Agenzia nazionale per le nuove tecnologie,
l'energia e lo sviluppo economico sostenibile

MINISTERO DELLO SVILUPPO ECONOMICO

Ricerca di Sistema elettrico

Telecontrollo digitale Smart Street: riproduzione di situazione di degradamento prestazioni ed analisi dei ritardi di servizio e studio dei servizi aggiuntivi

Giuseppe Bernieri, Federica Pascucci

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Report RdS/PAR2016/018

TELECONTROLLO DIGITALE SMART STREET: RIPRODUZIONE DI SITUAZIONE DI DEGRADAMENTO PRESTAZIONI ED ANALISI DEI RITARDI DI SERVIZIO E STUDIO DEI SERVIZI AGGIUNTIVI

Giuseppe Bernieri, Federica Pascucci (Università degli Studi Roma Tre)

Settembre 2017

Report Ricerca di Sistema Elettrico
Accordo di Programma Ministero dello Sviluppo Economico - ENEA
Piano Annuale di Realizzazione 2016
Area: Efficienza energetica e risparmio di energia negli usi finali elettrici e interazione con altri vettori energetici
Progetto: D.6 Sviluppo di un modello integrato di smart district urbano
Obiettivo: c. Controllo e valutazione delle infrastrutture pubbliche energivore
Responsabile del Progetto: Claudia Meloni, ENEA

Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione ""Telecontrollo digitale Smart Street: riproduzione di situazione di degradamento prestazioni ed analisi dei ritardi di servizio e studio dei servizi aggiuntivi""
Responsabile scientifico ENEA: Francesco Pieroni
Responsabile scientifico: Prof.ssa Federica Pascucci

Indice

Sommario

Il presente documento riporta le attività riguardanti la riproduzione di situazioni di degradamento delle prestazioni el'analisi dei ritardi della rete di comunicazione per servizi aggiuntivi nelle Smart Street.

In particolare esso riporta

1. analisi di alcuni sistemi di telecontrollo digitale per le Smart Street: sono presi in considerazione otto diversi sistemi sviluppati da piccole/medie imprese o grandi multinazionali. Questi sistemi sono un campione di quelli presenti nel mercato e vengono presi a titolo di esempio

2. breve descrizione delle installazioni di Smart Street presenti nel mondo e sviluppate dalle aziende esaminate in precedenza. Una descrizione più puntuale viene fatta del sistema installato nello Smart Village Enea – Casaccia con particolare attenzione alle possibili vulnerabilità del sistema.

3. Presentazione del test-bed di replica dell'architettura di rete Smart Village ENEA – Casaccia e descrizione dei test che sono stati eseguiti per la valutazione delle prestazioni.

Dall'analisi del sistema di Smart Street installato presso ENEA – Casaccia emerge che, a causa del collegamento Internet tra sistema di telegestione digitale per Smart Street e centrale operativa, i servizi associati potrebbero essere degradati. Per tale motivo sono stati effettuati i test di Denial of Service (DoS) per valutare quantitativamente il degrado delle prestazioni.

1 Introduzione(PowerLineCommunication)

L'illuminazione stradale rappresenta un'infrastruttura importante sia nelle zone urbane che in quelle rurali: essa è in grado di rendere le vie più sicure sia per i pedoni che per gli automobilisti.

Il costo dell'illuminazione stradale è in genere a carico delle municipalità e ha rappresentato per lungo tempo una delle maggiori spese di bilancio. Gli operatori dell'energia hanno spesso offerto tale servizio ad un costo fisso, tuttavia, con la rivoluzione del mercato elettrico, spesso anche l'illuminazione pubblica viene pagata a consumo.

La prima fonte di risparmio è rappresentata dalla sostituzione delle lampade al sodio con corpi illuminanti a LED. Questi ultimi consentono un duplice risparmio essendo più efficienti dal punto di vista energetico e meno soggetti a manutenzione rispetto alle lampade tradizionali.

Il risparmio economico ed energetico, tuttavia, rappresenta solo una parte di quello che si potrebbe avere considerando un sistema Smart Street, ossia connettendo in rete il sistema di illuminazione stradale e fornendo ulteriori servizi.

La connessione dei lampioni in rete, secondo il noto paradigma dell'Internet of Things (IoT) consente ulteriori abbattimenti di costi. Dal punto di vista energetico, infatti, è possibile impostare dei profili di illuminazione più articolati in grado di ridurre il consumo energetico. Dal punto di vista della manutenzione è possibile identificare ed isolare un guasto o verificare una segnalazione senza mandare squadre sul posto.

Portando connettività nelle Smart Street si fornisce alla cittadinanza la possibilità di fruire di ulteriori servizi, non strettamente legati all'illuminazione. Ad esempio, su un lampione intelligente si possono installare sensori per il monitoraggio della qualità dell'aria, il controllo del traffico in tempo reale o telecamere di sicurezza e facilmente connetterli alla rete.

Come ogni nuova tecnologia, la Smart Street va introdotta prestando attenzione non solo ai vantaggi che porta, ma anche alle sfide. Una di queste, oggetto del presente report, è la sicurezza. La connettività, come apre la porta a nuovi servizi, così apre la porta a problemi relativi alla sicurezza.

Lo scopo di questo report, quindi, è duplice: da una parte mostrare alcune soluzioni già disponibili sul mercato analizzandone le architetture, dall'altra analizzare le degradazioni della qualità del servizio a causa di attacchi informatici sul sistema Smart Street ENEA presente nella sede ENEA di Casaccia.

Il documento si articola in tre macro-sezioni:

- *Analisi dei principali sistemi per Smart Street presenti sul mercato*: vengono analizzate le architetture proposte sul mercato nazionale ed internazionale
- *Analisi di alcune installazioni di Smart Street:* vengono presentate alcune installazioni di Smart Street presenti nel mondo ed in particolare la Smart Street ENEA
- *Analisi delle prestazioni della Smart Street ENEA in presenza di attacchi di Denial of Service (DoS):*vengono presentati alcuni test effettuati sulla Smart Street ENEA quando le prestazioni del servizio di monitoraggio vengono degradate da attacchi che compromettono l'efficienza della rete

2 Sistemi di telecontrollo digitale per Smart Street e servizi aggiuntivi

L'introduzione di sistemi di Smart Street prevede anche la possibilità di introdurre servizi aggiuntivi, non necessariamente legati all'illuminazione stradale. Negli ultimi anni questa possibilità ha suscitato l'interesse di diverse aziende che operano non solo nel settore dell'illuminazione, ma anche in quello che si collocano nell'ambito del mercato IoT.

Nel presente paragrafo vengono presentate le architetture di alcuni operatori presenti sul mercato internazionale. La scelta delle aziende è stata effettuate in base alla possibilità di reperire pubblicamente il materiale per descrivere i loro sistemi.

In linea generale, il mercatorisulta diviso in due segmenti: da una parte di ci sono le grandi aziende che, insieme agli operatori telefonici, sono in grado di fornire servizi e di trasformare grandi sistemi di illuminazioni in Smart Street; dall'altra ci sono piccole e medie imprese in grado di sviluppare architetture competitive. L'attenzione di questo report, lungi dall'essere completo ed esaustivo, si è fermata soprattutto su quest'ultime, in quanto più attente a sviluppare soluzioni in cui i servizi aggiuntivi possano essere facilmente integrati.

Come già sottolineato, l'introduzione delle Smart Street porta nuove sfide legate soprattutto alla sicurezza informatica del sistema. Tradizionalmente questa viene approcciata secondo il paradigma Confidenziality, Integrity e Availability (CIA), che rispecchia la confidenzialità, l'integrità e la disponibilità di un dato. Nel caso delle Smart Street, così come avviene per i sistemi di controllo industriale, la disponibilità del dato ha un peso nettamente maggiore rispetto alla confidenzialità e all'integrità. La availability risulta così importante, che recentemente si è introdotto, come ulteriore termine di valutazione, anche la Quality of Service (QoS), che significa la possibilità di disporre di un dato in maniera certa entro un determinato istante temporale.

L'analisi proposta nel seguito presenta l'architettura dei sistemi analizzandone i componenti principali (di cui vengono proposte anche le specifiche tecniche da datasheet), il sistema di comunicazione e le soluzioni di sicurezza adottate.

2.1 Il sistema UVAX (Spagna)

L'architettura per implementare il sistema di telecontrollo digitale per Smart Street di UVAX si compone essenzialmente di tre elementi:

- **Nodi** sono installati sui singoli corpi illuminanti e sono collegati tramite rete ad onde convogliate (rete PLC - PowerLineCommunication) ai concentratori. Essi sono dotati di indirizzo IP unico e si comportano da modem PLC, inviando e ricevendo informazioni dalla powerline, senza ulteriori necessità di cablaggio. I nodi controllano i corpi illuminanti, consentendo la variazione dell'illuminazione, ma possono integrare dispositivi diversi (GPS, ripetitori Wi-Fi, contatori intelligenti, sensori di temperatura e luce, telecamere).

- **Concentratori** sono installati generalmente all'interno delle cabine elettriche. Essi controllano i nodi direttamente collegati tramite rete ad onde convogliate e si interfacciano con il backbone della rete (in genere Ethernet wired/wireless) del management center.

- **Central Management Software (CMS)**web app attraverso cui il gestore del sistema accede all'infrastruttura in maniera sicura mediante autenticazione e cifratura e può impostare e configurare ogni singolo elemento della rete.

I nodi ed i concentratori hanno lo stesso firmware e implementano lo stesso livello fisico. Per trasmettere utilizzano entrambi la OFDM che presenta numerosi vantaggi in termini di robustezza dovuti all'approccio a bassa frequenza della modulazione. Questo infatti consente da una parte di semplificare l'equalizzazione del canale, dall'altra di trasmettere dati attraverso cavi in rame caratterizzati da interferenze e multipath. In particolare viene utilizzato la modalità High Ultra Reliable Transmission OFDM (HURTO)[2], in cui i canali vengono selezionati in maniera adattativa rispetto alla qualità della connessione e le trasmissioni ridondate in modo da garantire la qualità del servizio.
Il sistema di telecontrollo digitale per Smart Street UVAX ha la capacità di auto-configurarsi con una topologia ad albero, la cui radice è rappresentata dai concentratori. Ogni nodo, infatti, ha un numero limitato di porte di comunicazione PLC, pertanto l'organizzazione ad albero consente di massimizzare la connessione tra un numero alto di nodi nella rete. I livelli degli alberi vengono aumentati quando un nodo *parent* ha esaurito la sua capacità di connessione: un nuovo nodo che appare sulla rete sceglie come riferimento una foglia cui connettersi. La rete è altamente flessibile, in quanto la configurazione può cambiare al verificarsi di un evento (spegnimento di un nodo, attivazione di un nodo a maggiore capacità.

Specifiche elettriche	
Tension input	100 – 277 VAC
Frequenza input	50 – 60 Hz
Fattore di potenza	>0.80
Massima potenza	15W
Massima tensione di uscita	4,5 V (RMS)
Massima corrente di uscita	70mA
LAN	Ethernet
Cablaggio	CAT-5
Specifiche ambientali	
Indoor	IEC 60529, IP43
NEMA2	Type 1
Temperatura di esercizio	-25°C - 60 °C
Temperatura	-25°C - 85 °C
Tc	65 °C
Certificazioni	
2006/95/CE	EN60950-1:2006+A11:2009 EN60529_1991+A1:200
2004/108/CE	EN55022:2006+A1:2007 EN61000-3-2:2006 EN61000-3-3:2008 EN61547:1995+A1:2000 TGN17
UL	UL 916, 4 Edition, 2010-06-04
FCC	FCC CFR47 PART15 SUBPART B ICES-003 ISSUE 5

Tabella 2.1 Specifiche tecniche dei concentratori UVAX [1]

2.2 Il sistema BEGHELLI (Italia)

L'architettura per implementare il sistema di telecontrollo digitale per Smart Street di BEGHELLI si compone essenzialmente dei seguenti elementi:

- **Centrale domotica** invia agli apparecchi di illuminazione i comandi necessari per regolarne il funzionamento e riceve dagli apparecchi stessi le informazioni di stato, di diagnostica e i dati di consumo di energia. Essa è in grado di pilotare singolarmente ogni diverso apparecchio di illuminazione connesso. La centrale coordina il funzionamento della rete di comunicazione magliata che consente il controllo degli apparecchi di illuminazione anche in sistemi di grandi dimensioni mediante instradamento automatico dei pacchetti informativi attraverso la rete costituita dagli apparecchi di illuminazione e di emergenza. Quando è collegata ad una rete WiFi può essere raggiunta e comandata in remoto direttamente da Smartphone.

- **Interfaccia trasmettitore radio domotico** è un dispositivo radio di interfaccia, alimentato a 230Vac in grado di inviare comandi radio agli apparecchi di illuminazione o agli opportuni ricevitori dotati di attuatori a relè. Attraverso il software di gestione e configurazione è possibile programmare le funzionalità domotiche legate all'illuminazione. L'interfaccia ha l'antenna integrata e può essere inserita in qualsiasi box non schermato. Le funzionalità associabili al trasmettitore sono la trasmissione di comando temporizzato e la trasmissione dello stato del dispositivo.

- **Interfaccia ricevitore radio domotico con Modulo radio per la rilevazione dei dati consumo energetico:** è un dispositivo radio di interfaccia, alimentato a 230Vac, che integra un relè in grado di pilotare apparecchi di illuminazione e altri carichi elettrici. Il ricevitore integra anche un misuratore della potenza e un contatore dell'energia elettrica erogata in uscita. I dati del contatore sono letti mediante messaggi radio e per questo è abilitato al progetto Grande ESCo Italia. Il dispositivo è associato a uno o più trasmettitori radio e ne attua i comandi corrispondenti.

- **Software SD manager** dopo l'installazione, il gestore del sistema accede all'infrastruttura tramite un'apposita applicazione (Software SD manager) di rete in maniera sicura mediante autenticazione e cifratura. L'amministratore può impostare, configurare ogni singolo elemento della rete. Gli elementi sono connessi tra loro in una rete mesh e comunicano con la centrale domotica.

La rete di controllo è di tipo wireless ed è realizzata mediante un protocollo sicuro proprietario, che si basa sul noto standard LoRa. Il protocollo consente di realizzare reti mesh per raggiungere tutti gli elementi illuminanti dotati di Interfaccia trasmettitore radio domotico.
La comunicazione sul canale wireless è criptata, garantendo l'integrità dei dati. La sicurezza è anche garantita a livello di confidenzialità mediante opportuni sistemi di autenticazione degli utenti.

