

Corso di Laurea Magistrale in

Ingegneria Informatica

Progetto di

Network Security

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Studenti**  Di Cello Danny 224527  Seminara Giuseppe 227540  Magurno Roberto 227501  Miriello Raffaele 227564 | |  | |
|  |  |  | |

Anno Accademico 2021/2022

***Indice***

*1 Introduzione 3*

*2 Ambiente di Sviluppo 5*

*3 Attacchi 7*

*3.1 DoS Attack 7*

*3.2 Rank Attack 13*

*3.3 Warmhole Attack*

*3.4 Fragment Duplication Attack*

*4 Conclusioni 18*

*5 Bibliografia 19*

***Introduzione***

L’obiettivo del seguente progetto è l’implementazione di un insieme di attacchi, e delle rispettive mitigazioni, in un ambiente IoT simulato. In questo tipo di contesti abbiamo a che fare con dispositivi dotati di bassa potenza di elaborazione che comunicano, ed è proprio a causa di tali caratteristiche che, i protocolli di comunicazioni devono essere leggeri in modo da poter essere eseguiti senza causare un overhead eccessivo. Per tale motivo spesso, tali protocolli, tralasciano alcuni aspetti di sicurezza che richiederebbero un elevato quantitativo di risorse, lasciando uno spazio per potenziali attacchi. Nel nostro caso di studio specifico sfrutteremo questi spiragli di sicurezza in riferimento ai protocolli **6LoWPAN** e **RPL**, implementando in particolare i seguenti attacchi:

* ***DoS Attack.***
* ***Rank Attack.***
* ***Warmhole Attack.***
* ***Fragment Duplication Attack****.*

*L’elaborato ha la seguente struttura:*

*Dopo aver descritto brevemente gli obiettivi del nostro lavoro, concludiamo la seguente sezione fornendo una breve descrizione dei due protocolli analizzati, al fine di rendere maggiormente comprensibile la discussione affrontata nei capitoli successivi.*

*Nel secondo capitolo descriviamo l’ambiente di sviluppo utilizzato per l’implementazione degli scenari descritti.*

*Nel terzo capitolo ci occupiamo di descrivere gli attacchi realizzati e le possibili mitigazioni in riferimento a diversi scenari applicativi.*

*Infine, concludiamo l’elaborato, traendo le conclusioni sul lavoro effettuato, analizzando e descrivendo i punti salienti affrontati ed eventuali effetti collaterali derivanti dagli scenari considerati.*

**6LoWPAN (Ipv6 over Low-Power Wireless Personal Area Networks)**

È un protocollo che definisce meccanismi di incapsulamento e compressione dell’intestazione che consentono l’invio e la ricezione di pacchetti IPv6 su reti basate su IEE 802.15.4, ovvero Low-Rate Wireless Personal Aerea Networks. Ai nodi IPv6 vengono assegnati indirizzi IP gerarchici a 128 bit, attraverso l’uso di un prefisso di lunghezza arbitraria. 6LoWPAN permette di superare i problemi legati alle grandi dimensioni delle intestazioni IPv4 e IPv6, permettendo anche a dispositivi a bassa potenza, con risorse hardware limitate di comunicare. Le specifiche di 6LoWPAN sono definite nei seguenti documenti RFC: **RFC 4919** e **RFC 4944**.

I principali problemi legati ai dispositivi LoWPAN sono i seguenti:

* **Frammentazione e riassemblaggio**: I vincoli di dimensione del pacchetto imposti da IPv6 e 802.15.4 rappresentano un problema di eccessiva frammentazione/riassemblaggio.
* **Compressione dell’intestazione IPv6**: con l’attuale intestazione IPv6 di 40 byte, il payload è ridotto. La compressione dell’intestazione IPv6 rappresenta una necessità per ottimizzare i trasferimenti su una rete 6LoWPAN.
* **Routing**: Le reti LoWPAN sono costituite da moltissimi nodi, è necessario adottare quindi un protocollo di instradamento per supportare tali reti, che al contempo soddisfi i vincoli hardware dei dispositivi stessi.

**RPL (IPv6 Routing Protocol for Low-Power and Lossy Networks)**

È un protocollo di routing per reti wireless a bassa potenza e generalmente soggette a perdita di pacchetti, ottimizzato per la comunicazione multi-hop e la comunicazione molti-a-uno, ma supporta anche la comunicazione uno-a-uno. Il protocollo è definito nel RFC 6550.

RPL crea una topologia simile ad un albero, che prende il nome di DAG (Grafo Diretto Aciclico). Ogni nodo all’interno della rete ha un rank assegnato, che aumenta man mano che i nodi si allontanano dal nodo radice. I nodi scelgono dunque il rank più basso come criterio di selezione della route. I messaggi ICMPv6 sono definiti nel RFC 4443, e in particolare possiamo individuare i seguenti:

* ***DIS (Information Request DODAG)****:* Utilizzato per richiedere informazioni al DODAG nelle vicinanze. È analogo ai messaggi di richiesta inviati dal router per scoprire le reti esistenti.
* ***DIO (Object of Information of the DAG):*** Messaggio che condivide le informazioni del DAG, inviato in risposta ai messaggi DIS, e utilizzato per aggiornare periodicamente le informazioni sulla topologia della rete.
* ***DAO (Object of Update to the Destination):*** Messaggio inviato dai vari nodi per aggiornare le informazioni relative al loro nodo padre in tutto il DAG.

