Експериментальна оцінка DoS атаки та її вплив на пропускну здатність у безпровідних мережах IEEE 802.11

Віталій Галета, Олена Жарова, Олександр Кукрі

Кафедра телекомунікаційних систем, Національний авіаційний університет, УКРАЇНА,
м.Київ, просп. Космонавта Комарова, 1, E-mail: vitaliy@galeta.org

In recent years, wireless LAN (WLAN) has gained popularity in a variety of locations. This has lead to development of high level security protocols for WLAN. The newest protocol IEEE 802.11i ratified to provide strong data encryption but it can not prevent Denial of Service (DoS) attacks on WLAN. This paper in a testbed, conducts an experimental framework to implement and quantify common types of DoS attacks against WLAN throughput. The results of implementation of our experiments shows that how easily DoS attacks can be performed on WLAN which causes to reduce throughput of communication considerably to make inaccessible wireless connection for its authorized members.

Ключові слова – DoS attack, wireless network, network security, management frame, IEEE 802.11

I. Вступ

В останні роки, безпровідна локальна мережа (WLAN) отримала велику популярність в багатьох місцях. Різні протоколи безпеки були запропоновані і використані у WLAN, щоб зробити її більш надійною. Останній протокол IEEE 802.11i (WPA2), забезпечує надійне шифрування даних з використанням алгоритму Advanced Encryption Standard (AES). Він також забезпечує високий рівень убезпечення даних з використанням протоколу IEEE 802.1x. Тому IEEE 802.11i може вирішувати більшість питань, що стосуються безпеки даних у WLAN, однак цей протокол не захищає WLAN від DoS атак.

Більша частина DoS атак на WLAN виникає з уміння використати базові вразливості, які не захищені в протоколі 802.11i. Це може бути використаним зловмисником для запуску різних видів DoS атак. Основні DoS атаки на WLAN включають флудинг пакетами запиту аутентифікації (AuthRF), асоційованими запитами (AssRF), запитів деаутентифікації (DeauthF) і дизасоціації. Ці DoS атаки є причиною відмови в обслуговуванні WLAN або деяких її вузлів. У даній роботі ми реалізуємо ряд загальних DoS атак для перевірки WLAN, яка використовує протокол безпеки IEEE 802.11i, щоб продемонструвати існуючі вразливості протоколу. Потім на основі експериментальної бази ми зможемо кількісно оцінити ефект від DoS атаки щодо пропускної здатності WLAN.

II. DoS атаки проти мереж 802.11

Деякі управляючі кадри передаються між точкою доступу (AP) та клієнтами, щоб забезпечити фізичний зв'язок. Ці кадри не захищені жодним з нинішніх безпровідних протоколів безпеки. Таким чином, зловмисник, використовуючи ці кадри, може виконати різноманітні DoS атаки. У цій статті ми розглядаємо найпоширеніші DoS атаки на безпровідну мережу – DeauthF, AuthRF і AssRF. При DeauthF атаці, зловмисник постійно відправляє підроблені деаутентифікаційні кадри для своєї жертви щоб вона стала недоступною для інших легальних клієнтів у WLAN. З моменту отримання повідомлення деаутентифікації, жертва не може ігнорувати його, і має забезпечити виконання відключення себе від мережі. Цю атаку можна зробити ще гірше, якщо зловмисник вибирає AP в якості потерпілого. У цьому випадку всі легальні клієнти відключаються і вся мережа стає недоступною.

При AuthRF атаці, коли легальна AP отримує запит авторизації від підробленого джерела MAC-адреси, вона посилає аутентифікаційну відповідь до підробленого безпровідного клієнта. З моменту зникнення підробленого безпровідного клієнта, AP не може отримати підтвердження прийому кадру для переданої аутентифікаційної відповіді. AP продовжує відправляти кілька кадрів відповіді аутентифікації, які перевантажують WLAN, оскільки процес перевірки автентичності цих прохань споживає багато ресурсів AP. В результаті, AP залишає мало ресурсів для роботи з іншими клієнтами, і вони страждають на бідний обмін даними або повну втрату повідомлень.