Caratteristiche generali	
Grado di protezione	IP20
Temp. ambiente	-25°C - 40 °C
Installazione	Su barra DIN 9 moduli
Trasmissione locale	Fino a 500 dispositivi radio gestibili tra lampade di illuminazione, di emergenza e dispositivi domotici
Trasmissione remota	Sistema radio Spread Spectrum SFH DSSS su 16 canali
Funzione	Completo controllo del funzionamento del sistema di illuminazione: - Accensione/spegnimento fino a 256 gruppi - Impostazione dei livelli di dimmer - Definizione della modalità di funzionamento (luminosità fissa al valore impostato oppure regolazione automatica della lumonisità) - Diagnostica - Misura della enerfia consumata e risparmiata - Creazione di scenari luminosi - Accensione/spegnimento temporizzati di gruppi di lampade - Configurazione dell'impianto di illuminazione - Gestione di tutte le funzionidel sistema di emergenza - Sincronizzazione e temporizzazione delle funzioni di test - Inibizione/abilitazione dell'emergenza - Gestione dettagliata degli errori

Tabella 2.2 Specifiche tecniche della centrale domotica Beghelli [2]

2.3 Il sistema Luminibus – APS Systems (Italia)

Rappresenta uno di sistemi di telegestione punto-punto degli impianti di illuminazione pubblica più avanzati. Esso utilizza un'architettura scalabile composta dai seguenti elementi.

- **Nodo concentratore M^{3}C-CB200**:gestisce e controlla in maniera remota gli armadi elettrici ed ogni singolo lampione. La comunicazione avviene tramite rete powerline. Grazie alle interfacce I/O integrate consente la gestione dell'impianto mediante programmazione remota e automatizzata, la trasmissione di allarmi, guasti e misure elettriche.

- **Nodo powerline M^{3}PLN/5-Lx** trasforma ogni singolo punto luce in un nodo di rete; esso è in grado di accendere e spegnere il corpo illuminante, acquisire informazioni di diagnostica, fornire dati sul consumo. Il corpo illuminante connesso al nodo M3-PLN/5-Lx è in grado di operare in accordo al piano di illuminazione previsto, gestendo il flusso luminoso richiesto, attivando profili luminosi in modalità sia standalone che in quella telegestione(ossia, controllato in modalità PowerLine dall'unità di concentrazione presente nel quadro elettrico e dal centro di controllo remoto con protocollo IP).La comunicazione dati tra M3-PLN/5-L e l'unità di concentrazione serie M3-CB200 avviene in modalità PLC con protocollo aperto conforme allo standard Meters&More.

- **Piattaforma Software M3-SCS**è la piattaforma applicativa disponibile in cloud che interagisce con il sistema LUMINIBUS per trasformare l'impianto di illuminazione in una rete di comunicazione dati a tecnologia mista (PLC e reti wireless pubbliche) per la telegestione e la fruizione dei servizi di smart city.

La piattaforma software M3-SCS rappresenta il punto di forza dell'architettura LUMINIBUS. Essa si configura come una piattaforma aperta che permette l'accesso ad addetti ai lavori, amministratori e cittadini. Per questo motivo essa è in grado di fornire servizi diversificati in base all'utenza.

Per gli addetti ai lavori consente la telegestione e la diagnostica punto-punto. Per semplificare le operazioni di manutenzione è disponibile una rappresentazione cartografica dei dispositivi di diagnostica, delle infrastrutture e dei servizi di Smart City basata su Google-Maps. La piattaforma M3-SCS dispone di un sistema di ticketing grazie al quale si raccolgono le segnalazioni e si supporta l'organizzazione delle attività di manutenzione. M3-SCS prevede anche una sezione dedicata al ciclo di vita degli apparati utilizzati sul campo per la telegestione ed i servizi di smart city; è possibile impostare ed aggiornare le fasi di vita che lo riguardano con informazioni sullo stoccaggio, installazione, manutenzione e dismissione degli stessi. Per facilitare il coordinamento delle attività di manutenzione sul campo, l'applicazione è disponibile anche su app.

Per gli amministratori fornisce informazioni puntuali sullo stato del sistema ed aggregate sulle performance e il consumo energetico. Queste statistiche sono rese disponibili in maniera dinamica mediante report che possono essere caricati su una pagina web di un sito istituzionale per informare l'utenza.

Per il cittadino offre la possibilità di fruire dei servizi di Smart City (prenotazione colonnine di ricarica, prenotazione di un posto auto, segnalazioni allarmi o incidenti, segnalazione malfunzionamenti, etc).

CPU	
CPU	ARM9 33MHz
Performance del processore	366 MIPS
Sistema operativo	Linux embedded
RAM	256 Mbytes
Memoria di massa	256 Mbytes (tipo di memoria NAND)
Real time clock	gestione integrata dell'orologio astronomico
Tecnologie di comunicazione dati	
Modem powerline	modem powerline tri-fase conforme a EN500061-1 e funzionante su banda CENELEC A, B, C con protocollo aperto Meters&More
Wide Area Network (WAN)	porta Ethernet (standard) - modem GPRS/3G/4G (opzionale)
Interfacce I/O	
Contatori per accensione on/off	con 2 uscite su relè
Ingressi digitali	4 ingressi digitali optoisolati
Altre I/O	n. 1 porta RS-485 n. 1 porta RS-232 con connettore DB9-f n. 1 USB female connector port n. 1 porta IEE802.3 con porta Ethernet 10-100Mbps n. 1 uscita 12VCC per alimentare dispositivi aggiuntivi n. 1 connettore per batteria di backup esterna (opz.)
Opzionali	modem GPRS/3G/4G analizzatore rete elettrica
Caratteristiche meccaniche ed ambientali	
Materiale involucro	materiale autoestinguente XAN-940A (standard UL94) permontaggio su guida DIN
Temperatura di esercizio	-25°C - +70°C [-13°F - +158 °F]
Dimensioni esterne	131 x 255 x 49 mm (HxWxD)

Tabella 2.3 Specifiche tecniche del nodo concentratore Luminibus [3]

La piattaforma M3-SCS è accessibile mediante APP per smartphone oppure mediante i più comuni browser, compresi quelli mobile come smartphones e tablets. La confidenzialità dei dati è garantita dal controllo degli accessi in base al profilo utente. I protocolli di comunicazione utilizzati sono aperti: questo da una parte può ridurre la sicurezza, ma ne aumenta la possibilità di espansione verso applicazioni di Smart City e smart metering.

Principali caratteristiche piattaforma software	
Architettura	3-tier
Tipologia di piattaforma	piattaforma orientata ai servizi (SOA) gestibile tramite postazione operatore web-based
Tecnologia	C#.NET, HTML5, CSS, Hasvascript, HTTP RESTful WS
Interoperabilità	trasporto HTTP, RESTfull WS, formati JSON/XML
Sicurezza	HTTPS, TLS/SSL
Performance	.NET, APS.NET MVC, SQL Server
Scalabilità	scalable session state mgmt, stateless ws, database cluster
Robustezza	supporta architetture di failover e high availability
Estendibilità	1 servizio = 1 plug-in
Multi-canalità	web app, mobile app
Ottimizzazione	gestione ottimizzata per esercizio e consuntivo basata su db eservizio, datawarehouse e piattaforma di business intelligence
Affidabilità	ciclo ALM chiuso, ambiente di sviluppo/test integrato, monitoring/log/ trace tool disponibili
Mappe	gestione integrata di Google Maps

Tabella 2.4 Specifiche tecniche della piattaforma software Luminibus [4]

2.4 Il sistema PLANet – Telensa (Regno Unito)

Il sistem PLANet di Telensa rappresenta uno dei sistemi di telecontrollo per smart lighting maggiormente installati. La sua architettura si basa sui seguenti elementi

- **Base station:** viene installata in alto (ossia sulla sommità di pali o sui tetti) per garantire la più ampia copertura. L'antenna della base station, in genere, può coprire fino a 1-5km in zone urbane e 5-10kmin zone rurali. La base station ha due interfacce di comunicazione. L'una è di tipo radio ultra narrowband (UNB) e serve per comunicare con le antenne dei dispositivi Telecell del sistema di illuminazione (sono garantite fino a 5.000 connessioni). L'altra è di tipo 3G o Ethernet e serve per connettere la base station al server centrale. Nella base station si trovano anche un processore e un sensore di luminosità: essi servono per programmare la luminosità dell'area connessa alla base station.

- **Luminaire component** è rappresentato dal dispositivo Telecell, che contiene un'antenna radio UNB, un processore per il controllo, il circuito per il monitoraggio e il controllo del corpo illuminante e sensori per valutare il consumo energetico. Utilizza connettori standard, pertanto può essere installato facilmente su sistemi esistenti. Alcune varianti consentono di inserire antenne radio diverse per garantire la compatibilità con sistemi precedentemente installati.

- **Central System** è il sistema in cui viene installato il software di gestione PLANet. Ogni base station è connessa con questo sistema centrale, che, a sua volta, è progettato per connettere fino a 150.000 corpi illuminanti. Telensa offre un servizio di hosting per i server contenenti i Central System. Il Central System gestisce la comunicazione tra le base station e la base di dati; inoltre essa fornisce un sistema di web server che rappresenta l'interfaccia verso l'utente.

- **User Interface** è implementata come una interfaccia web capace di adattarsi a diversi dispositivi. Può essere richiamata via Internet o intranet e serve per definire il controllo e il monitoraggio di gruppi di corpi illuminanti. Fornisce, interagendo con il database del Central System, le informazioni collezionate dai corpi illuminanti che possono essere raccolti in report facilmente esportabili in file di formato standard (come, ad esempio, CSV o XML).

Il sistema PLANet fornisce tutti gli strumenti per il controllo, la rilevazione dei malfunzionamenti, la reportistica sui consumi energetici ed ha ottenuto la certificazione Elexon CMS per i sistemi di fatturazione nel Regno Unito.

Esso si basa su tecnologia wireless e utilizza i protocolli tipici dell'Internet of Things (IoT). A questa scelta è dovuto il grande numero di installazioni di questo prodotto. In particolare, Telensa ha definito dei protocolli per Ultra Narrow Band (UNB), un particolare tipo di Low Power Wide Area (LPWA) wireless che sta diventando lo standard de facto per le Smart City e per le applicazioni di controllo legate al paradigma IoT. L'utilizzo di questo protocollo crea numerosi vantaggi, quali la facilità di installazione, la mancanza di costi aggiuntivi per realizzare il sistema di comunicazione, la possibilità di scegliere se connettere direttamente o meno un sistema di illuminazione alla rete. Probabilmente il vantaggio più rilevante è la scalabilità della rete e la capacità di questa di adattarsi: ogni dispositivo Telecell, infatti, si collega in automatico alla base station più potente.

Al momento Telensa ha sviluppato il sistema di smart lightning in previsione di aggiungere ulteriori servizi da veicolare sulla rete di comunicazione. Il sistema, nello stato attuale, rimane prevalentemente un sistema di smart lightning.

Specifiche tecniche	
Temperatura di esercizio	20°C - +60°C
Protezione	IP66
Tensione	110V – 277V nominal 50/60Hz

	(single phase A.C)
Dimensioni	285w x165d x 350h mm (1350h mm conantenna)
Peso	8.2kg
Portata antenna	1-5 km urbano, 5-10 miles rurale
I/O	3G, Ethernet
Standard	CE, Elexon (UK)

Tabella 2.5 Specifiche tecniche della base station PLANet [5]

2.5 *Il sistema InteliLIGHT – Flashnet (Romania)*

InteliLIGHT è un'architettura basata su comunicazioni PLC, facilmente integrabile ed adattabile con installazioni convenzionali di sistemi di illuminazione stradali. Il sistema IntelliLIGHT prevede l'utilizzo di software in grado di analizzare le prestazioni del sistema, individuare malfunzionamenti ed integrare servizi tipici delle Smart City. L'architettura è composta da vari livelli:

- **Lamp level** è composto da vari controllori per la rete PLC (inteliLIGHT PLC FPX-220, inteliLIGHTPLC FPE-220/220D, inteliLIGHTPLC FPM-152, inteliLIGHTPLC FPM-402) compatibili con diverse tipologie di corpi illuminanti. Essi sono in grado di gestire e controllare ogni lampione, impostando orari di accensione e spegnimento, livelli di luminosità e riportando eventuali malfunzionamenti.

- **Remote Terminal Unit (RTU) level** rappresenta al contempo l'intelligenza e la comunicazione del sistema. Ogni RTU è inserito in un quadro elettrico e riceve da remoto i comandi da inviare ai controllori dei lampioni (lamp level). Al suo interno sono presenti alcuni moduli in grado di analizzare e pre-processare alcuni dati. In particolare è composto da
  - *Data concentrator/Smart server* utilizza la tecnologia Echelon powerline per ricevere dati dal canale PLC. I dati ricevuti sono convertiti nel protocolloLONWORKS/ANSI709.1 e inviati al software control level mediante un qualsiasi canale di comunicazione scelto dall'utente (PLC, Ethernet, Infrarosso, fibra ottica). Al suo interno sono implementate alcune procedure di sicurezza che vengono utilizzate in caso di perdita del canale di comunicazione con il software level.
  - *Electric Network Analyzer* fornisce al inteliLIGHT StreetLight Control software i parametri elettrici ed eventuali allarmi.
  - *Voltage presence monitor* fornisce informazioni sulla tensione della rete.
  - *Intelligent communicator*: il cuore della RTU, contiene le procedure di processamento, recovery e trasmissione dei dati.

- **Software control level**consente il telecontrollo, la manutenzione e la gestione del sistema di illuminazione intelligente. Si presenta come una piattaforma aperta in grado di comunicare utilizzando differenti standard e protocolli (ad esempio dispositivi di terze parti che utilizzano PLC, LoRaWANTM or GSM/GPRS). Si basa sulla piattaforma inteliLIGHT StreetLight Control software, una piattaforma cloud cui si può facilmente accedere tramite computer o dispositivi mobili. Questa piattaforma fornisce la possibilità di reportistica che può essere facilmente adattata ai diversi utenti. Le funzionalità delsoftwareinteliLIGHT StreetLight Control prevedono di poter scalare all'aumentare dei corpi illuminanti connessi. Sono disponibili strumenti per raggruppare il controllo di lampioni, pianificare la manutenzione, fornire degli allarmi in caso di malfunzionamento. La visualizzazione grafica è supportata da mappe (basandosi su ESRI GIS, Google maps, Open

Streetmaps, etc.) e la manutenzione prevede l'utilizzo di un'apposita app. Al suo interno sono previsti anche strumenti per l'analisi dei dati.

La piattaforma inteliLIGHT è stata sviluppata appositamente per le Smart City, pertanto essa prevede la possibilità di gestire diversi sensori e diverse funzionalità. Essa è in grado di fornire un'infrastruttura wireless di comunicazione ad alta velocità. Può essere utilizzata per implementare un'infrastruttura di sicurezza basata su telecamere e sensori. Ancora può fornire l'infrastruttura di comunicazione per creare sistemi di monitoraggio della qualità dell'ambiente o per regolare il traffico urbano.