***Ambiente di Sviluppo***

Per l’implementazione degli scenari descritti si è deciso di utilizzare Contiki-NG, come sistema operativo per i dispositivi IoT, e il simulatore COOJA per costruire il nostro ambiente virtualizzato. La principale motivazione che ha influito su tale scelta è che Contiki è il sistema operativo più utilizzato per l’implementazione del protocollo RPL, essenziale per i nostri scopi, inoltre il sistema è Open Source e supporta un elevato numero di dispositivi diversi, dai computer a 8 bit fino ai nodi che formano le reti di sensori.

Di seguito illustriamo il processo di installazione e configurazione dell’ambiente.

Sebbene sia possibile seguire diverse strade per l’installazione del sistema Contiki, abbiamo deciso di seguire l’approccio consigliato nella documentazione ufficiale, utilizzando quindi un’immagine Docker. La scelta effettuata presenta diversi vantaggi, i cui due più rilevanti sono i seguenti:

* ***Facilità di installazione***: l’installazione richiede pochi passi, al termine dei quali si dispone di un ambiente totalmente configurato e funzionante.
* ***Compatibilità:*** l’installazione attraverso un’immagine Docker fornisce una maggiore compatibilità ed un maggior numero di dispositivi simulati, rispetto ad un processo di installazione nativa sul sistema Host.

***Requisiti***

Se non è già presente sul sistema è necessario installare il pacchetto Docker-CE, con il seguente comando:

*$ sudo apt-get install docker-ce*

Successivamente è opportuno aggiungere l’utente corrente al gruppo Docker. Questo passaggio è facoltativo, ma permette di interagire col Docker senza l’utilizzo dei privilegi di amministratore.

*$ sudo usermod -aG docker ns*

***Installazione***

Installato Docker-ce sul sistema host è possibile procedere al download dell’immagine di Contiki-ng digitando

*$ docker pull contiker/contiki-ng*

Tale comando scarica l’ultima versione di Contiki disponibile. Una volta completato il download è necessario clonare il repository GitHub di Contiki-ng e inizializzare tutti i sotto moduli con i seguenti comandi

*$ git clone https://github.com/contiki-ng/contiki-ng.git*

*$ cd contiki-ng*

*$ git submodule update --init –recursive*

Infine, per semplificare il processo di avvio è stato creato il seguente alias:

*export CNG\_PATH=/home/ns/contiki-ng*

*alias contiker="docker run --privileged --sysctl net.ipv6.conf.all.disable\_ipv6=0 --mount type=bind,source=$CNG\_PATH,destination=/home/user/contiki-ng -e DISPLAY=$DISPLAY -v /tmp/.X11-unix:/tmp/.X11-unix -v /dev/bus/usb:/dev/bus/usb -ti contiker/contiki-ng"*

A questo punto l’ambiente di sviluppo è installato ed è possibile lanciare il simulatore digitando il comando

$ contiker cooja

***Struttura Cartelle***

Per la riproduzione degli esperimenti sviluppati è necessario identificare due cartelle importanti:

~/contiki-ng: contiene tutti i file di configurazione di Contiki-NG.

~/attacchi: contiene tutti i file modificati per implementare gli attacchi e le rispettive mitigazioni descritte nel capitolo 3.

La cartella attacchi è suddivisa in sottocartelle ognuna delle quali contiene l’implementazione di un attacco e della rispettiva mitigazione, riferita a due topologie differenti, una media e una più complessa (cartella Complex). Inoltre, è presente uno script Bash che permette di preparate tutti i file necessari e pulire l’ambiente prima di caricare una simulazione, utilizzando i file di backup presenti nella rispettiva cartella.

***Attacchi***

In questo capitolo andremo a descrivere i diversi attacchi implementati, esponendo una trattazione teorica degli stessi e allegando il relativo codice implementativo, opportunamente documentato.

***DOS (Denial of Service)***

L’attacco DoS mira a compromettere la disponibilità di un servizio, sovraccaricando una risorsa con richieste inutili, impedendole così di soddisfare le richieste legittime. L’attacco DoS è un attacco difficile da mitigare perché sfrutta il normale schema di funzionamento del sistema.

Nel nostro caso specifico abbiamo implementato due varianti dell’attacco, nella prima variante abbiamo una topologia semplice, composta da un solo nodo attaccante ed un solo nodo vittima, nella seconda variante, invece, abbiamo implementato una topologia più complessa dove simuliamo un DDoS (Distributed Denial of Service), in cui sono presenti più attaccanti che attaccano lo stesso nodo vittima.

Prima di analizzare i due casi specifichi, per poter effettuare un confronto, mostriamo con la seguente figura, un possibile scenario legittimo.