При AssRF атаці, коли AP отримує асоціативний запит з підробленого джерела MAC-адреси, вона перевіряє свій буфер і вважає, що підробленого безпровідного клієнта не існує в справжній таблиці AP. Потім вона направляє деаутентифікаційний кадр до підробленого безпровідного клієнта. Оскільки немає підтвердження від підробленого безпровідного клієнта, він відправляє кілька деаутентифікаційних кадрів. Для AssRF DoS атак, атакована AP завжди веде перевірку буферів і багаторазове відправлення повідомлень-відповідей на кожний отриманий асоційований запит. Вона не має часу або ресурсів для обслуговування інших безпровідних клієнтів. Це змушує безпровідних клієнтів зменшити швидкість обміну даними або навіть припинити його взагалі.

III. Проведення випробувального експерименту

Ми провели випробувальний експеримент з використанням усіх сучасних протоколів безпеки, таких як WEP, WPA, та WPA2. Експеримент показав, що жоден з цих протоколів не перешкоджає проведенню вищезгаданих DoS атак. Для повного представлення наслідків DoS атаки в кількісній формі у WLAN ми обрали найбільш захищений протокол 802.11i (WPA2) для захисту тестової мережі. Тестова модель мережі представлена на рис. 1.

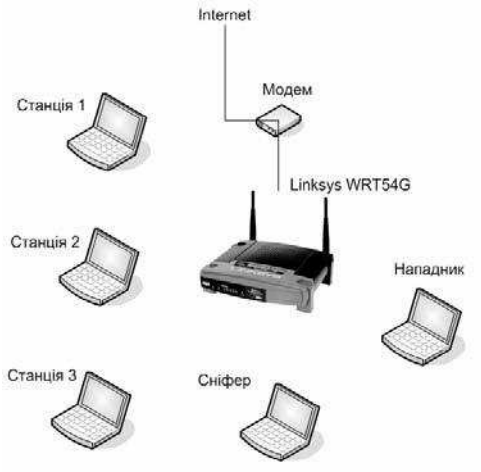

Рис. 1. Тестова мережа для випробовування DoS атак

WLAN містить безпровідний маршрутизатор Linksys WRT54G в якості базової станції. Три легальні станції обладнані мережевими адаптерами IEEE 802.11g на базі чіпсету Intel під управлінням операційної системи Windows XP SP2. Ще одна станція використовувалась як сніфер для збору всіх пакетів, що передавались через тестову радіомережу. Вона використовує програму wireshark як сніфер для відстеження шляху атакуючого. Сніфер та нападник обладнані мережевими адаптерами IEEE 802.11g на базі чіпсету Atheros AR5212 під управлінням операційної системи Ubuntu Intrepid Ibex 8.10. Нападник використовує програму aircrack-ng як інструмент проведення DoS атак. Всі клієнти та безпровідний маршрутизатор підтримають аутентифікацію користувачів 802.1x.

Для проведення дослідження, ми розглядаємо три поширених типи атак на бездротові мережі, такі як DeauthF, AuthRF і AssRF. В трьох експериментах ми визначили пропускну здатність WLAN для оцінки наслідків цих атак на безпровідні мережі.

A. Показники ефективності

Коли зловмисник починає DoS атаку в різних можливих формах, він намагається переповнити безпровідну мережу фальшивим трафіком. Тому, щоб показати вплив тестових атак, це дослідження розглядає пропускну здатність радіомережі в двох станах: до атаки та під час атаки.

Ми використовуємо ці дві величини для порівняння пропускної здатності безпроводової мережі у разі атаки. В усій статті ми вважаємо пропускну здатність як кількість байт, отриманих приймачем, за одиницю часу.

IV. Експериментальний аналіз

Даний розділ описує проведення вимірювання пропускної здатності для трьох згаданих DoS атак. В усіх нападах, одиницею виміру вважається загальна кількість байт, отриманих на приймачі за одну секунду. В досліді вважаємо, що зловмисник обирає Станцію 1 як жертву. Сніфер відслідковує будь-які атаки для отримання результатів досліду.