Le comunicazioni sono di due tipologie: powerline communication dalla RTU ai corpi illuminanti e basate su IP dalla RTU al software di gestione. La comunicazione PLC utilizza un protocollo proprietario LonWorks. Esso prevede la possibilità di ripetizione nella trasmissione dei dati e di adattamento nel caso di grandi infrastrutture. La comunicazione tra RTU e software di controllo utilizza qualsiasi mezzo fisico disponibile (Ethernet, GPRS, 3G, etc). Per rendere sicure le comunicazioni sono create delle connessioni VPN e particolari algoritmi per il bilanciamento dei carichi sulla rete di comunicazione vengono utilizzati per assicurare la continuità del servizio.

Tutte le comunicazioni vengono criptate per garantire l'integrità dei dati scambiati all'interno del sistema e il software viene continuamente aggiornato per limitare o eliminare le vulnerabilità. La confidenzialità dei dati è garantita da un sistema di controllo degli accessi basato su profilazione dell'utente.

FRB-110 intelligent communicator	
Processore	High performance industrial processor (400 MHz, 400 MIPS)
Memoria	8Mbyte Flash, 128Mbyte NAND Flash, 128Mbyte SDRAM
Memoria esterna	8Mbyte Flash, 128Mbyte NAND Flash, 128Mbyte SDRAM
Funzioni di sicurezza	Built-in operation monitoring Mobile connection recovery SNTP time handlink SIM PIN-code Certificati basato su connessione VPN sicura Sistemi di accesso controllato
I/O	1x Ethernet port (10/100, RJ45) 2x USB 2.0 connector(High Speed) 1x Micro-SD memory card slot (max. 32 GB) 1x Push insert SIM-card bay 4-pin Microfit power connector 3x SMA-M 50 Ohm antenna connector (WiFi, 2G-3G) Internal conn. for expansion modules
Alimentazione	6-30 VDC, 4-pin Microfit connector 12V 2A Consumo: max 8W
Accessori opzionali	SMA antenna, DIN-rail fix. Unit RS232 extension module (serial port) RS232/RS485 module (Modbus TCP, RTU, M-bus master communication) 868MHz ShortRF radio expansion module (AMR meters, Wireless M- bus)

	IO-extender board (for analog/digital input and output lines) Zigbee module (for wireless sensors)
Protezione	IP 51 protection
Dimensione	95x45x130mm(l x w x h)
Temperatura di esercizio	-30°C - +65°C con umidità relativa 5 – 95
Certificazione	CE, R&TTE 99/5/CE, FCC, ROHS

Tabella 2.6 Specifiche tecniche RTU InteliLIGHT [6]

2.6 Lo Smart Outdoor Control and Management System – Billion (Taiwan)

Smart Outdoor Control and Management System (Smart outdoor LCMS) è una piattaforma per il monitoraggio e il controllo di ambienti smart all'aperto (parcheggi, campus, impianti industriali, illuminazione stradale). L'architettura è composta da diversi dispositivi e sistemi di gestione software, nello specifico

- **Intelligent Power Line Street Lighting Control Box** gestiscono il singolo corpo illuminante, comunicando tramite power line allo Powerline Smart Streetlight Wireless Bridge o direttamente al Powerline Smart Streetlight Segment Controller. Più dispositivi possono essere connessi configurandosi come segmenti

- **Broadband Powerline Smart Streetlight Wireless Bridge** collegano i segmenti della rete remoti tramite collgamento wireless. Pertanto hanno un'interfaccia powerline che li college alle varie Power Line Street Lighting Control del segmento e un'interfaccia wireless per collegarsi con il sistema di controllo remoto

- **Broadband Powerline Smart Streetlight Segment Controller** ha un'interfaccia PLC verso la rete di illuminazione ed una 3G verso il sistema di controllo remoto.

- **Sistema di controllo** remoto consente di pianificare l'accensione/spegnimento di ogni segmento, la manutenzione. Esso consente l'inserimento di altri sensori e la visualizzazione tramite supporto di mappe (Google, Bing, ArcGIS, and Open Layer-Open Street).

Il sistema Smart Outdoor LCMSTM è progettato per le Smart City e inserisce la possibilità di realizzare reti ibride (ossia composte in parte da reti PLC e in parte da reti wireless/wired). La confidenzialità dei dati è protetta dal controllo di accesso. Il sistema fornisce alcuni strumenti di analisi dei dati e reportistica.

Standard	Broadband over powerline
Freq. trasm	2MHz ~ 30MHz
Standard comunicazione	OFDM
Sicurezza	DES, 3DES data encryption
Tensione input	Voltage: AC 100V ~ 277V , 50/60Hz
Wireless LAN	Compliant with IEEE802.11n, 802.11g and 802.11b standards 64/128 bits WEP supported for encryption Wireless security with WPA-PSK and WPA2-PSK support
Management	Web-based for remote and local management Firmware upgrades and

	configuration data upload / download via web-based interface / System Log monitoring
Potenza	12 Watt (Max)
Temperatura di esercizio	-40 °C ~ 60 °C
Umidità	10 % ~ 95 %
Dimensioni	27.5 cm x 18.0 cm x 8.0 cm (L x W x H)

Tabella 2.7 Specifiche tecniche del Broadband Powerline Smart Lighting Wireless Bridge [7]

Standard	Broadband over powerline
Frequenza di trasm.	2MHz ~ 30MHz
Standard comunicazione	OFDM
Sicurezza	DES, 3DES data encryption
Tensione in ingresso	Voltage: AC 100V ~ 277V , 50/60Hz
Protocolli di rete	NAT, static routing and RIP-1 / 2 NAT supports PAT and multimedia applications Transparent bridging Virtual server and DMZ SNTP, DNS relay and DDNS IGMP snooping and IGMP proxy
Gestione firewall	Built-in NAT Firewall Stateful Packet Inspection (SPI) Prevents DoS attacks including Land Attack, Ping of Death, etc. Remote access control for web base access IP, MAC, and URL filtering Password protection for system management VPN pass-through
QoS Control	Supports the DiffServ approach Traffic prioritization based on IP protocol, port number and address
Gestione	Web-based for remote and local management Firmware upgrades and configuration data upload / download via web-based interface System Log monitoring
Potenza	12 Watt (Max)
Temperatura di esercizio	-40 °C ~ 60 °C
Umidità	10 % ~ 95 %
Dimensioni	32.5 cm x 20.0 cm x 10.5 cm (L x W x H)

Tabella 2.8 Specifiche tecniche del Broadband Powerline Smart Lighting Segment Controller [8]

2.7 SmartELI Street Lighting Control System

Il sistema di controllo SmartELI è un sistema wirelss per il controllo di Smart Street e la fruizione di servizi di Smart City. Esso è composto da tre elementi:

- **Wireless Luminaire Controller** gestisce il singolo corpo illuminante. Esso ha un indirizzo IP e può essere controllato mediante una rete mesh basata su protocollo 6loWPAN (IPv6 over Low power Wireless Personal Area). Il Wireless Luminaire Controller consente l'accensione e lo spegnimento del corpo illuminante, il controllo di luminosità e il monitoraggio dei consumi. Ad esso possono essere collegati ulteriori sensori analogici o digitali per i servizi di Smart City. Al suo interno si trovano sensori di temperatura e memoria per memorizzare fino a 52 profili settimanali di funzionamento dei lampioni (equivalenti ad un anno solare di gestione dell'impianto illuminante).

- **Control Cabinet Gateway** è un dispositivo basato su comunicazione 3G capace di gestire in maniera intelligente un sistema di illuminazione all'interno di una via o di un insieme di vie. Può essere connesso con interfacce radio o cablate mediante appositi moduli. Può connettere controllori di dispositivi diversi (corpi illuminanti, colonnine per le ricariche elettriche, paline elettroniche, colonnine per il pagamento dei parcheggi, etc). Esso si collega con il Control Server.

- **Control Server and SmartELI Software** consente di gestire in tempo reale il sistema di illuminazione per Smart Street, può essere installato su server reali o su macchine virtuali. Consente il monitoraggio, il controllo, la rilevazione dei guasti e la manutenzione. Gestisce gli allarmi inviando mail e sms ad operatori remoti. I dati rilevati possono essere facilmente esportati in formato CSV per ulteriori analisi.

Il sistema SmartELI protegge l'integrità dei dati in quanto comunica su canali criptati.La disponibilità dei dati è garantita da sistemi di rilevazione degli errori di comunicazione. La confidenzialità è protetta mediante un controllo degli accessi basato su privilegi.

Specifiche tecniche	
Peso/dimensioni/protezione	65x155x42 mm 200 g Enclosure IP class 44 (optional up to IP67)
I/O	Wireless 2.4GHz IEEE 802.15.4 Encryption AES128
Alimentazione	Tensionee: 230 VAC -15% ...+15% (110 VAC optional) Frequenza: 50/60 Hz (picco di tolleranza 2000 V)
Consumi energetici	Standby mode <0.5 W Operating mode <3 W

Requisiti ambientali	Temperatura di esercizio -40° - +60° C Temperatura: -40° - +65°C con umidità relativa < 95%
I/O	Tensione: 230VAC 50/60 Hz Type: 0-10V or DALI Input digitali: 1 Tipo: TTL compatible, 12V tolerant (motion sensor input)Analog inputs: 2 Type: 12V tolerant (temperatura) Power out: 12VDC 50mA per sensori UART Type: TTL logic Relay output Number: 1 (+1 optional) Changeover relay Load: 250 VAC @2A

Tabella 2.9 Specifiche tecniche del Wireless Luminaire Controller [9 Errore. L'origine riferimento non è stata trovata.**]**

2.8 Philips

Il sistema Philips per la gestione delle Smart Street è rappresentato dalla piattaforma CityTouch. Essa ha una parte hardware composta dai corpi illuminanti (ad esempio la serie Digistreet), che sono predisposti per essere interconnessi con tale piattaforma.

Il sistema CityTouch è basato su web: corpi illuminanti, controllori e cabine sono collegate alle applicazioni di gestione. Il sistema è scalabile e consente di adattare l'illuminazione di una strada o di una zona alle attività che in essa vengono svolte, con particolare attenzione al consumo energetico.

La piattaforma CityTouch si declina attraverso due software principali: l'uno, CityTouch LightPoint, è finalizzato alla manutenzione dell'impianto illuminante, l'altro, CityTouch LightWave è un'app per la gestione in remoto dei sistemi di illuminazione stradale e delle centraline. A livello hardware sono invece previsti degli adattatori wireless. Complessivamente il sistema si articola in questi elementi:

- **CityTouch Ready Luminaries** sono corpi illuminanti contenenti un'antenna wireless per comunicare verso il sistema centralizzato di controllo ed un controller per interagire con il corpo illuminante stesso

- **CityTouch Connector Kit** è il dispositivo che controlla un insieme di lampioni e si connette con i software di gestion

- **LightPoint** semplifica la gestione dell'impianto di illuminazione urbano. Il sistema prevede di visualizzare su mappe le posizioni degli impianti e di gestire i flussi di lavoro per gli interventi di manutenzione mediante grafici e diagrammi intuitivi. Mediante questo strumento è più facile avere informazioni sull'impianto di illuminazione per identificare aree non coperte o nelle quali è possibile ridurre i costi operativi e quelli di manutenzione. Consente di supervisionare le opere di riparazione, semplificando gli interventi di manutenzione di routine. Il software è predisposto per interfacciarsi con i sistemi informativi delle amministrazioni al fine ditenere traccia degli interventi o registrare e documentare i lavori di manutenzione.

- **CityTouch LightWave** è un'applicazione che gestisce, invece, il funzionamento giornaliero dell'impianto. Il sistema, pertanto, si connette con i sistemi di illuminazione e le centraline, in modo da poter controllare i singoli corpi illuminanti o interi settori. Attraverso questo software è possibile programmare l'accensione, lo spegnimento dei corpi illuminanti, regolarne la luminosità in base alle esigenze. Il profilo di illuminazione può essere programmate con un calendario settimanale o giornaliero. Il sistema consente anche di monitorare i consumi energetici, gestisce gli allarmi e le

interruzioni di servizio. Dispone si un sistema di diagnostica remoto che consente di controllare i principali parametri del sistema di illuminazione senza interventi sul campo. Per i consumi energetici sono disponibili anche strumenti di aggregazione dati che consentono di valutare in maniera approfondita l'efficienza energetica.

Le piattaforme citate sono predisposte per l'introduzione dei servizi tipici di una smart city. Per quanto riguarda la sicurezza offrono un livello di protezione piuttosto alto. Le sessioni utente e tutte le comunicazioni sono criptate. La disponibilità di dati storici e la continuità operativa del sistema è garantita mediante un sistema di back up [10].

2.9 Conclusioni

In questa sezione sono stati riportati alcuni sistemi per la gestione di Smart Street, ritenuti rappresentativi rispetto al mercato. In particolare si è posta attenzione sui sistemi integrati prodotti principalmente da piccole e medie imprese.

Tutti i sistemi possono essere accomunati per alcune caratteristiche. In tutti i sistemi, infatti, sono presenti

- Nodi di interfaccia verso il sistema di illuminazione da installare nei corpi illuminanti
- Nodi di raccolta dati da installare nelle cabine elettriche
- Software di gestione con interfaccia utente.

Queste caratteristiche si ritrovano nei sistemi di controllo industriale, di cui i sistemi in oggetto sono una derivazione.

I vari sistemi si differenziano principalmente per il mezzo fisico attraverso cui avviene la comunicazione. Alcuni considerano la comunicazione attraverso powerline, sfruttando il collegamento elettrico, altri utilizzano una connessione wireless, infine alcuni utilizzano connessioni di tipo ibrido.

Un'ulteriore differenza riguarda la collocazione fisica dei software: per alcuni risiede nei nodi concentratori, per altri su appositi server, per altri ancora si appoggia su servizi di cloud esterni.

Tutte le architetture ritengono critica la sicurezza in termini di confidenzialità ed integrità dei dati: tutti i sistemi prevedono un controllo dell'accesso al sistema con differenti privilegi in base alla tipologia di utente e tutti prevedono la protezione dei dati mediante criptazione. Meno sentito sembra essere il problema della disponibilità del dato che viene risolta solo lato sistema di illuminazione consentendo il funzionamento del controllore del corpo illuminante in caso di mancanza di connessione.

3 Sistemi di Smart Street installati

Esistono diversi sistemi di Smart Street installati nel mondo. In questo report vengono presi in considerazione solo i sistemi sviluppati dalle aziende precedentemente descritte. Anche in questo caso, lungi dall'essere esaustivi, si sono considerati i casi che sono sembrati più rappresentativi e di cui è reperibile pubblicamente maggiore materiale informativo. Nello specifico sono state considerate installazioni dei sistemi InteliLIGHT, Billion, Philips ed Eliko: questi sono trattati in maniera simile tramite rapide schede. Per quel che riguarda il progetto che UVAX ha sviluppato nello Smart Village ENEA – Casaccia, invece, si è ritenuta necessaria un'analisi più approfondita.