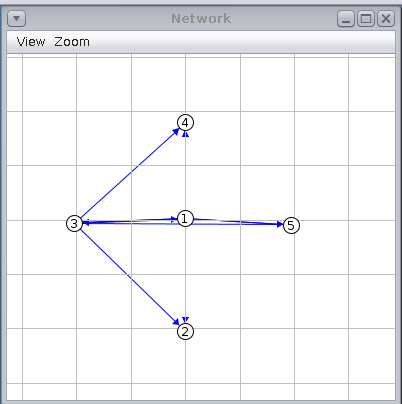


Figura 1a: Topologia base

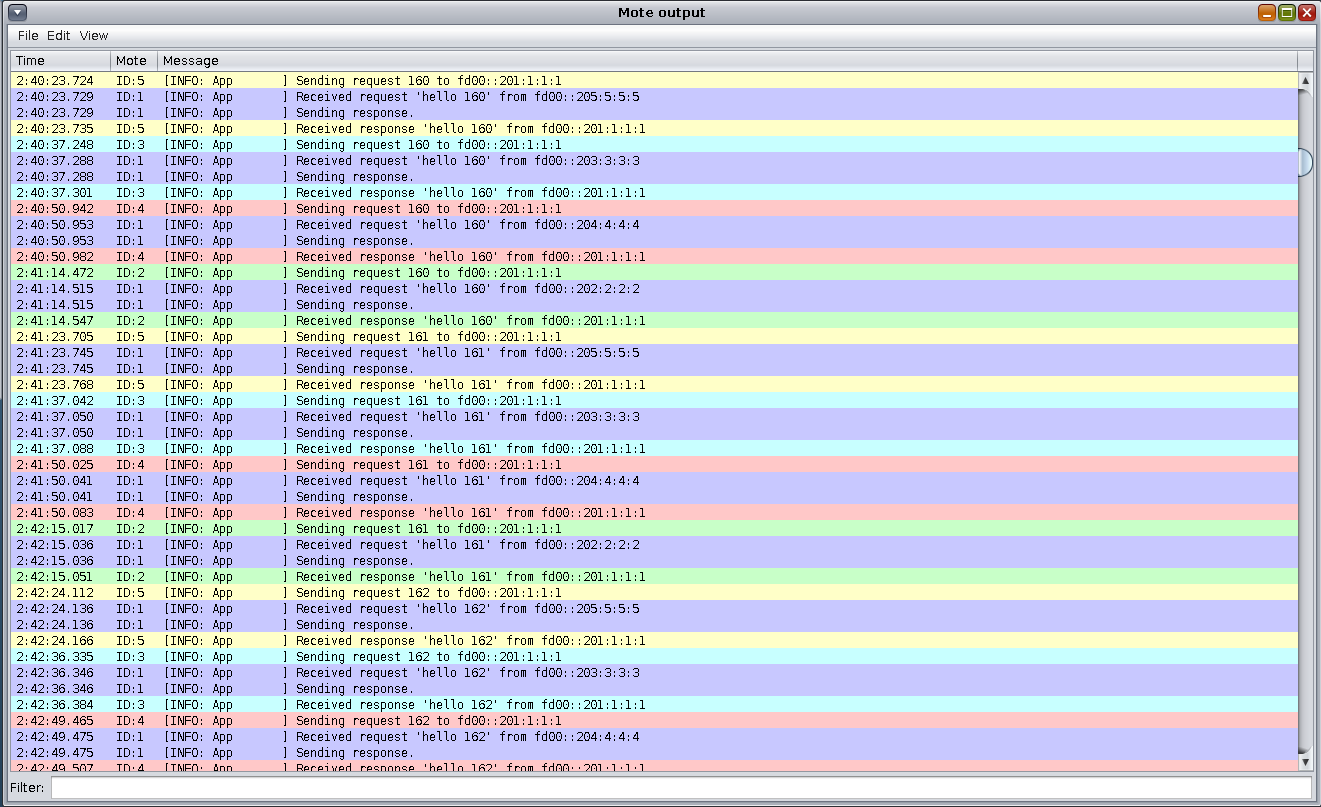
La figura 1a mostra la topologia della rete considerata, che consiste in un server UDP, identificato da ID=1, e di quattro nodi client che inviano richieste ad intervalli casuali.

Figura 1b: Log Scenario Legittimo

La figura 1b mostra il log dei messaggi scambiati ed è possibile osservare che subito dopo che un client fa la richiesta, il server la riceve e invia una risposta che viene ricevuta correttamente dal client.

Andiamo a descrivere ora le due varianti di attacco implementate.

***Variante 1***

Questa prima variante è un semplice attacco DoS, con una topologia relativamente semplice, ma funzionale per la comprensione dell’attacco, in cui troviamo un solo nodo attaccante che inonda il server di richieste impedendogli di rispondere a richieste legittime.