A. Експеримент 1: Вимір пропускної здатності для атаки DeauthF.

Ми провели цей експеримент, щоб продемонструвати вплив DeauthF атаки на пропускну здатність тестової WLAN. У цьому експерименті зловмисник постійно флудить жертву (Станція 1) 100 підробленими деаутентифікаційними кадрами за секунду для відключення Станції 1 з мережі. Ми постійно спостерігаємо ці підроблені кадри завдяки сніферу для дослідження будь-якого відхилення пропускної здатності жертви чи інших легальних клієнтів (Станції 2 та 3) WLAN. Сніфер показує, що відразу ж після отримання першого підробленого деаутентифікаційного кадру на 62 секунді, жертва відключається від WLAN і не може передавати будь-яку інформацію до завершення атаки на 100 секунді. Тривалість нападу в даному експерименті складає близько 38 секунд, він призводить до нульової пропускної здатності для жертви.

Цей експеримент вимірює кількість пакетів, що передаються будь-яким легальним клієнтом тестової мережі чи зловмисником до або під час DeauthF атаки впродовж визначеного часу. Результати експерименту представлені в таблиці 1.

ТАБЛИЦЯ 1

Результати DeauthF атаки на тестову WLAN

		Мережа	Нападник
Загальна к-ть пакетів		39478	3638
Загальна тривалість експерименту (сек)		147,460	37,988
Середнє завантаження (Байт/сек)		45479,977	16280,255
Байт		6706490	618460
До атаки	К-ть пакетів даних	1077	0
	Байт	789835	0
	Час (сек)	63,075	63,075
Впродовж атаки	К-ть пакетів даних	0	3638
	Байт	0	618460
	Час (сек)	37,988	37,988

З вищезазначеної таблиці 1, ми приходимо до висновку, що пропускна здатність до атаки=789835/63,075=12522,15616 Байт/сек.
Під час атаки=0/37,988=0 Байт/сек.

Результати вимірювання пропускної здатності показані на рис.2 в трьох станах: до, під час та після DeauthF атаки через тестову WLAN.

Як показує рис.2, до та після атаки жертва обмінюється інформацією в нормальному режимі. Нападник починає атаку на 62 секунді впродовж приблизно 38 секунд до 100-ї секунди. Впродовж цих 38 секунд, жертва не веде передачу даних, через те що вона була від'єднана від WLAN нападником, отже, пропускна здатність для жертви дорівнює нулю. З графіку видно, що тільки один передавач нападника зайняв увесь канал WLAN з його підробленими

деаутентифікаційними кадрами і не дозволив жертві використовувати її законний канал.

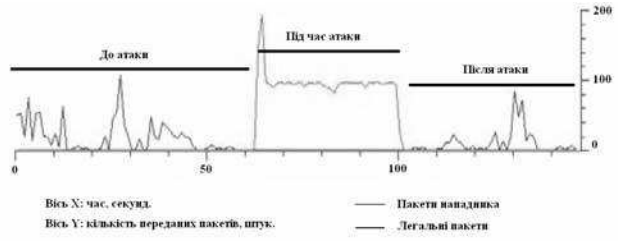

Рис. 2. Пропускна здатність WLAN
під час DeauthF атаки

B. Експеримент 2: Вимір пропускної для AuthRF атак

В даному досліді ми демонструємо вплив AuthRF атаки на пропускну здатність тестової WLAN. Нападник постійно відправляє кадри аутентифікаційних запитів до жертви (Станція 1). Після відправлення цього типу підроблених кадрів, нападник очікує отримати кадри відповіді з безпроводового маршрутизатора, що означає успішну аутентифікацію Станції 1. Наш сніфер відслідковує ці підроблені кадри.

Цей експеримент вимірює кількість пакетів, що передаються будь-яким легальним клієнтом тестової мережі чи зловмисником до або під час AuthRF атаки впродовж визначеного часу. Результати експерименту представлені в таблиці 2.

ТАБЛИЦЯ 2

Результати AuthRF атаки на тестову WLAN

		Мережа	Нападник
Загальна к-ть пакетів		126444	15927
Загальна тривалість експерименту (сек)		190,554	39,319
Середнє завантаження (Байт/сек)		129306,123	76303,766
Байт		15717686	2771298
До атаки	К-ть пакетів даних	2380	0
	Байт	2191940	0
	Час (сек)	115,302	0
Впродовж атаки	К-ть пакетів даних	76	15927
	Байт	12768	618460
	Час (сек)	39,319	39,319

З вищезазначеної таблиці 2, ми приходимо до висновку, що пропускна здатність до атаки=2191940/66,302=33059,9 Байт/сек.
Під час атаки=12768/36,319=351,55 Байт/сек.