3.1 Le installazioni InteliLIGHT

Le installazioni InteliLIGHT coprono principalmente l'Europa e l'Asia. Nel seguito sono presentati quattro casi di studio.

3.1.1 Brasov

Brasov è una delle città più grandi della Romania, nota soprattutto come centro turistico. Nel 2014 la municipalità, mediante finanziamenti europei, ha deciso di migliorare l'efficienza del sistema di illuminazione, minimizzando l'impatto sull'infrastruttura già presente. Ancora nel progetto era richiesta l'interoperabilità con telecamere a circuito chiuso e l'installazione di colonnine per l'emergenze.

La soluzione implementata è composta dai seguenti sistemi:

- 2300 x inteliLIGHT FPX-220 ON/OFF controller appositamente progettati per controllare lampioni d'epoca
- 6990 x inteliLIGHT FPM-152 electromagnetic ballast controller
- 2850 x inteliLIGHT FPM-402 electromagnetic ballast controller
- 200 x Remote Terminal Unit equipment sets (FPC-200 data concentrator, FNM-232 electric network analyzer and FRB-110 intelligent communications router).
- 1 x inteliLIGHT streetlight control software

L'installazione del sistema è durata complessivamente 16 mesi, durante i quali il sistema è divenuto a poco a poco disponibile in maniera scalare.

Maggiori informazioni sono disponibili in [11]

3.1.2 Hîncești

Hîncești è una piccola cittadina a pochi chilometri dalla capitale moldava. Nel 2016 la municipalità di Hîncești ha colto l'occasione di rinnovare i sistemi di illuminazione stradale sfruttando la connettività offerta da un operatore telefonico interessato a provare l'infrastruttura LoRaWAN.
La soluzione proposta ha portato all'installazione di

- 62 x inteliLIGHT street lighting controllers
- 4 x inteliLIGHT compatible lighting panel control and monitoring unit
- 1 x LoRaWAN Compatible Network Management Server
- 1 x inteliLIGHTStreetlight Control Software on the Cloud.

Il sistema è in funzione dal novembre 2016 ed ha ottimizzato sia i consumi energetici che i costi di manutenzione.
Maggiori informazioni sono disponibili in [12]

3.1.3 Dubai water canal

Il Dubai Water Canal è una delle più recenti attrazioni turistiche costruite a Dubai. Si tratta di circa 3 km di percorso su cui si affacciano costruzioni architettonicamente all'avanguardia.
L'installazione effettuata è composta dai seguenti elementi

- 5 x Remote Terminal Unit all'interno di pali di alimentazione contenenti concentratori dati, analizzatori di rete e router per le comunicazioni
- 23 x Remote Terminal Unit all'interno di pali di illuminazione contenenti concentratori dati, analizzatori di rete e router per le comunicazioni
- 775 x inteliLIGHT controllers, 242 dei quali inseriti all'interno di rifiniture progettati dall'azione produttrice dei corpi illuminanti
- 1 x inteliLIGHT streetlight control software

L'installazione ha portato a ridurre i costi di mantenimento di circa il 40%, ridurre i consumi energetici del 35%, migliorare la qualità dell'illuminazione (avendo a disposizione allarmi in tempo reale) e ha reso l'area più sicura.

Maggiori informazioni sono disponibili in [13]

3.1.4 Szada

Szada è unpiccolo centro abitato vicino la capitale ungherese. Per la sua posizione strategica è stata scelta per effettuare l'attività di testing del sistema InteliLIGHT alla fine del 2015. Anche in questo caso un operatore telefonico locale ha fornito la connettività mediante rete LoRaWAN. Nello specifico il l'installazione ha previsto:

- 4 x inteliLIGHT lighting controller, con limitate capacità di connesione
- 1 x Kerlink gateway / 868 MHz con capacità di comunicazione bidirezionale, con supporto per connessioni GPRS/EDGE/3G or Ethernet e LoRA, sviluppato su framework open source linux
- 1 x inteliLIGHT Streetlight Control Software

Il progetto pilota si è rilevato ben strutturato ed ha consentito l'attività di testing delle comunicazioni prevista.

Maggiori informazioni sono disponibili in [14]

3.2 *Le installazioni Billion*

Le installazioni Billion sono sviluppate soprattutto a Taipei, dove da qualche anno la municipalità sta finanziando un progetto per l'ammodernamento di tutto il sistema di illuminazione della città. Billion ha effettuato tre interventi lavorando con diversi operatori di mercato e raggiungendo obiettivi diversi in ogni installazione.

3.2.1 Taipei1

L'installazione nasce dall'esigenza di creare un supporto ad un'azienda produttrice di sistemi di illuminazione che aveva sviluppato un sistema di monitoraggio wireless basato su ZigBee. Purtroppo l'adozione di tali sistemi prevede un forte costo di installazione che può essere evitato considerando i sistemi PLC. A tal fine Billion ha effettuato un'istallazione presso Miaoli a Taipei. L'installazione copre circa 2.4 km ed ha previsto l'utilizzo di

- 50 x Intelligent Power Line Street Lighting Control Box sui supporti dei corpi illuminanti
- 1 x Broadband Powerline Smart Streetlight Segment Controller
- 1 x Smart Outdoor LCMS software.

Il sistema ha mostrato un risparmio energetico complessivo del 67%, dal software è possibile monitorare e controllare tutti i parametri di ogni singolo corpo illuminante.

Maggiori informazioni sono disponibili in [15]

3.2.2 Taipei 2

Billion ha collaborato con un'azienda del settore ICT per la realizzazione di 7km di Smart Street collocati in quattro siti differenti. Nel progetto erano previste l'installazione di 200 corpi illuminanti LED e del sistema di controllo. L'installazione ha previsto l'utilizzo di

- 50 x Intelligent Power Line Street Lighting Control Box sui supporti dei corpi illuminanti
- 4 x Broadband Powerline Smart Streetlight Segment Controller
- 1 x Smart Outdoor LCMS software.

L'obiettivo dell'installazione era il calcolo del risparmio energetico che si poteva ottenere tramite con la luce al LED, che andava opportunamente contabilizzato.

Maggiori informazioni sono disponibili in [16]

3.2.3 Taipei 3

Sempre all'interno dell'installazione di corpi illuminanti al led nella municipalità di Taipei la Billion ha effettuato un ulteriore intervento in collaborazione con un produttore locale di corpi illuminanti.
In particolare in questa installazione si è previsto l'utilizzo di telecamere collegate sulla rete per sorveglianza. In questo caso, circa 1km di strada si è cablata con

- 14 x Intelligent Power Line Street Lighting Control Box sui supporti dei corpi illuminanti
- 3 x Smart Lighting Wireless Bridges
- 1 x Broadband Powerline Smart Streetlight Segment Controller
- 1 x Smart Outdoor LCMS software.

In questo particolare set up le telecamere IP sono collegate direttamente agli Smart Lighting Wireless Bridges via Ethernet. Le immagini vengono poi trasferite al Broadband Powerline Smart Streetlight Segment Controller tramite collegamento wireless su VPN (Virtual Private Network).

Maggiori informazioni sono disponibili in [17]

3.3 Le installazioni Philips

Le installazioni eseguite da Philips riguardano grandi centri urbani. In particolare in questo report vengono proposti i casi di studio relativi alle città di Los Angeles e di Buenos Aires. In questi contesti Philips ha cooperato con gli operatori delle telecomunicazioni locali per ottenere la connettività desiderata.

3.3.1 Los Angeles

Il sistema di illuminazione intelligente di Los Angeles copre le 215.00 luci stradali che illuminano i 12.000 km di strade. Il suo rapido sviluppo è stato consentito mediante la realizzazione di un nodo di connessione CityTouch sviluppato per le Americhe. Esso si va ad inserire nella presa NEMA standard che si trova in cima ad un lampione. Mediante questo sistema di nodi di connessione, i corpi illuminanti tradizionali o LED di qualsiasi produttore possono essere inseriti nel sistema CityTouch. Una volta installato il nodo di connessione comincia a trasmettere wireless le informazioni operative, che sono accessibili in tempo reale tramite browser web.

Il maggior impatto nell'introduzione del sistema di illuminazione intelligente a Los Angeles si è avuto nella gestione dei guasti. Le interruzioni di servizio, infatti, vengono riportate automaticamente nel sistema di controllo. Questo permette di verificare anche le segnalazioni dei cittadini senza procedere necessariamente ad una costosa ispezione sul posto. Anche i tempi di risposta ai guasti di conseguenza sono stati ridotti da qualche giorno a poche ore.

Maggiori informazioni sono disponibili in [18]

3.3.2 Buenos Aires

L'installazione è cominciata nel 2013 ed è stata completata nel 2015 articolandosi in 3 fasi. Nella prima fase sono stati installati 11.000 corpi illuminanti LED sui viali e sulle strade principali. Nel periodo 2014-2015 sono stati installati complessivamente 91.000 nuovi punti luce nelle strade secondarie. Alla fine del 2015 il 75% dell'illuminazione della città era stata aggiornata.

Questo sforzo di aggiornamento ha consentito alla città di Buenos Aires di risparmiare il 50% dei costi operativi, riducendo anche le emissioni di CO2. A questo successo ha contribuito anche la sinergia con società di analisi dati che hanno fornito informazioni sulle criticità dell'impianto.

Maggiori informazioni sono disponibili in [19]

3.4 L'installazione Eliko a Tallin

Kalaranna è una strada di Tallinn lunga 2 km, completamente rinnovata nel 2015: tutti i lampioni sono stati sostituiti con lampade LED controllate dal sistema SmartELI.
Il sistema crea una rete mesh tra i lampioni della strada. Dal momento che la capacità della rete va ben oltre quella della gestione del sistema di controllo dell'illuminazione, ad essa sono stati collegati anche diversi sensori installati per monitorare il consumo energetico, il livello di rumore, la presenza di rifiuti negli appositi cestini.

Il sistema è stato installato per dimostrare l'interoperabilità di diverse tecnologie attraverso dispositivi intelligenti.

I dati collezionati dal sistema sono disponibili alla seguente pagina web http://www.eliko.ee/smartcity/. Essi hanno contribuito a migliorare i servizi della municipalità in termini di svuotamento dei cestini e analisi della riduzione dei costi, frequentazione della strada da parte dei pedoni e delle macchine, monitoraggio dell'inquinamento.

Maggiori informazioni sono disponibili in [20]

3.5 Il Sistema Smart Street in ENEA e la sicurezza

Figura 3.1Area interessata dal progetto Smart Street ENEA (Fonte UVAX [1])

Il progetto Smart Street di ENEA realizza un sistema di strada intelligente all'interno dello Smart Village nella sede di ENEA – Casaccia. Esso si compone di una strada illuminata e sensorizzata in maniera intelligente, come è possibile vedere in Figura 3.1.
Il sistema è costituito da una serie di venti lampione con armature LED Ampera Midi Schreder, equipaggiate con nodi di telecontrollo UVAX. L'obiettivo dell'installazione è il test di servizi a banda larga [21] (Videosorveglianza analisi video, Illuminazione adattiva, Servizio WiFi).

Il nodo concentratore è collegato tramite switch alla rete ENEA-Casaccia per la condivisione delle informazioni di diagnostica e di operatività del sistema.

La sicurezza di un sistema su rete dipende dalla progettazione della rete e dalla tipologia di servizi che in essa vengono introdotti.
Uno dei vantaggi più grandi del sistema adottato sta nel fatto che la rete è cablata. Le comunicazioni, infatti, utilizzano come mezzo la linea elettrica. Questa tecnologia, sebbene più soggetta ad attacchi fisici,

risulta intrinsecamente più resistente ad attacchi cyber: confrontata con una rete wireless, la rete cablata su powerline più complessa da penetrare.

A livello di integrità dei dati, un elemento di sicurezza è rappresentato dalla criptazione. Tutti i dati trasmessi sulla rete sono, infatti, criptati secondo il algoritmo di cifratura a blocchi DES/3DES (Data Encryption Algorithm/Triple Data Encryption Algorithm) per realizzare il totale isolamento tra reti e garantire la privacy degli utenti. Questa tecnica di criptazione risulta molto sicura: l'algoritmo 3DES non è attacabile a forza bruta in quanto utilizza 3 livelli annidati di criptazione (ossia l'algoritmo DES viene applicato 3 volte utilizzando 3 chiavi diverse) e risulta, allo stato dell'arte, una delle tecniche più affidabili.

A livello di confidenzialità dei dati, la rete PLC implementata nello Smart Street utilizza il sistema RADIUS (Remote Authentication Dial In User Service) [22] che fornisce servizi di autenticazione, autorizzazione e accounting centralizzato per computer che si connettono ed utilizzano connessioni di rete. Il protocollo RADIUS, pur avendo qualche criticità a livello di sicurezza, ma rappresenta lo standard de facto per l'autenticazione remota. Nel sistema in oggetto di analisi viene utilizzato dai nodi concentratori per controllare i nodi che si possono connettere in maniera sicura sulla rete.

Riguardo la disponibilità dei dati in rete, questa potrebbe essere compromessa dall'attacco a particolari nodi della rete o dall'attacco al nodo concentratore e alla workstation della sala controllo connesse tramite Internet.
Per quanto riguarda gli attacchi ai singoli nodi della rete PLC, la topologia ad albero della rete sembrerebbe mettere in evidenza una criticità nella robustezza: qualora un nodo *parent* venisse attaccato, tutto il suo sottoalbero perderebbe connettività. Esiste, tuttavia, una procedura per la definizione della rete che viene richiamata ogni volta che un nodo perde la connettività. La rete, quindi, risulta adattativa e non c'è alcun bisogno di intervento da parte di utenti o gestori della rete stessa.Il sistema CMS, sebbene utilizzi collegamenti sicuri, rappresenta una vulnerabilità del sistema in quanto soggetto ad attacchi tipo Denial of Service (DoS) che potrebbero degradare la qualità del servizio.

Il sistema, ben protetto dal punto di vista della confidenzialità e integrità dei dati, potrebbe essere soggetto a problemi di disponibilità del dato dovuti ai collegamenti di rete TCP/IP tra il concentratore e l'operatore che controlla il sistema. Nel prossimo paragrafo, pertanto, verranno proposti alcuni test che dovrebbero mettere in evidenza questa criticità.

4 Analisi delle prestazioni del sistema di telecontrollo

4.1 Test-bed per l'analisi delle prestazioni del sistema di telecontrollo e metodologia sperimentale

Al fine di valutare le prestazioni del sistema installato presso lo Smart Village nella sede di ENEA – Casaccia, si è sviluppato un apposito test-bed. Esso riproduce le condizioni della rete di comunicazione ENEA e presenta diversi vantaggi. In questo modo, è possibile valutare con maggiore accuratezza le prestazioni del sistema, senza compromettere il funzionamento del sistema reale.