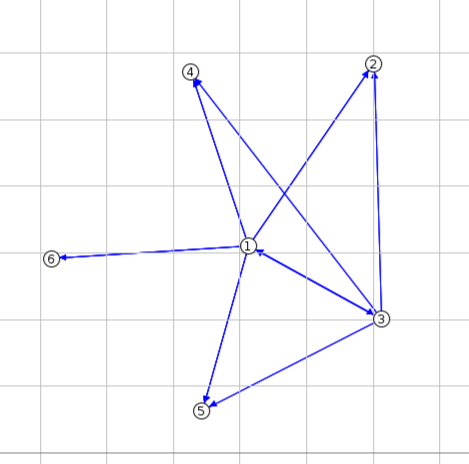


Figura 2a: Topologia DoS

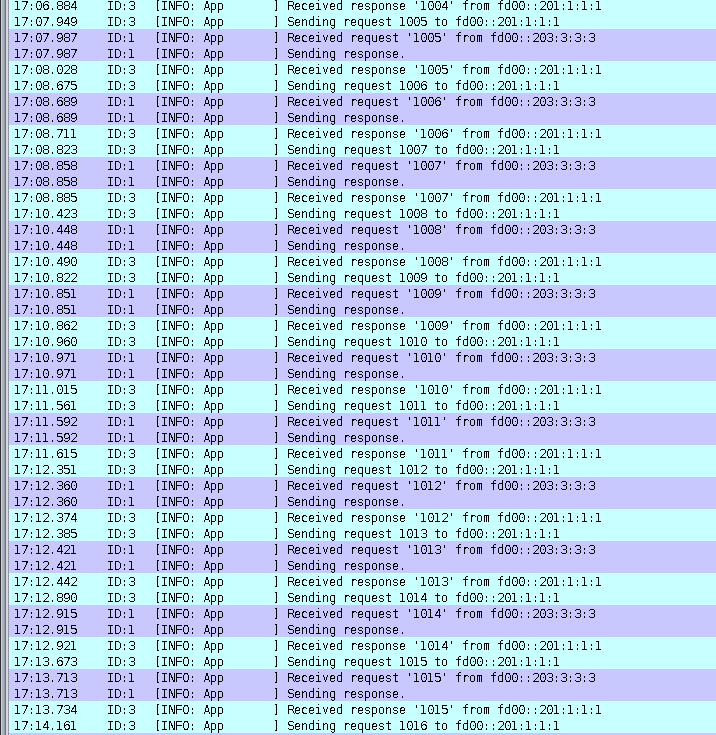


Figura 2b: Log attacco DoS

La figura 2a mostra la topologia di questo attacco, in cui abbiamo 1 server, identificato sempre da ID=1 lì dove non esplicitamente indicato diversamente, e 5 nodi client di cui 4 legittimi e uno malevolo indicato con ID=3. Come è possibile osservare dal log il nodo 3 inonda di richieste il server consumando tutte le sue risorse, costringendolo a scartare le richieste provenienti dai nodi legittimi.

*Mitigazione*

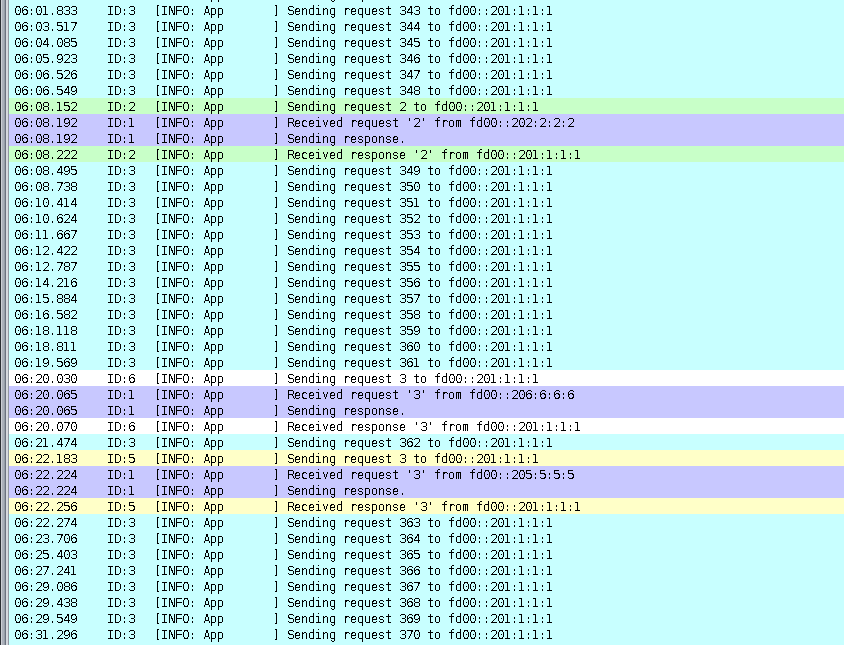
*La mitigazione dell’attacco si basa sul rate di ricezione dei messaggi da parte del server. In particolare, si fissa una soglia, stabilita in modo empirico sulla base della topologia della rete, e si vanno a scartare i messaggi provenienti da nodi che hanno un rate più elevato rispetto alla soglia stabilita. Il valore della soglia ricopre un’importanza cruciale, fissando un valore troppo basso, infatti, anche i nodi legittimi potrebbero essere classificati come malevoli, viceversa fissando un valore troppo elevato potrebbe passare troppo tempo prima di accorgersi dell’attacco consumando tutte le risorse a disposizione e iniziando a scartare richieste legittime. Per implementare tale mitigazione è stato creato un thread sul server che calcola e aggiorna periodicamente il rate di ricezione dei pacchetti per ogni nodo presente nella rete e che comunica con lui. Sulla base di tale valore calcolato, ogni volta che arriva un pacchetto si decide se elaborarlo o scartarlo.*

