Отже, дослідження атак на SDN-орієнтовані системи керування мережею є актуальним, оскільки централізація функцій адміністрування, моніторингу та керування трафіком підвищує критичність контролера як об'єкта захисту. На прикладі Omada Controller показано, що використання лише готових наборів пакетів не завжди забезпечує достовірність результатів, адже вони можуть не враховувати особливості конкретної топології, службової взаємодії пристроїв і реальних умов експлуатації. Запропонована експериментальна схема дає змогу формувати власний набір даних, фіксувати нормальний та атакувальний трафік у ключових точках мережі й створює основу для подальшої розробки методів виявлення аномалій та протидії атакам на системи централізованого керування мережею.

1. Mansoor, A., Anbar, M., Bahashwan, A. A., Alabsi, B. A., & Rihan, S. D. A. (2023). Deep Learning-Based Approach for Detecting DDoS Attack on Software-Defined Networking Controller. Systems, 11(6), 296. https://doi.org/10.3390/systems11060296

Дослідження вразливостей протоколів динамічної маршрутизації

УДК 004.056.

Сергій Мостовий[1], Сергій Савченко[2]

Хмельницький національний університет,
[1]serhii.mostovyi@khmnu.edu.ua, [2]sserggii@yahoo.com

Корпоративні мережі постійно піддаються впливу різноманітних загроз, які можуть призвести до порушення конфіденційності, цілісності або доступності мережевих сервісів. У контексті динамічної маршрутизації ці загрози мають критичне значення, оскільки впливають на механізми обміну маршрутною інформацією, що є основою функціонування будь-якої IP-мережі. Завдяки використанню динамічних протоколів маршрутизації, таких як RIP, OSPF, IS-IS, EIGRP, та BGP [1,3], забезпечується автоматичне оновлення таблиць маршрутизації в реальному часі, що дозволяє адаптувати мережу до змін. Однак, ці самі властивості роблять протоколи маршрутизації вразливими до різноманітних атак, що можуть порушити їхню функціональність і безпеку.

Загрози у корпоративних мережах можна умовно класифікувати на кілька груп, кожна з яких стосується певних аспектів функціонування мережі.

Перша група загроз стосується маршрутизаторів та мережевого обладнання. Ці загрози включають атаки, метою яких є виведення маршрутизатора з ладу або отримання доступу до його конфігурації [1].

Друга група загроз - загрози цілісності маршрутної інформації. Зловмисники можуть змінювати або підмінювати маршрутні оголошення, що суттєво впливає на мережу. У межах динамічної маршрутизації подібні дії можуть спричинити перехоплення трафіку, його перенаправлення або повне блокування комунікацій [1].

Третя група загроз - загрози доступності. Атаки типу DoS (Denial of Service) та DDoS (Distributed Denial of Service) можуть спричинити перевантаження маршрутних процесів, що призводить до зниження продуктивності або відмови

протоколів маршрутизації. Для протоколів, чутливих до частоти та своєчасності оновлень, таких як OSPF [1-3], це може мати критичні наслідки.

Четверта група загроз пов'язані з автентифікацією. Відсутність автентифікації дозволяє атакуючому змінювати таблиці маршрутизації, не будучи виявленим, що може призвести до серйозних порушень у роботі мережі [1].

Остання група загроз стосується загрози від внутрішніх порушників. Внутрішні порушники можуть мати доступ до конфіденційної маршрутної інформації, яку вони можуть змінювати або використовувати для несанкціонованого доступу до корпоративних сервісів.

Більшість наведених загроз використовує вразливості протоколів динамічної маршрутизації.

Аналіз вразливостей протоколів динамічної маршрутизації показує, що кожен з протоколів має свої специфічні слабкі місця, які можуть бути використані зловмисниками для атак на мережу. У таблиці 1 представлено порівняння основних вразливостей протоколів маршрутизації RIP, OSPF, EIGRP і BGP, а також типи атак, до яких ці протоколи схильні.