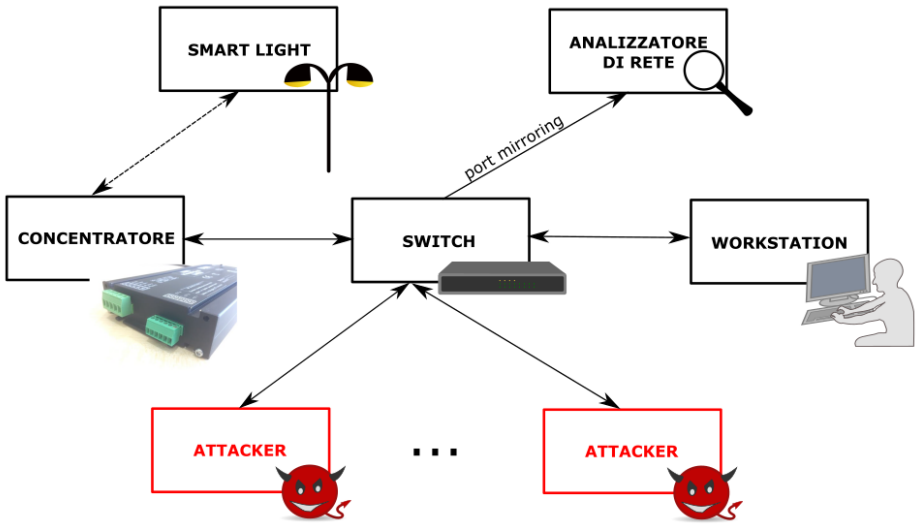

Figura 4.1Test-bed per lo studio del sistema di telecontrollo digitale dello Smart Street

Il test-bed riproduce la parte di rete che può essere soggetta ad attacchi con impatto sulla qualità del servizio ed è presentato in Figura 4.1Test-bed per lo studio del sistema di telecontrollo digitale dello Smart StreetIn particolare, esso è composto dai seguenti elementi:

- **Nodo concentratore:** simula la rete ad onde convogliate della Smart Street ed al suo interno contiene la WebApp che consente all'operatore remoto di avere informazioni sul corretto funzionamento della rete e di agire sui singoli nodi
- **Switch:** emula la rete
- **Workstation operatore:** emula la sala di controllo
- **Analizzatore di rete**: permette di valutare il degrado delle prestazioni ed è collegato sulla porta di mirroring dello switch
- **Nodi malevoli:** nodi che realizzano gli attacchi.

Le connessioni sono tutte Ethernet su cavo e passano attraverso lo switch. Quest'ultimo può essere configurato in modo da limitare la banda a disposizione delle sue porte, consentendo di limitare il numero di nodi malevoli che attaccano il target, degradando le prestazioni.

Gli strumenti software particolari utilizzati nel test-bed per la sperimentazione sono Kali-Linux e Wireshark. Kali Linux [23] è una distribuzione Linux, basata su Debian GNU/Linux, progettata per l'informatica forense e per effettuare penetration test, nell'ambito della sicurezza informatica. È una piattaforma supportata del Metasploit Framework del Metasploit Project, uno strumento per lo sviluppo e l'esecuzione di exploit di sicurezza.

Wireshark [24] è un analizzatore di pacchetti gratuito, e open source. Viene utilizzato per la risoluzione di problemi di rete, l'analisi, lo sviluppo dei protocolli software e di comunicazione, e a scopo didattico. Le funzionalità di Wireshark sono molto simili a quelle di tcpdump, ma con un'interfaccia grafica e maggiori funzionalità di ordinamento e filtraggio. Permette all'utente di osservare tutto il traffico presente sulla rete utilizzando la modalità promiscua dell'adattatore di rete. Tipicamente si riferisce alle reti Ethernet, ma è possibile analizzare altri tipi di rete fisica.

Per la sperimentazione si prevede di valutare la perdita d'efficienza per comunicazioni/operatività durante gli attacchi che sono inseriti nella Tabella 4.1.

Al fine di valutare il degrado delle prestazioni due tipologie di attacco mirano a interrompere o limitare l'operatività del sistema. A tal fine si utilizzeranno uno o più nodi malevoli, che attaccheranno i nodi target (concentratore e workstation) immettendo sulla rete pacchetti in flooding oppure eliminando alcuni pacchetti della connessione concentratore-workstation.

#	Metodologia attacco	Obiettivo attacco
1	*DoS flooding attack* con singolo nodo malevolo	Concentratore
2	*DoS flooding attack* con n nodi malevoli	Concentratore
3	*DoS flooding attack* con singolo nodo malevolo	Workstation
4	*DoS flooding attack* con n nodi malevoli	Workstation
5	*DoS flooding attack* con singolo nodo malevolo, porta switch limitata	Concentratore
6	*DoS flooding attack* con n nodi malevoli, porta switch limitata	Concentratore
7	*DoS flooding attack* con singolo nodo malevolo, porta switch limitata	Workstation
8	*DoS flooding attack* con n nodi malevoli, porta switch limitata	Workstation
9	*DoS* tramite *Random Packet Drop*	Concentratore
10	*DoS* tramite *Random Packet Drop*	Workstation
11	*DoS* tramite *Time Packet Drop*	Concentratore
12	*DoS* tramite *Time Packet Drop*	Workstation
13	*Sniffing attack*	Multipli

Tabella 4.1 Attacchi di test per la valutazione delle prestazioni del sistema di telecontrollo digitale della Smart Street

La topologia di rete utilizzata, schematizzata in Figura 4.1, prevede l'analisi delle comunicazioni attraverso un analizzatore di rete (*Wireshark*) collegato alla porta di *mirroring* settata sullo Switch. In questo modo tutto il traffico di rete viene replicato in uscita verso l'analizzatore di rete permettendo l'identificazione di problematiche in situazione di attacco informatico.

Si è scelto di analizzare il traffico di rete della topologia di test inserendo fino a due nodi malevoli.
Di seguito è analizzata la situazione di normalità per poi confrontarla con le situazioni malevoli descritte in Tabella 4.1.

Tutti i test effettuati hanno una durata approssimativa di un minuto.

4.2 Minaccia informatica alla disponibilità delle risorse

Un attacco informatico alla disponibilità delle risorse di un sistema mira a ridurre/annullare le possibilità di usufruire di un determinato servizio informatico da parte di un generico utente interessato.Questo tipo di minaccia, in inglese *Denial-of-Service (DoS)*, è un evento di sicurezza che si verifica quando un attore malevolo intraprende un'azione che impedisce agli utenti legittimi di accedere a sistemi informatici, dispositivi o altre risorse di rete.

Il modo più comune di effettuare attacchi alla disponibilità delle risorse di rete è attraverso tecniche di *flooding*. Questo attacco viene in genere effettuato contro server, sistemi o reti, congestionando il traffico di rete per sopraffare le risorse delle vittime e rendere difficile o impossibile l'utilizzo dei servizi da parte degli utenti legittimi. Mentre un attacco che blocca un server può essere spesso risolto riavviando il sistema, gli attacchi che saturano un canale di trasmissione possono essere più difficili da risolvere.

Gli strumenti classici di *detection* non sempre riescono a distinguere in maniera chiara quando un degrado delle comunicazioni di rete è dovuto ad un attacco informatico alla disponibilità delle risorse. In tal senso, il *Computer Emergency Response Team (CERT)* degli Stati Uniti d'America suggerisce alcune linee guida per identificarlo. Caratteristiche che potrebbero indicare un attacco alla disponibilità delle risorse sono le seguenti:

- Degradazione delle prestazioni di rete, specialmente quando si tenta di aprire file memorizzati in rete o accedere a siti web
- Incapacità di raggiungere un particolare sito web
- Difficoltà di accesso a qualsiasi sito web
- Un volume di e-mail spam superiore al normale.

Il profitto finanziario non è di solito il motivo alla base di questo tipo di attacco. In molti casi, gli aggressori vogliono arrecare danno all' organizzazione o alla persona oggetto dell'attacco; in altri casi, gli attaccanti stanno semplicemente tentando di sabotare la vittima, causando il maggior danno o disagio al maggior numero di utenti.

Molti attacchi alla disponibilità delle risorse di alto profilo sono in realtà attacchi distribuiti, il che significa che il traffico di attacco è diretto da più sistemi verso la vittima. Mentre gli attacchi provenienti da un'unica fonte possono essere più facili da mitigare perché i difensori possono bloccare il traffico di rete dalla fonte dell'infrazione, gli attacchi diretti da più sistemi di attacco sono molto più difficili da individuare. Anche le misure di difesa risultano più complesse in quanto può essere difficile differenziare il traffico legittimo da quello maligno e filtrare i pacchetti maligni quando vengono inviati da tutto Internet.

4.3 Attacco SYN Flooding

Per la fase di sperimentazione, si è scelto di utilizzare un attacco di tipo *SYN Flooding* al fine di testare la disponibilità delle risorse del test-bed.

Il *SYN Flooding* è un attacco di tipo *DoS* che abusa del processo di *three way handshake* del protocollo TCP, ovvero del processo mediante il quale un client stabilisce una connessione TCP con un server. Il *three way handshake* prevede i seguenti passaggi:

1. Il *client* richiede una connessione inviando un pacchetto SYN al server e così facendo richiede la sincronizzazione del *Sequence Number*, un segmento di 32-bit del TCP che serve per riconoscere il pacchetto inviato;

2. Il *server* risponde a tale richiesta inviando un pacchetto diSYN-ACK al client e inviando il *Sequence Number* ricevuto incrementato di una unità. Il server inoltre alloca dello spazio in memoria salvando la richiesta effettuata dal client;

3. Il *client* risponde con un *ACK* e il server dealloca la memoria utilizzata per salvare la richiesta effettuata dal client con il pacchetto di *SYN*. A questo punto la connessione si è instaurata correttamente.

In un attacco *SYN Flooding* l'attore malevolo invia un flusso di richieste SYN per aprire connessioni TCP con il server vittima, senza alcuna intenzione di completare effettivamente la connessione. Il costo di generazione del flusso di pacchetti SYN è relativamente basso, ma rispondere a tali richieste richiede risorse ingenti per le vittime. Il risultato che vuole raggiungere l'attaccante è quello di negare agli utenti legittimi l'accesso al server sotto attacco.

Molte volte il *SYN Flooding* viene utilizzato solo come fase iniziale di altri attacchi molto più sofisticati.
Per il nostro caso di studio, si è utilizzato l'applicativo hping3 su sistema operativo Kali Linux per effettuare i test di *SYN Flooding*.

Un esempio di utilizzo di questo software per questo tipo di attacco è il seguente:

$ sudo hping3 -i u1 -S -p 80 192.168.1.1

Questo codice invia pacchetti SYN ad un'ipotetica vittima localizzata all'indirizzo IP 192.168.1.1.
Analizzando il codice, possiamo osservare:

- **-i u1**: indica che il tempo di invio di ogni pacchetto malevolo avviene ogni microsecondo;
- **-S**: indica il flag di pacchetto SYN;
- **-p 80**: indica che la porta obiettivo dell'attacco è la 80.

Per tutti i test sviluppati si assume che gli attaccanti siano connessi alla LAN del test-bed.

	Attaccante 1	**Attaccante 2**
Processore	Intel Core i7-2670QM	Intel Core i3-2330M
Memoria RAM	6 GB	8 GB
Scheda di rete	Realtek PCIe GBE Family Controller #2	Realtek PCIe GBE Family Controller
Sistema operativo	Kali Linux	Kali Linux

Tabella 4.2: Specifiche nodi malevoli utilizzati.

4.4 *Test preliminare: Situazione di normalità*

Per la sperimentazione effettuata, si è scelto di eseguire una serie di test di attacco alla disponibilità delle risorse confrontandone i risultati con una situazione di normalità della rete.Per situazione di normalità si è inteso un minuto di analisi di traffico della rete del test-bed, utilizzando il traffico ricevuto dall'analizzatore di rete collegato alla porta di *mirroring*. Durante questo periodo non sono presenti azioni malevoli contro i nodi di rete connessi.

Nello specifico, il caso di test prende in considerazione l'analisi di traffico tra due nodi di rete legittimi, una workstation ed il concentratore PLC. La workstation, una volta collegatasi al *webserver* del concentratore in rete LAN, richiede in automatico l'aggiornamento della pagina riguardante la *energy performance (*Figura 4.2*)*. Non avendo a disposizione sensori/attuatori reali collegati al concentratore PLC, si è scelto di utilizzare questa pagina web per rendere ciclica la campagna di test di attacco informatico al fine di poterne confrontare i risultati.

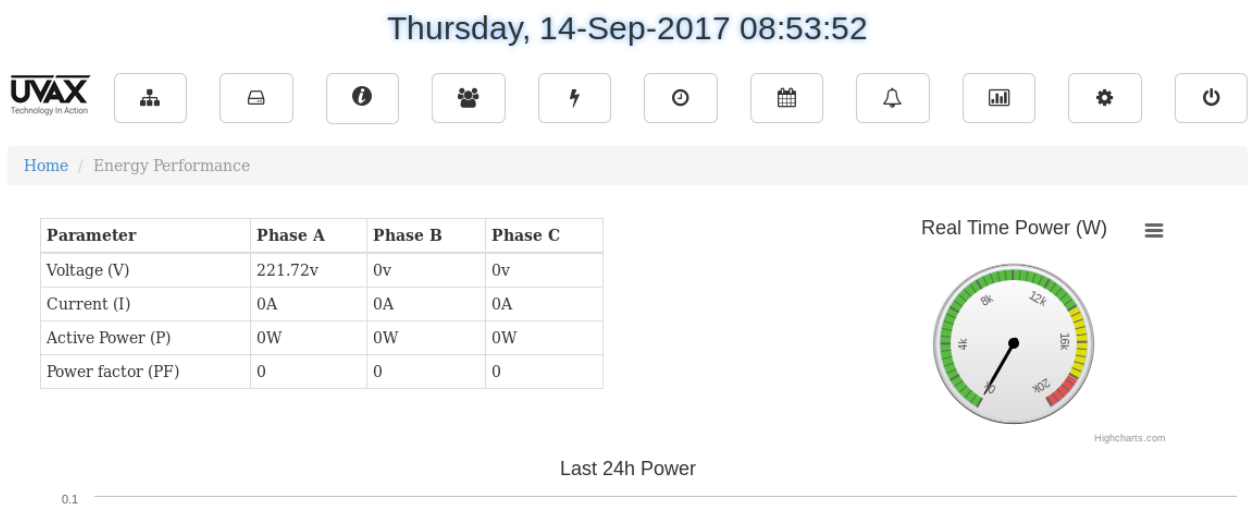

Figura 4.2 Pagina Energy Performance

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102

Tabella 4.3: Descrizione nodi di rete utilizzati

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
5	0.526146	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
11	0.756371	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
17	1.280339	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
21	1.493020	193.204.161.87	193.204.161.102	HTTP	1357	HTTP/1.1 200 OK (text/html)
41	2.014163	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
45	2.236043	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
51	2.755186	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
57	2.979138	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
61	3.497550	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
65	3.724116	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
69	4.243542	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
75	4.464513	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
89	4.992369	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1
95	5.225259	193.204.161.87	193.204.161.102	HTTP	1338	HTTP/1.1 200 OK (text/html)
101	5.753205	193.204.161.102	193.204.161.87	HTTP	731	GET /APP/web/index.php?r=energy/realtimecompsumtion HTTP/1.1