Figura 2c: Mitigazione DoS

*Come è possibile osservare dalla figura 2c, applicando tale mitigazione, il server non risponde più ai messaggi di richiesta del nodo malevolo 3, e al contempo riesce a rispondere correttamente alle richieste dei nodi legittimi.*

*L’elevata presenza di messaggi da parte del nodo 3 rispetto ai nodi legittimi è legata al fatto che ha un rate di invio molto elevato rispetto agli altri nodi.*

***Variante 2***

In questo secondo scenario si vuole simulare un attacco DDoS, abbiamo quindi una topologia più complessa in cui abbiamo 4 nodi malevoli (ID: 3, 16, 9, 6) che attaccano il nodo server. Mostriamo in modo analogo al caso precedente prima l’attacco e subito dopo lo scenario con la mitigazione attiva, quest’ultima è la medesima del caso precedente, ma come si può osservare dalle figure seguenti risulta efficace.

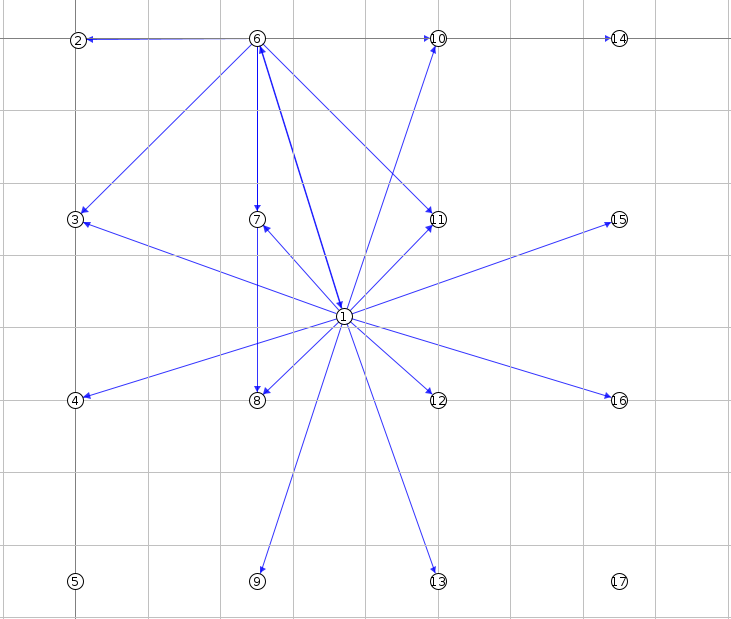
**

Figure 3a: Topologia DDoS

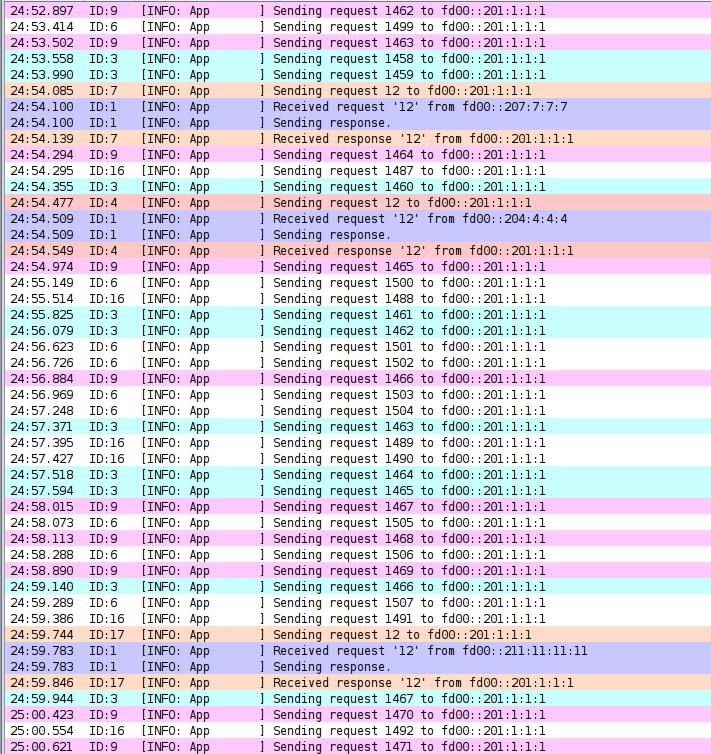


Figura 3b: Mitigazione DDoS

Come è possibile osservare in questo secondo scenario descritto manca il log riferito all’attacco senza la mitigazione attiva. Questo è dovuto al fatto che nel momento in cui si esegue il DDoS, i nodi malevoli consumano tutte le risorse del Server, facendo terminare, quasi immediatamente, la simulazione con un errore. La figura 3b, oltre la corretta esecuzione dello scenario con la mitigazione attiva, permettono di visualizzare l’efficacia della soluzione proposta.