Таблиця 1

Порівняльний аналіз вразливостей протоколів динамічної маршрутизації

Протокол	Вразливість	Типи атак
RIP	Відсутність автентифікації, повільна конвергенція	Spoofing,route injection,DoS
OSPF	Вразливість до впровадження фальшивих LSA-пакетів	Spoofing, replay-атаки, DoS
EIGRP	Відсутність криптографії, маніпуляція оновленнями	Spoofing, route injection, replay-атаки
BGP	Вразливості в AS-PATH, BGP hijacking	BGP hijacking, Route Leak, DoS

Захист мережі від цих загроз потребує застосування різноманітних методів, серед яких автентифікація, шифрування, виявлення аномалій і застосування політик маршрутизації, що дозволяють мінімізувати ризики та забезпечити безпеку даних, що передаються між маршрутизаторами [3].

Відсутність належного захисту маршрутних оголошень може призвести до катастрофічних наслідків, включаючи втрату конфіденційності трафіку, його перенаправлення через вузли зловмисника, блокування сегментів мережі або порушення доступності критичних сервісів. Тому виникає потреба у створенні універсального методу захисту, здатного підвищити стійкість динамічної маршрутизації до атак, не знижуючи продуктивність і не змінюючи логіку роботи протоколів.

1. Manzoor A., Hussain M., Mehrban S. Performance analysis and route optimization: redistribution between EIGRP, OSPF & BGP routing protocols. Computer Standards & Interfaces, 2020, 68: 103391.
2. Cisco. Dynamic Routing Protocols: OSPF, EIGRP, RIPv2, IS-IS, BGP. URL: https://community.cisco.com/t5/networking-knowledge-

base/dynamic-routing-protocols-ospf-eigrp-ripv2-is-is-bgp/ta-p/4511577 (дата звернення: 20.04.2026).
3. Кульчинський І. Аналіз роботи протоколів динамічної маршрутизації. Збірник тез V Всеукраїнської студентської науково-технічної конференції „Природничі та гуманітарні науки. Актуальні питання “, 2012, 1: 67-67.

Analysis of Authentication-Based Attacks in Wireless Networks

UDC 004.7.056

Danylo Matiuk[1], Maryna Derkach[2],
Inna Skarga-Bandurova[3]

Ternopil Ivan Puluj National Technical University,
[1]matiuk.danylo@icloud.com, [2]m_derkach@tntu.edu.ua,
Oxford Brookes University,
[3]iskarga-bandurova@brookes.ac.uk

Modern wireless networks play a crucial role in data exchange and are widely deployed across commercial, governmental, educational, and residential environments. However, they remain among the most vulnerable components of both corporate and household security infrastructures. As their adoption increases, so does the number of potential targets for cyberattacks. Most attacks on wireless networks target authentication mechanisms, as these mechanisms are designed to prevent unauthorized access to access points.

Several widely used protocols provide secure authentication for wireless networks, including WPA, WPA2, and WPA3. These protocols differ in the data required for successful authentication, as well as in their encryption and validation methods. Each protocol supports two main authentication modes: WPA-Personal and WPA-Enterprise. The WPA-Personal mode relies on a pre-shared key (PSK), where all users and devices must know the same password to access the network. In contrast, WPA-Enterprise uses a RADIUS server for centralized authentication, where user credentials are verified individually.

Although WPA is considered obsolete for modern devices, it is still used in practice, particularly in low-power or legacy systems that rely on older algorithms. Similarly, WPA2, introduced in 2006 as the standard for secure Wi-Fi networks, remains widely used today. This is supported by the results of a wireless network scan (Fig. 1) performed using a portable NetScope device as part of ethical hacking activities [1].

SSID	RSSI	Channel	Security	Vendor	BSSID
[redacted]	-59 dBm	11	WPA*	Shenzhen	[redacted]
	-65 dBm	10	WPA2		
	-71 dBm	2	WPA*	TendaTec	
	-80 dBm	1	WPA2	Tp-LinkT	
	-81 dBm	1	WPA*		
	-82 dBm	10	WPA*	TendaTec	
	-83 dBm	6	WPA2		
	-88 dBm	8	WPA*		

Fig.1. Results of a wireless network scan

The compromise of wireless networks is rarely an isolated issue and often serves as an entry point for deeper intrusions into IT environments. By analysing information