Figura 4.3: Traffico di rete HTTP tra workstation e concentratore in situazione di normalità

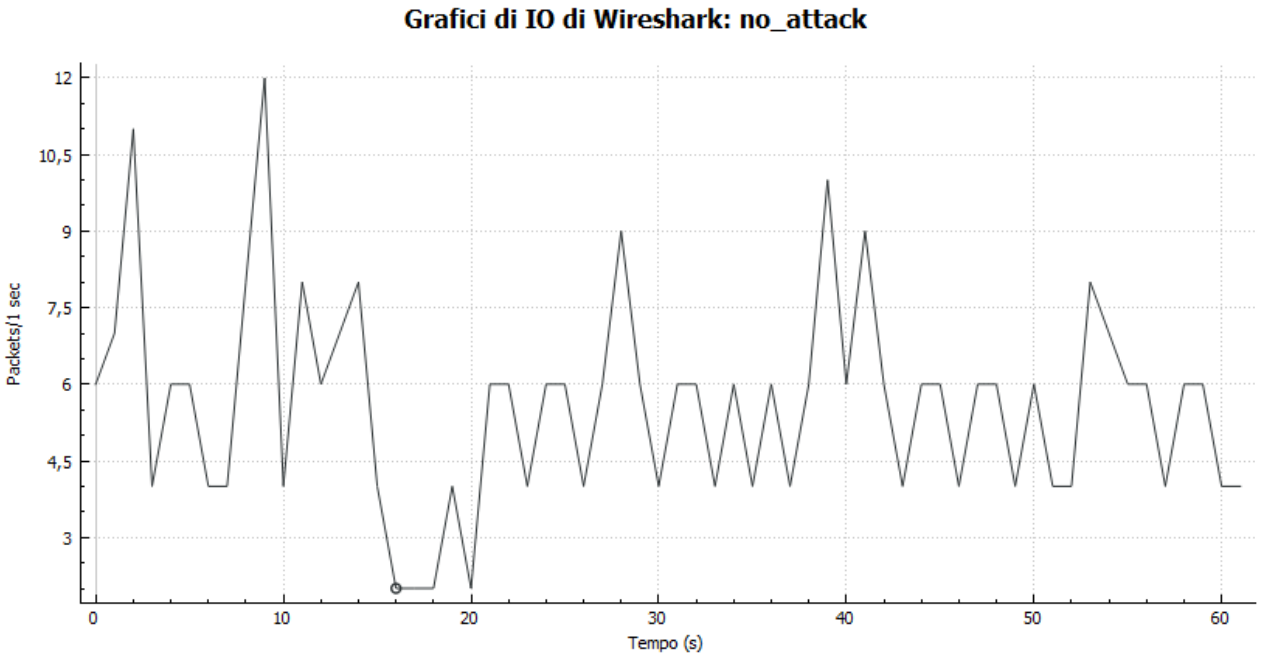

Figura 4.4: Analisi traffico TCP

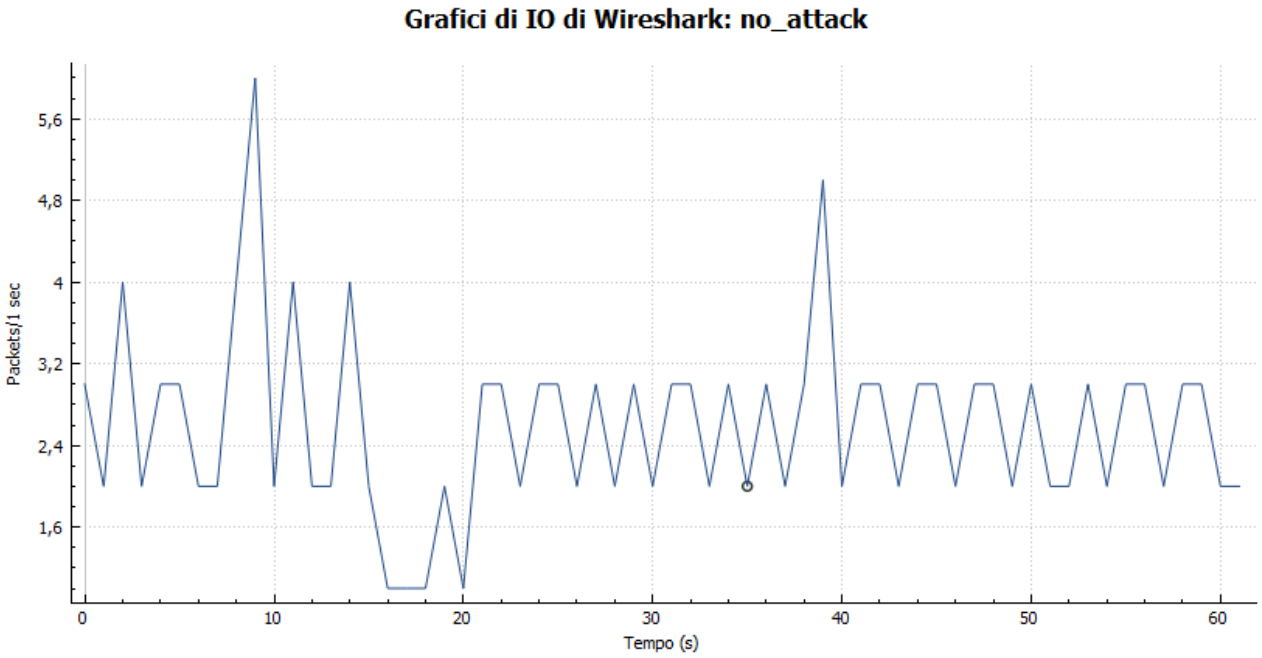

Figura 4.5: Analisi traffico http

Pkts TCP totali	Pkts http totali	Pkts TCP dest concentratore	Pkts TCP src concentratore	Pkts http dest concentratore	Pkt http src concentratore
348	161	176	172	80	81

Tabella 4.4: Analisi specifica traffico

4.5 SYN Flooding attack con singolo nodo malevolo

Descrizione: in questo test viene effettuato un attacco *SYN Flooding* utilizzando un singolo nodo malevolo. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dall'attaccante ogni microsecondo. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: concentratore.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.5Descrizione nodi di rete utilizzati

No.	Time	Source	Destination	Protocol	Length	Info
316	21.105638	193.204.161.113	193.204.161.87	TCP	60	1227 → 80 [SYN] Seq=0 Win=512 Len=0
321	21.106047	193.204.161.113	193.204.161.87	TCP	60	1228 → 80 [SYN] Seq=0 Win=512 Len=0
323	21.106050	193.204.161.113	193.204.161.87	TCP	60	1229 → 80 [SYN] Seq=0 Win=512 Len=0
325	21.106432	193.204.161.113	193.204.161.87	TCP	60	1230 → 80 [SYN] Seq=0 Win=512 Len=0
327	21.106836	193.204.161.113	193.204.161.87	TCP	60	1231 → 80 [SYN] Seq=0 Win=512 Len=0
329	21.106837	193.204.161.113	193.204.161.87	TCP	60	1232 → 80 [SYN] Seq=0 Win=512 Len=0
331	21.107231	193.204.161.113	193.204.161.87	TCP	60	1233 → 80 [SYN] Seq=0 Win=512 Len=0
333	21.107232	193.204.161.113	193.204.161.87	TCP	60	1234 → 80 [SYN] Seq=0 Win=512 Len=0
337	21.107657	193.204.161.87	193.204.161.113	TCP	60	80 → 1227 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
339	21.107658	193.204.161.87	193.204.161.113	TCP	60	80 → 1228 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
341	21.107659	193.204.161.87	193.204.161.113	TCP	60	80 → 1229 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
343	21.107660	193.204.161.87	193.204.161.113	TCP	60	80 → 1230 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
345	21.107661	193.204.161.87	193.204.161.113	TCP	60	80 → 1231 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
347	21.107662	193.204.161.87	193.204.161.113	TCP	60	80 → 1232 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
349	21.107663	193.204.161.87	193.204.161.113	TCP	60	80 → 1233 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
351	21.107664	193.204.161.87	193.204.161.113	TCP	60	80 → 1234 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460

Figura 4.6: Evidenza dell'attacco SYN Flooding avente come vittima il concentratore

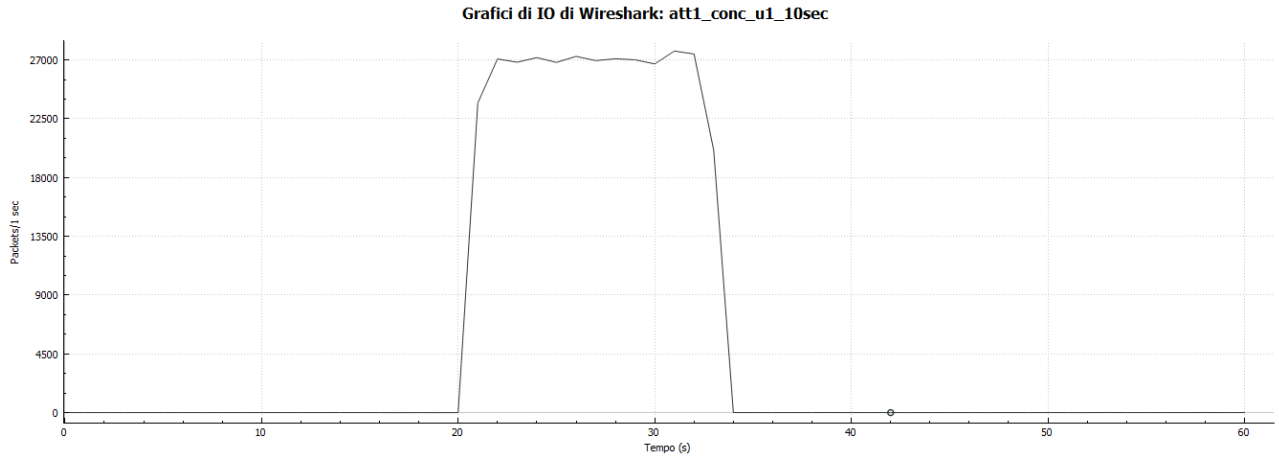

Figura 4.7: Analisi traffico TCP

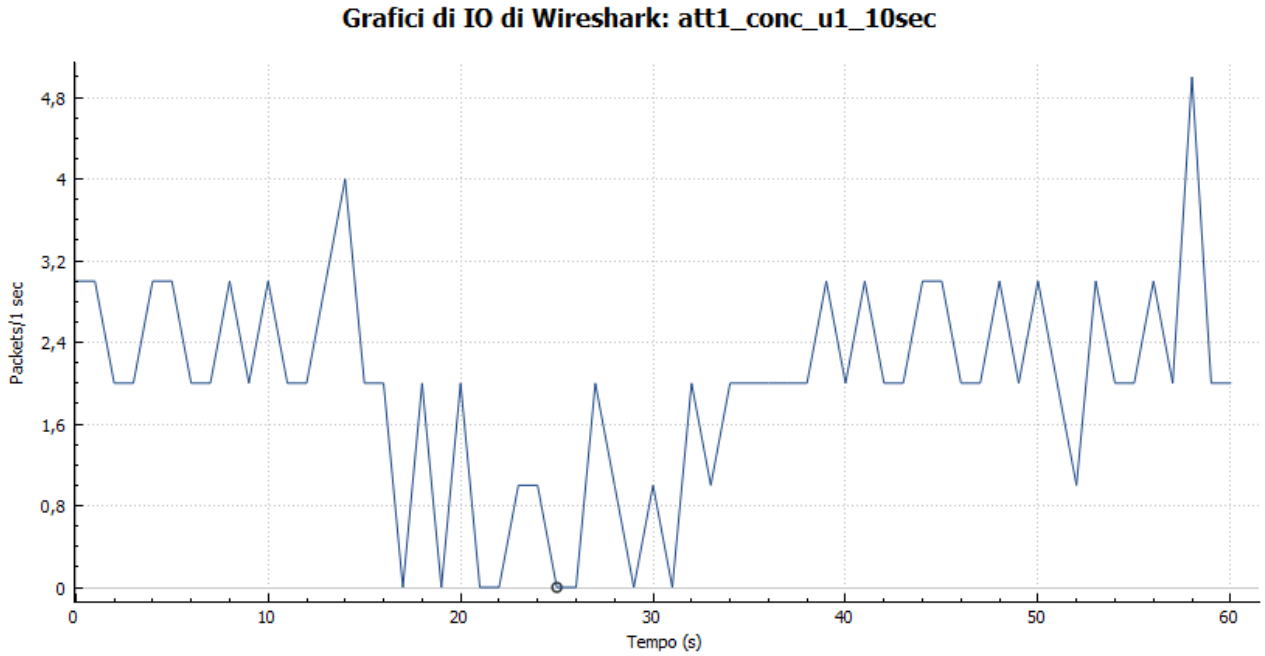

Figura 4.8: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest concentratore	Pkts TCP src concentratore	Pkts http dest concentratore	Pkt http src concentratore
342008	120	170980	171028	60	60

Tabella 4.6Analisi specifica traffico

4.6 SYN Flooding attack con due nodi malevoli

Descrizione: in questo test viene effettuato un attacco *SYN Flooding* utilizzando due nodi malevoli. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dagli attaccanti ogni microsecondo. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: concentratore.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113
Attaccante 2	193.204.161.101

Tabella 4.7Descrizione nodi di rete utilizzati

No.	Time	Source	Destination	Protocol	Length	Info
320…	21.909236	193.204.161.113	193.204.161.87	TCP	60	15421 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909237	193.204.161.113	193.204.161.87	TCP	60	15422 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909238	193.204.161.101	193.204.161.87	TCP	60	5984 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909239	193.204.161.101	193.204.161.87	TCP	60	5985 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909240	193.204.161.87	193.204.161.101	TCP	60	80 → 5686 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
320…	21.909240	193.204.161.113	193.204.161.87	TCP	60	15423 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909241	193.204.161.101	193.204.161.87	TCP	60	5986 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909241	193.204.161.113	193.204.161.87	TCP	60	15424 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909242	193.204.161.113	193.204.161.87	TCP	60	15425 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909243	193.204.161.101	193.204.161.87	TCP	60	5987 → 80 [SYN] Seq=0 Win=512 Len=0
320…	21.909244	193.204.161.101	193.204.161.87	TCP	60	5988 → 80 [SYN] Seq=0 Win=512 Len=0
321…	21.909434	193.204.161.87	193.204.161.113	TCP	60	80 → 14820 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460
321…	21.909435	193.204.161.113	193.204.161.87	TCP	60	15426 → 80 [SYN] Seq=0 Win=512 Len=0
321…	21.909435	193.204.161.113	193.204.161.87	TCP	60	15427 → 80 [SYN] Seq=0 Win=512 Len=0
321…	21.909436	193.204.161.101	193.204.161.87	TCP	60	5989 → 80 [SYN] Seq=0 Win=512 Len=0
321…	21.909437	193.204.161.87	193.204.161.113	TCP	60	80 → 14821 [SYN, ACK] Seq=0 Ack=1 Win=14600 Len=0 MSS=1460