Результати вимірювання пропускної здатності показані на рис.3 в трьох станах: до, під час та після AuthRF атаки через тестову WLAN.

Як показує рис.3, до та після атаки мережа працює в нормальному режимі. Під час атаки, що почалась з, приблизно, 115 секунди до 154 секунди спостерігалась дуже мала передача легальних пакетів порівняно з величезною кількістю підроблених пакетів нападника. Жертва мала дуже малу пропускну здатність впродовж 39 секунд атаки. Це відбувалось через те, що нападник займав більшість ресурсів безпровідного маршрутизатора і він був повністю зайнятий відповідями на підроблені кадри атакуючого. Тому під час атаки мережа працювала дуже повільно для будь-яких клієнтів.

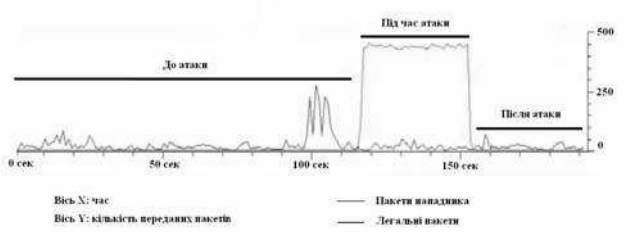

Рис. 3. Пропускна здатність WLAN
під час AuthRF атаки

C. Експеримент 3: Вимір пропускної для AssRF атак

В даному досліді ми демонструємо вплив AssRF атаки на пропускну здатність тестової WLAN. В цьому експерименті нападник постійно флудить жертву (Станція 1) підробленими кадрами асоціювання для завантаження безпровідного маршрутизатора відповідями на ці підроблені кадри, що означає завантаження каналу. У цьому експерименті наш сніфер відстежує велику кількість переданих маршрутизатором деаутентифікаційних пакетів до нападника.

Цей експеримент вимірює кількість переданих пакетів легітимними клієнтами та нападником до та під час атаки впродовж визначеного часу. Результати експерименту представлені в таблиці 3.

ТАБЛИЦЯ 3

Результати AssRF атаки на тестову WLAN

		Мережа	Нападник
Загальна к-ть пакетів		132038	500
Загальна тривалість експерименту (сек)		58,851	9,477
Середнє завантаження (Байт/сек)		237459,433	41785,8
Байт		13974812	103500
До атаки	К-ть пакетів	283	0
	Байт	219393	0
	Час (сек)	16,029	0
Впродовж атаки	К-ть пакетів	7	500
	Байт	5293,5	103500
	Час (сек)	9,477	2,477

З вищезазначеної таблиці 3, ми приходимо до висновку, що пропускна здатність до атаки=219393/22,029=9959.28 Байт/сек.
Під час атаки=5293.5/2.477=2136.45 Байт/сек.

Результати вимірювання пропускної здатності показані на рис.4 в трьох станах: до, під час та після AssRF атаки через тестову WLAN.

Як показує рис.4, до та після атаки мережа працює в нормальному режимі. На відміну від DeauthF атаки,

ми спостерігаємо малу кількість легальних пакетів, що показує, що легальний користувач не повністю від'єднаний і має дуже малу пропускну здатність через велику кількість підроблених пакетів нападника. Нападник починає атаку на 16 секунді та припиняє її на 25. Впродовж 9 секунд нападник споживає пропускну здатність мережі за допомогою підроблених пакетів асоціативних запитів тому зв'язок для клієнтів WLAN дуже повільний.

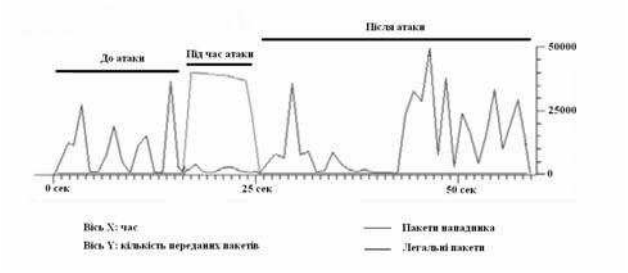

Рис. 4. Пропускна здатність WLAN під час AssRF атаки

V. Обговорення результатів

Рис. 5 підбиває підсумки та порівнює пропускну здатність для всіх виконаних атак.