Il codice, opportunamente commentato, relativo a questo attacco e le rispettive simulazioni avviabili con Cooja sono presenti all’interno delle seguenti cartelle:

* Attacchi/DOS.
* Attacchi/Complex/DOS.

***Rank Attack***

L’introduzione del concetto di rank all’interno del protocollo RPL risulta utile a diverse applicazioni come l’ottimizzazione del percorso o la prevenzione di cicli, ma al contempo rappresenta un efficace vettore di attacco, che può incidere sulle performance della rete. Un nodo malevolo può infatti falsificare il valore del rank, e gli altri nodi non hanno modo di verificare l’autenticità di tale valore.

In questa tipologia di attacco un nodo malevolo modifica il proprio rank in modo da attirare e manipolare l’intera rete, causando, ad esempio, ritardi nella consegna dei messaggi, perdita dei pacchetti, creazione di loop che rendono la topologia instabile e rendendo necessario un elevato numero di messi di controllo per correggere la struttura della rete.

Di seguito mostriamo un possibile scenario legittimo e successivamente proponiamo due varianti dell’attacco, con due topologie differenti.

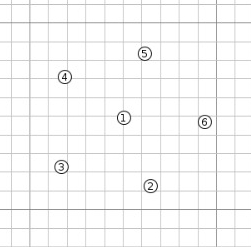


Figura 4a: Topologia Base

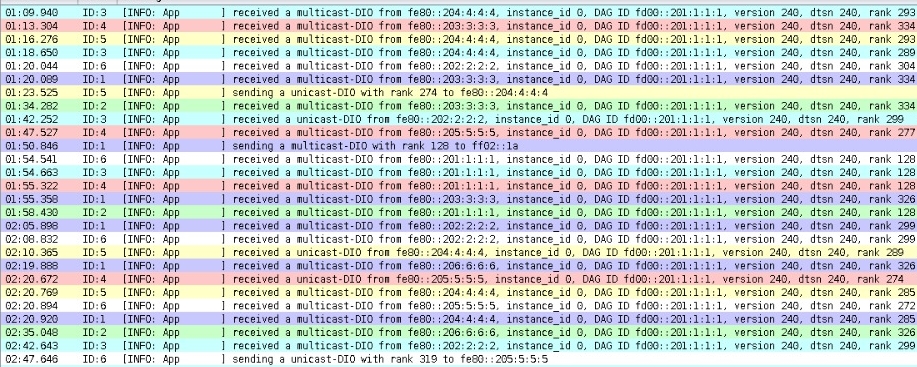


Figura 4b: Log scenario Legittimo

**Variante 1**

In questo caso abbiamo una topologia semplice in cui abbiamo un solo nodo attaccante e un solo nodo vittima. Il nodo attaccante, quindi, invia al nodo vittima un valore di rank falso. In particolare, dall’analisi dei log è possibile osservare come il nodo attaccante con ID=4 invii dei messaggi DIO con rank posto pari a 1000 solo al nodo 3, il quale riceve e registra tale valore di rank associato al nodo attaccante.

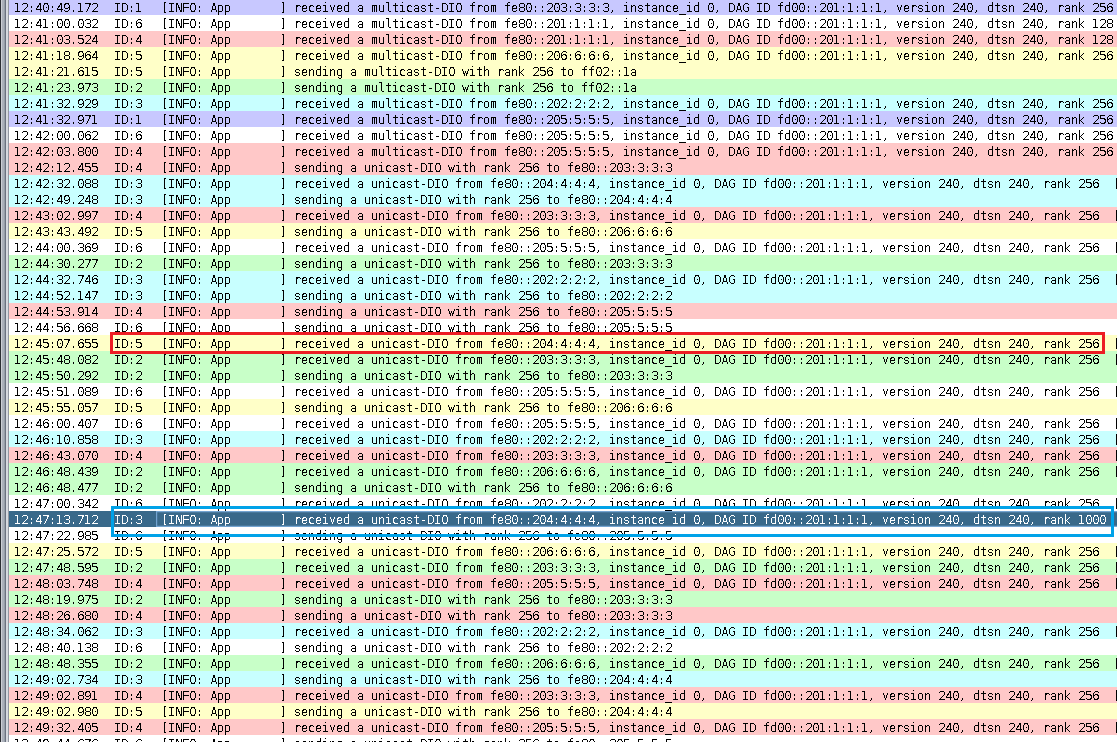
Per semplificare la visualizzazione è stato cerchiato in blu il messaggio DIO indirizzato al nodo 3 con rank fasullo, mentre in rosso è stato evidenziato il messaggio DIO che riceve il nodo 5 contente il valore di rank reale del nodo 4.