Figura 4.9: Evidenza dell'attacco SYN Flooding avente come vittima il concentratore

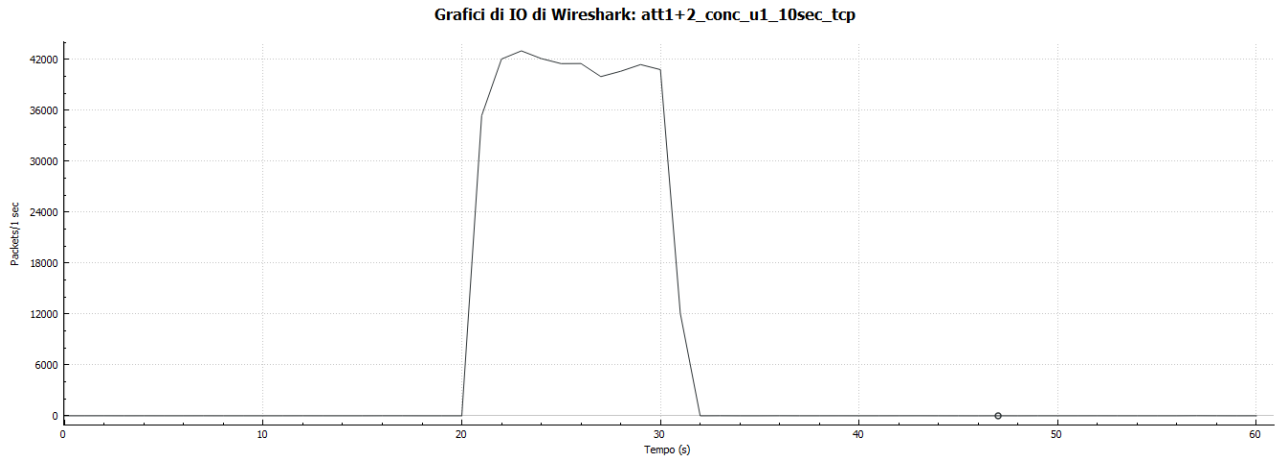

Figura 4.10: Analisi traffico TCP

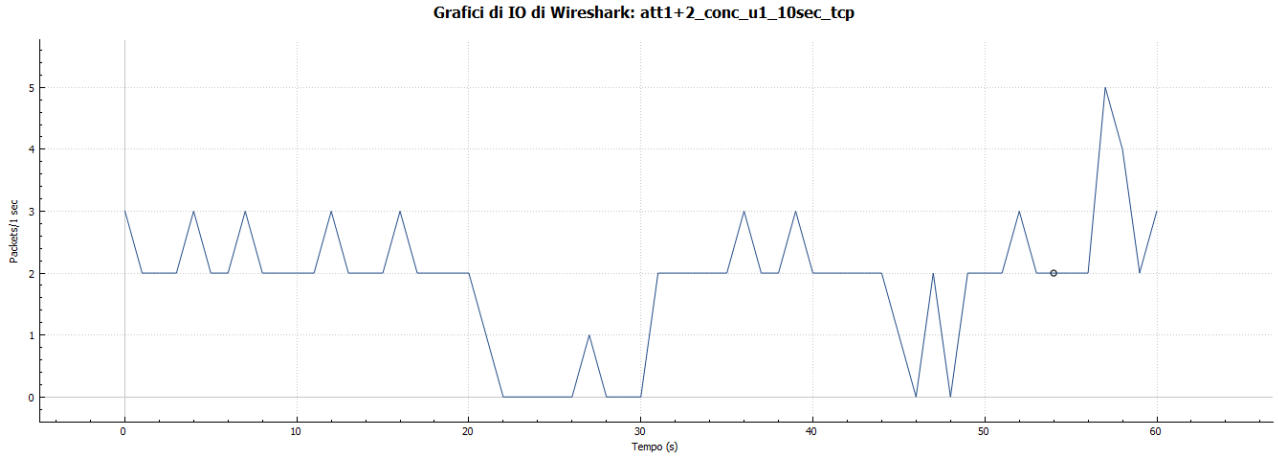

Figura 4.11: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest concentratore	Pkts TCP src concentratore	Pkts http dest concentratore	Pkt http src concentratore
420539	113	246205	174334	56	57

Tabella 4.8 Analisi specifica traffico

4.7 SYN Flooding attack con singolo nodo malevolo

Descrizione: in questo test viene effettuato un attacco *SYN Flooding* utilizzando un singolo nodo malevolo. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dall'attaccante ogni microsecondo. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.9Descrizione nodi di rete utilizzati

No.	Time	Source	Destination	Protocol	Length	Info
503	21.165233	193.204.161.113	193.204.161.102	TCP	60	3248 → 80 [SYN] Seq=0 Win=512 Len=0
504	21.165234	193.204.161.113	193.204.161.102	TCP	60	3249 → 80 [SYN] Seq=0 Win=512 Len=0
505	21.165235	193.204.161.113	193.204.161.102	TCP	60	3250 → 80 [SYN] Seq=0 Win=512 Len=0
506	21.165444	193.204.161.113	193.204.161.102	TCP	60	3251 → 80 [SYN] Seq=0 Win=512 Len=0
507	21.165446	193.204.161.113	193.204.161.102	TCP	60	3252 → 80 [SYN] Seq=0 Win=512 Len=0
508	21.165449	193.204.161.113	193.204.161.102	TCP	60	3253 → 80 [SYN] Seq=0 Win=512 Len=0
509	21.165450	193.204.161.113	193.204.161.102	TCP	60	3254 → 80 [SYN] Seq=0 Win=512 Len=0
510	21.165640	193.204.161.113	193.204.161.102	TCP	60	3255 → 80 [SYN] Seq=0 Win=512 Len=0
511	21.165641	193.204.161.113	193.204.161.102	TCP	60	3256 → 80 [SYN] Seq=0 Win=512 Len=0
512	21.165645	193.204.161.113	193.204.161.102	TCP	60	3257 → 80 [SYN] Seq=0 Win=512 Len=0
513	21.165843	193.204.161.113	193.204.161.102	TCP	60	3258 → 80 [SYN] Seq=0 Win=512 Len=0
514	21.165847	193.204.161.113	193.204.161.102	TCP	60	3259 → 80 [SYN] Seq=0 Win=512 Len=0
515	21.165849	193.204.161.113	193.204.161.102	TCP	60	3260 → 80 [SYN] Seq=0 Win=512 Len=0
516	21.166431	193.204.161.113	193.204.161.102	TCP	60	3261 → 80 [SYN] Seq=0 Win=512 Len=0
517	21.166432	193.204.161.113	193.204.161.102	TCP	60	3262 → 80 [SYN] Seq=0 Win=512 Len=0
518	21.166433	193.204.161.113	193.204.161.102	TCP	60	3263 → 80 [SYN] Seq=0 Win=512 Len=0

Figura 4.12: Evidenza dell'attacco SYN Flooding avente come vittima la workstation

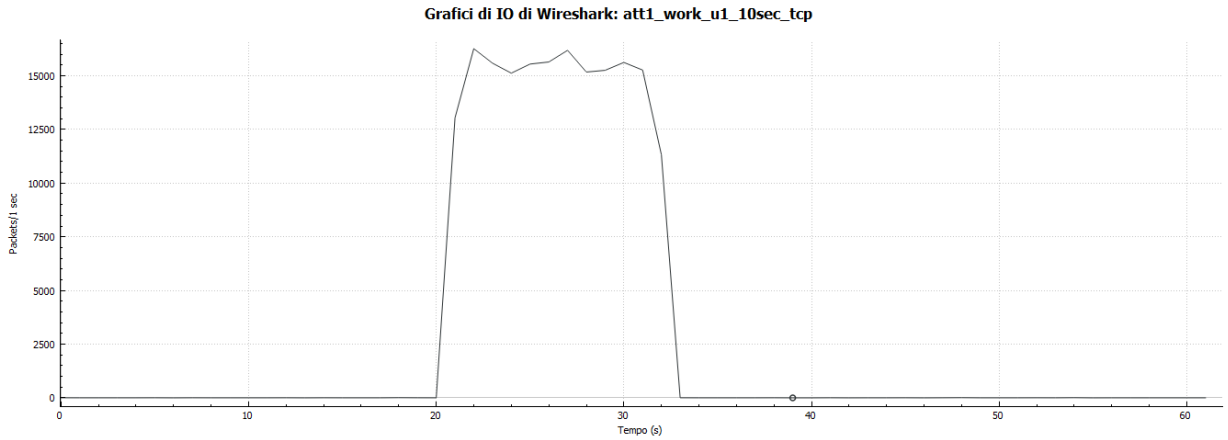

Figura 4.13: Analisi traffico TCP

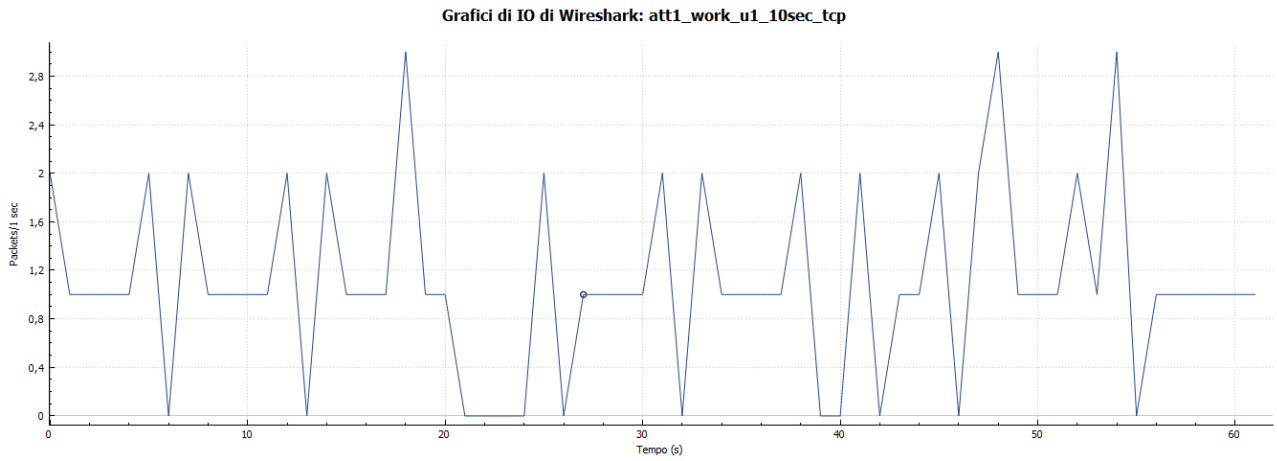

Figura 4.14: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest workstation	Pkts TCP src workstation	Pkts http dest workstation	Pkt http src workstation
180090	68	180016	74	34	34

Tabella 4.10Analisi specifica traffico

4.8 SYN Flooding attack con due nodi malevoli

Descrizione: in questo test viene effettuato un attacco SYN Flooding utilizzando due nodi malevoli. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dagli attaccanti ogni microsecondo. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113
Attaccante 2	193.204.161.101

Tabella 4.11Descrizione nodi di rete utilizzati

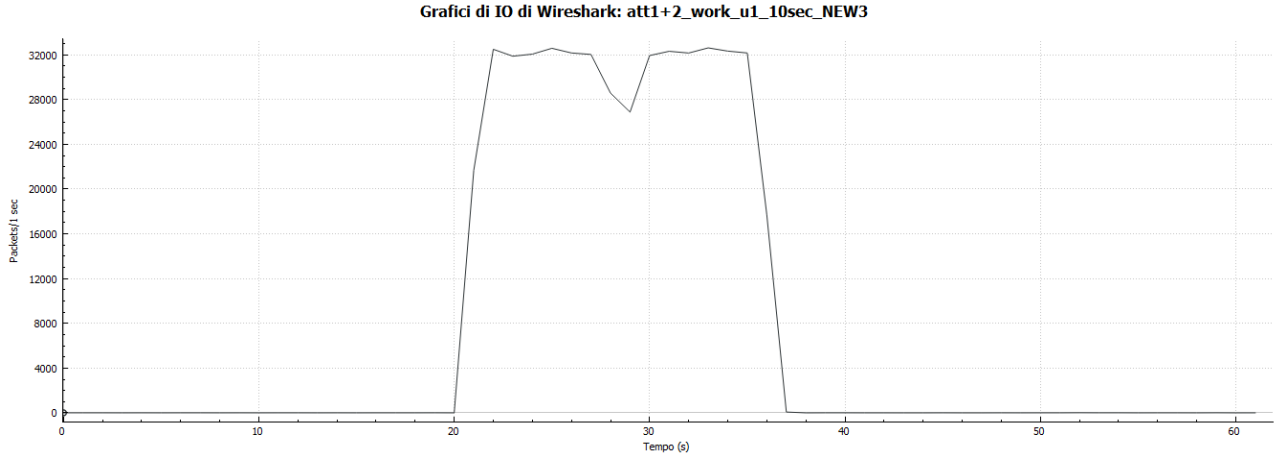

Figura 4.15: Analisi traffico TCP

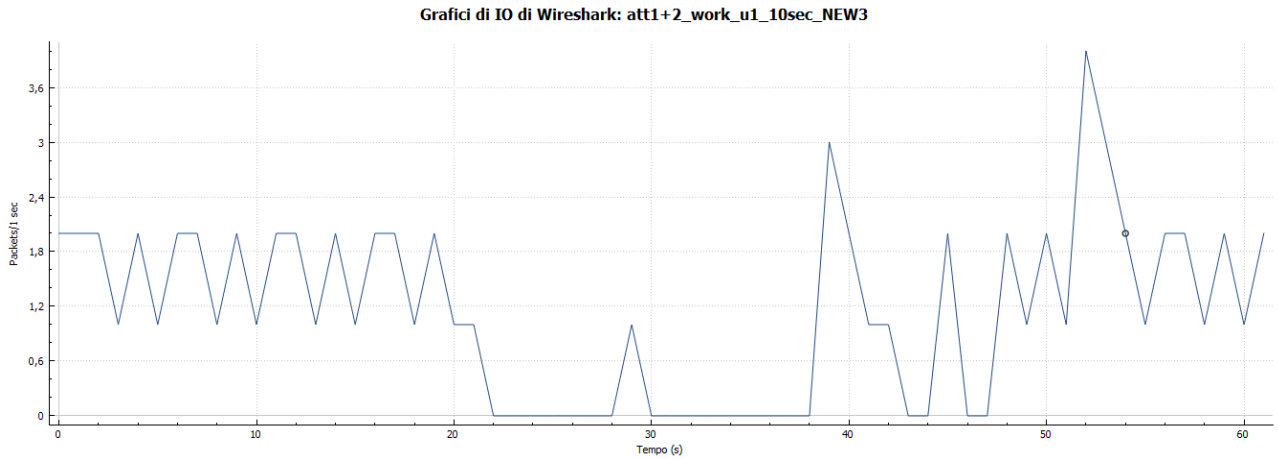

Figura 4.16: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest workstation	Pkts TCP src workstation	Pkts http dest workstation	Pkt http src workstation
481711	71	481622	89	35	36