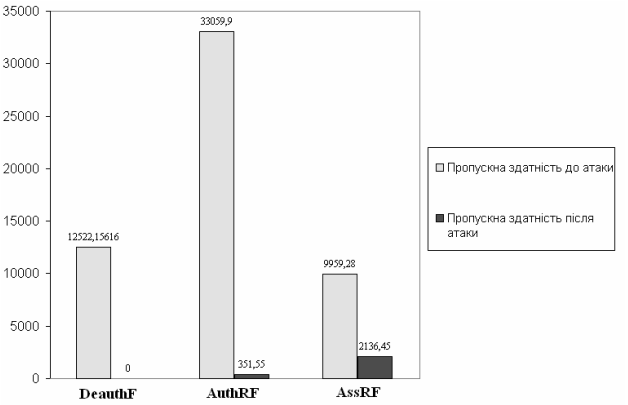

Рис. 5. Порівняння пропускної здатності для проведених DoS атак.

З рис.5 вгорі ми бачимо, що DeauthF атака є найбільш серйозною щодо зменшення пропускної здатності WLAN. DeauthF атака повністю зменшує пропускну здатність WLAN до нуля так, що жертва чи всі легальні користувачі не можуть використовувати WLAN взагалі. З вищенаведеного графіку видно, що під час AuthRF та AssRF атак, на відміну від DeauthF атаки, користувачі можуть отримати доступ до мережі, але дуже повільно, і швидкість падає на стільки, що передача даних стає дуже повільною.

Графік показує, що AuthRF атака більше впливає на роботу WLAN, ніж AssRF. Під час AuthRF атаки пропускна здатність нижча ніж під час AssRF атаки через те, що жертва потребує більшого обміну кадрами для початку роботи у WLAN.

VI. Висновки

Протокол безпеки 802.11i було прийнято для забезпечення більшої безпеки в безпровідних мережах. Але навіть при наявності цього протоколу безпровідні мережі є вразливими до DoS атак. Нападник може легко використовувати незахищене управління кадрами для проведення різних типів атак, графіки та таблиці, наведені вище, демонструють ці вразливості. У даній роботі ми провели три загальних тести DoS атак на мережі IEEE 802.11. Ми продемонстрували наслідки DeauthF, AuthRF, та AssRF DoS атак на пропускну здатність тестових WLAN, що використовували протокол 802.11i. З результатів експериментів ми надійшли до висновку, що DoS атаки є серйозною загрозою безпеці пропускній здатності WLAN. Результати показують, що ці DoS атаки можуть споживати ресурси WLAN так, що частина пропускної здатності, яка залишилась (нуль при DeauthF та трохи при AuthRF та AssRF) буде недостатньою для продовження нормальної роботи мережі з її легальними членами.

References

[1] IEEE Computer Society LAN MAN Standards Committee. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications in IEEE Std 802.11". 1999.

[2] Bellardo J. and Savage S. "802.11 Denials-of-Service Attacks: Real Vulnerabilities and Practical Solutions". Proceedings of the USENIX Security Symposium. 2003.

[3] Liu C. "802.11 Disassociation Denial of Service (DoS) attacks". School of CTI DePaul University. 2005.

[4] IEEE Standard 802.11i . "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Amendment 6: Medium Access Control (MAC) Security Enhancements". 2004.

[5] He C. and Mitchell J. C. "Security Analysis and Improvements for IEEE 802.11i". Proceedings of the 12th Annual Network and Distributed System Security Symposium. 2005.

[6] IEEE 802.11i. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications". 2004.

[7] Edney J., Arbaugh W. "Real 802.11 Security: Wi-Fi Protected Access and 802.1li". 2003.

[8] "Announcing the advanced encryption standard (AES) ". Federal Information Processing Standards Publication. 2001.

[9] Walker J. "IEEE 802.11i Standard Improves Wireless LAN Security". 2005.