Figura 5a: Rank Attack

**Mitigazione**

Esistono diverse tecniche per mitigare tale tipologia di attacco, nel nostro caso di studio abbiamo deciso di adottare una tecnica di analisi statistica basata sul valore di rank dei nodi vicini. L’idea alla base di tale tecnica risiede nella convinzione che generalmente il valore di rank di un nodo, non può essere eccessivamente diverso rispetto a quello degli altri vicini. Il nostro obiettivo, quindi, è stabilire una soglia e considerare corretto il valore del rank solo se inferiore a tale soglia. In [4] viene proposto di calcolare tale valore di soglia nel seguente modo:

Dove:

* **MaxRank:** è il massimo valore di rank tra i vicini del nodo corrente.
* **N**: è il numero di vicini del nodo corrente.
* **K**: è una costante da determinare in modo sperimentale in funzione della topologia della rete.
* **RankMed**: è il rank medio dei vicini.

Di seguito è possibile visionare il corretto funzionamento della mitigazione, proponiamo un confronto rispetto al DAG del nodo vittima con e senza mitigazione attiva, dove in quest’ultimo caso possiamo osservare l’assenza del valore 1000 associato al rank del nodo attaccante.

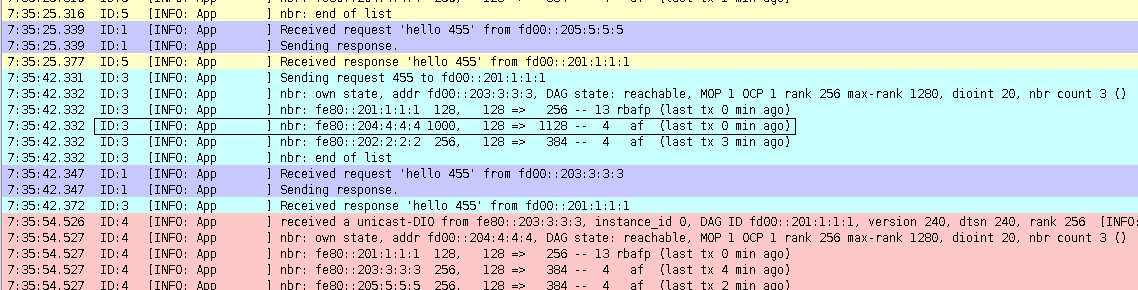


Figura 5b: Rank Attack. Mitigazione Disattivata.

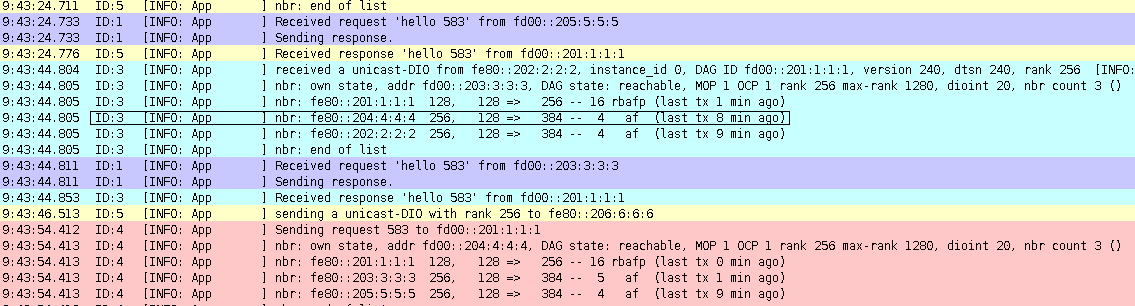
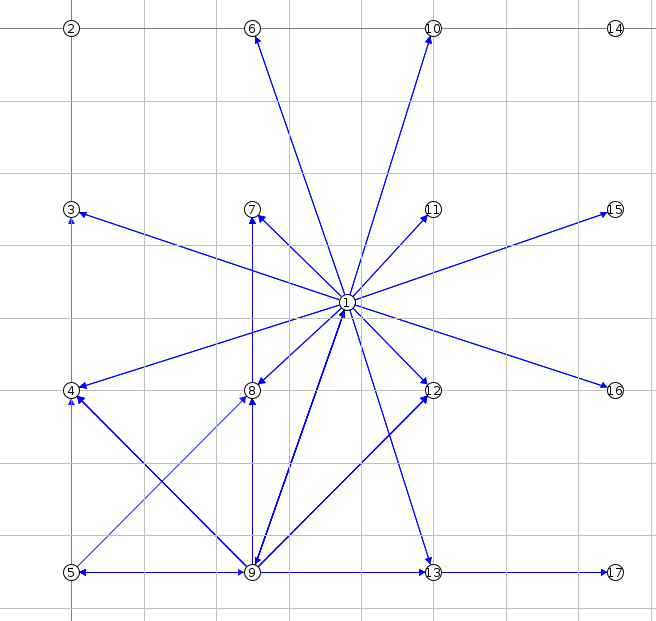


Figura 5c: Rank Attack. Mitigazione Attiva.

