT.2019.8847838. 2) M. Wairisal and N. Surantha, "Design and Evaluation of Efficient Bandwidth Management for a Corporate Network," 2018 International Conference on Information Management and Technology (ICIMTech), 2018, pp. 98-102, doi: 10.1109/ICIMTech.2018.8528162.
Proponowana liczba osób	1
Informacje dodatkowe	
Komentarz	
Studia	Informatyka II stopnia