Variante 2

In questo secondo scenario affrontiamo uno scenario più complesso in cui troviamo due nodi malevoli (ID= 2 e 4) che inviano dai rank fasulli ai nodi 3 e 8. In questo modo si provoca un aumento di messaggi di controllo che RPL utilizza per sistemare il DAG, il che può comportare ritardi nella ricezione dei pacchetti. In modo analogo al precedente mostriamo i due scenari con e senza mitigazione.



Il codice, opportunamente commentato, relativo a questo attacco e le rispettive simulazioni avviabili con Cooja sono presenti all’interno delle seguenti cartelle:

* Attacchi/Rank.
* Attacchi/Complex/Rank.

Continua……

**Altri attacchi...**

***Conclusioni***

Con il seguente elaborato sono stati implementati i seguenti attacchi: DoS Attack, Rank Attack, Fragment Duplication Attack e Warmhole Attack; in un ambiente IoT simulato attraverso l’uso del sistema operativo Contiki-NG e del simulatore Cooja. È stata fornita una breve trattazione dei principali protocolli trattati, evidenziando la loro importanza ed il ruolo assunto nei diversi scenari applicativi in riferimento sia ad un ambiente sicuro che ad un ambiente esposto a rischi. È stata descritta inoltre la procedura di installazione e configurazione dell’ambiente di sviluppo. Per concludere l’elaborato è bene fare presente ad eventuali assunzioni effettuate riguardo l’implementazione delle soluzioni proposte e l’ambiente di sviluppo:

* Per quanto riguarda l’attacco DoS, la mitigazione assume che la rete, intesa in numero di nodi, rimanga costante. Quest’assunzione è dovuta dall’impossibilità di passare argomenti al simulatore a tempo di esecuzione. Quest’assunzione non mira però in alcun modo l’efficacia o la generalità della soluzione proposta, in un ambiente reale, infatti, è sufficiente sostituire le allocazioni di memoria statiche, con delle allocazioni dinamiche (esempio usando la funzione malloc) in modo da poter allocare nuovo spazio, per memorizzare le informazioni suoi nuovi nodi, qualora fosse necessario.
* Sempre in riferimento al DDoS con mitigazione, è bene precisare che sono state effettuate simulazioni anche su reti più complesse, formate da 30+ nodi con diversi attaccanti e diverse vittime. Sebbene il tutto continui a funzionare correttamente, è stato scelto di non presentare tale scenario. L’elevato numero di messaggi scambiati, infatti, rende poco chiaro il contesto e richiede un’attenta analisi del log completo, che per questioni di leggibilità, si è deciso di non allegare vista la sua eccessiva lunghezza.
* Il rank attack può essere utilizzato come vettore di partenza per la costruzione di altri attacchi, come ad esempio il Sinkhole o il DoS. Analizzando quest’ultimo esempio, infatti, un nodo malevolo combinando Rank Attack e IP Spoofing, potrebbe inviare pacchetti DIO sulla rete, contenenti un valore di rank ottimale e l’indirizzo IP del nodo vittima. In tal modo gli altri nodi della rete sceglieranno il nodo vittima come nodo di inoltro dei pacchetti e questo potrebbe causare un DoS su tale nodo, se il numero di pacchetti è eccessivamente elevato.

Aggiungere descrizione script avvio…..

**Bibliografia**

[1] K. K. Rai and K. Asawa, "Impact analysis of rank attack with spoofed IP on routing in 6LoWPAN network," 2017 Tenth International Conference on Contemporary Computing (IC3), 2017, pp. 1-5, doi: 10.1109/IC3.2017.8284340.

[2] P. Perazzo, C. Vallati, D. Varano, G. Anastasi and G. Dini, "Implementation of a wormhole attack against a rpl network: Challenges and effects," 2018 14th Annual Conference on Wireless On-demand Network Systems and Services (WONS), 2018, pp. 95-102, doi: 10.23919/WONS.2018.8311669.

[3] Hummen, René & Hiller, Jens & Wirtz, Hanno & Henze, Martin & Shafagh, Hossein & Wehrle, Klaus. (2013). 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms. 10.1145/2462096.2462107.

[4] Iuchi, Kenji & Takumi, Matsunaga & Toyoda, Kentaroh & Sasase, I.. (2015). Secure Parent Node Selection Scheme in Route Construction to Exclude Attacking Nodes From RPL Network. IEICE Communications Express. 4. 10.1587/comex.4.340.