Tabella 4.12Analisi specifica traffico

4.9 SYN Flooding attack con singolo nodo malevolo, porta switch limitata

Descrizione: in questo test viene effettuato un attacco SYN Flooding utilizzando un singolo nodo malevolo. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dall'attaccante ogni microsecondo. La porta Ethernet utilizzata dalla vittima viene limitata a 10 Mbit/s. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: concentratore.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.13Descrizione nodi di rete utilizzati

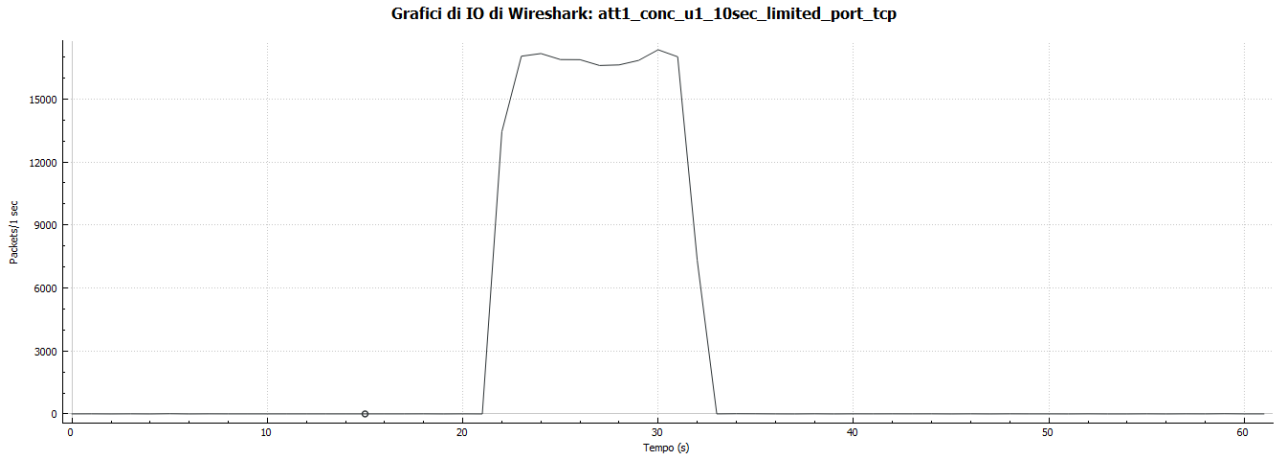

Figura 4.17: Analisi traffico TCP

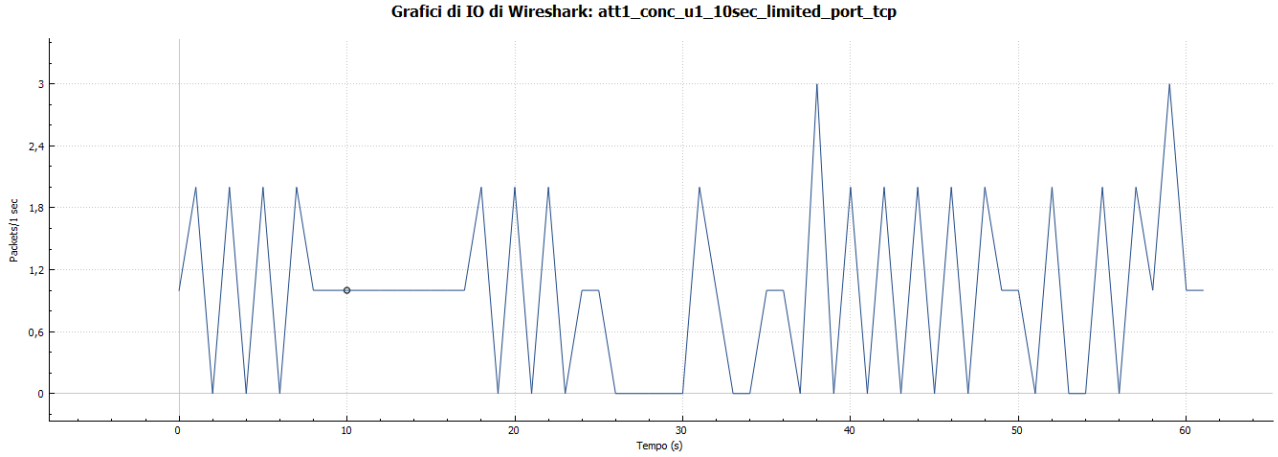

Figura 4.18: Analisi traffico HTTP

Pkts TCP	Pkts http	Pkts TCP dest	Pkts TCP src	Pkts http dest	Pkt http src

totali	totali	concentratore	concentratore	concentratore	concentratore
173205	59	126568	46637	30	29

Tabella 4.14Analisi specifica traffico

4.10 SYN Flooding attack con due nodi malevoli, porta switch limitata

Descrizione: in questo test viene effettuato un attacco SYN Flooding utilizzando due nodi malevoli. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dagli attaccanti ogni microsecondo. La porta Ethernet utilizzata dalla vittima viene limitata a 10 Mbit/s. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: concentratore.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113
Attaccante 2	193.204.161.101

Tabella 4.15Descrizione nodi di rete utilizzati

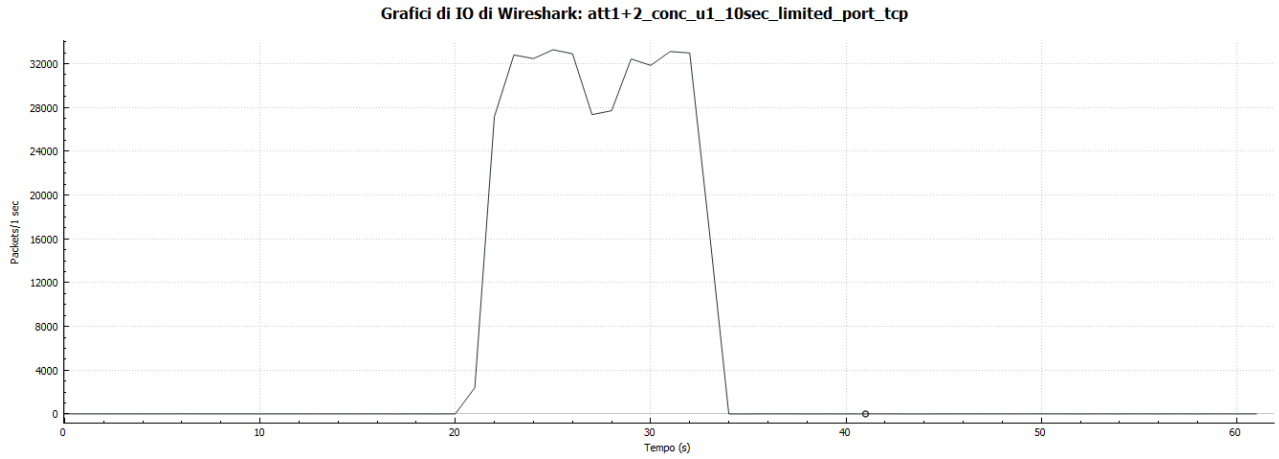

Figura 4.19: Analisi traffico TCP

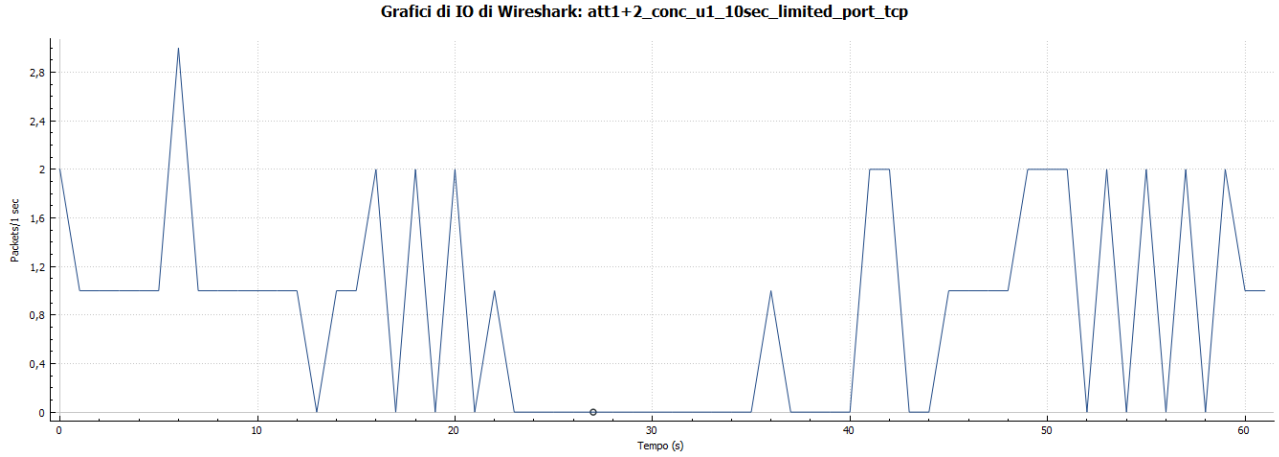

Figura 4.20: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest concentratore	Pkts TCP src concentratore	Pkts http dest concentratore	Pkt http src concentratore
363197	50	306598	56599	25	25

Tabella 4.16Analisi specifica traffico

4.11 SYN Flooding attack con singolo nodo malevolo, porta switch limitata

Descrizione: in questo test viene effettuato un attacco SYN Flooding utilizzando un singolo nodo malevolo. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dall'attaccante ogni microsecondo. La porta Ethernet utilizzata dalla vittima viene limitata a 10Mbit/s. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.17Descrizione nodi di rete utilizzati

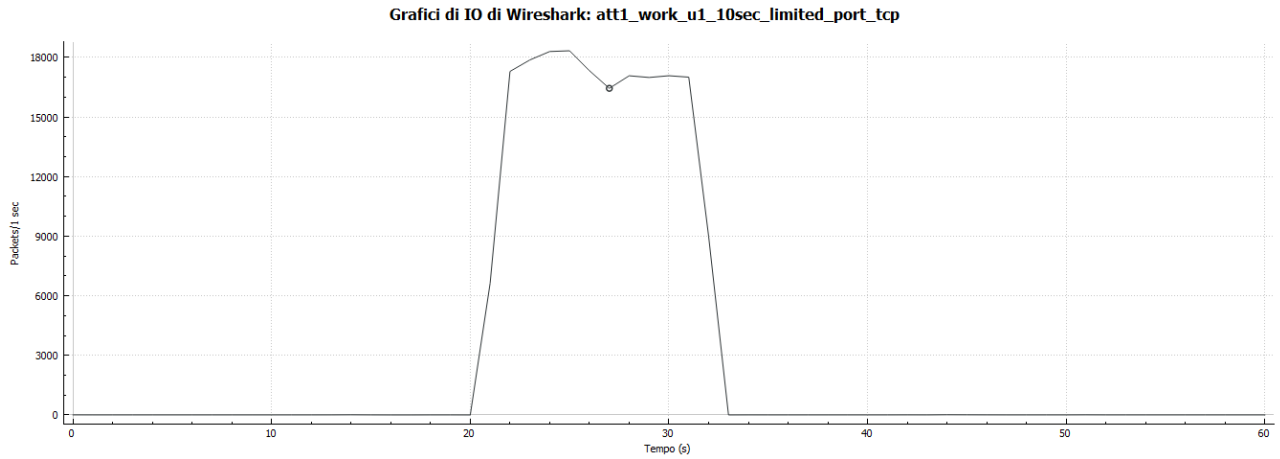

Figura 4.21: Analisi traffico TCP

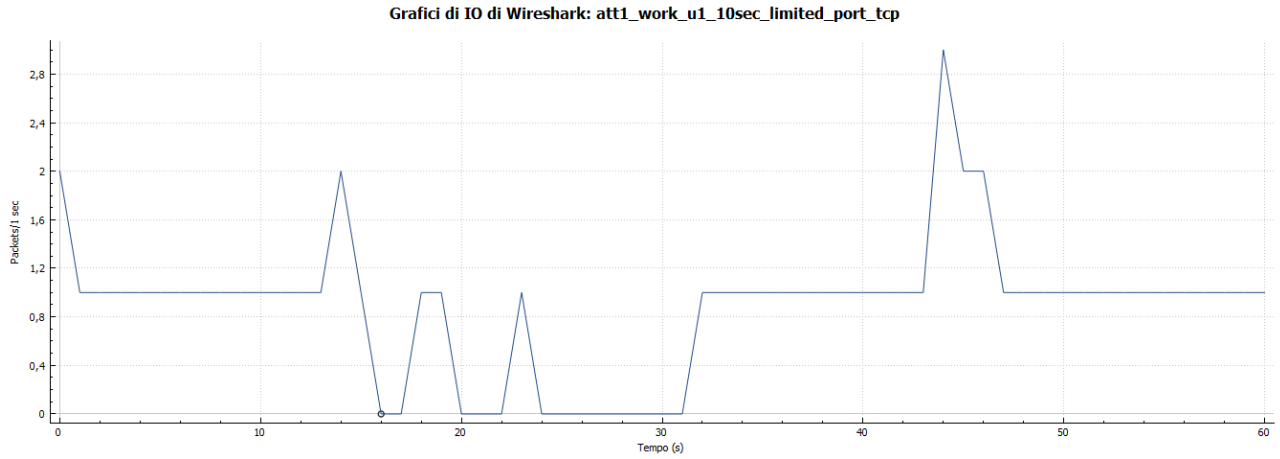

Figura 4.22: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest workstation	Pkts TCP src workstation	Pkts http dest workstation	Pkt http src workstation
189437	54	189358	79	27	27

Tabella 4.18Analisi specifica traffico

4.12 SYN Flooding attack con due nodi malevoli, porta switch limitata

Descrizione: in questo test viene effettuato un attacco *SYN Flooding* utilizzando due nodi malevoli. L'attacco viene inizializzato a circa 20 secondi dall'inizio dell'analisi di rete e ha una durata di circa 10 secondi. I pacchetti SYN vengono inviati dagli attaccanti ogni microsecondo. La porta Ethernet utilizzata dalla vittima viene limitata a 10 Mbit/s. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113
Attaccante 2	193.204.161.101

Tabella 4.19Descrizione nodi di rete utilizzati

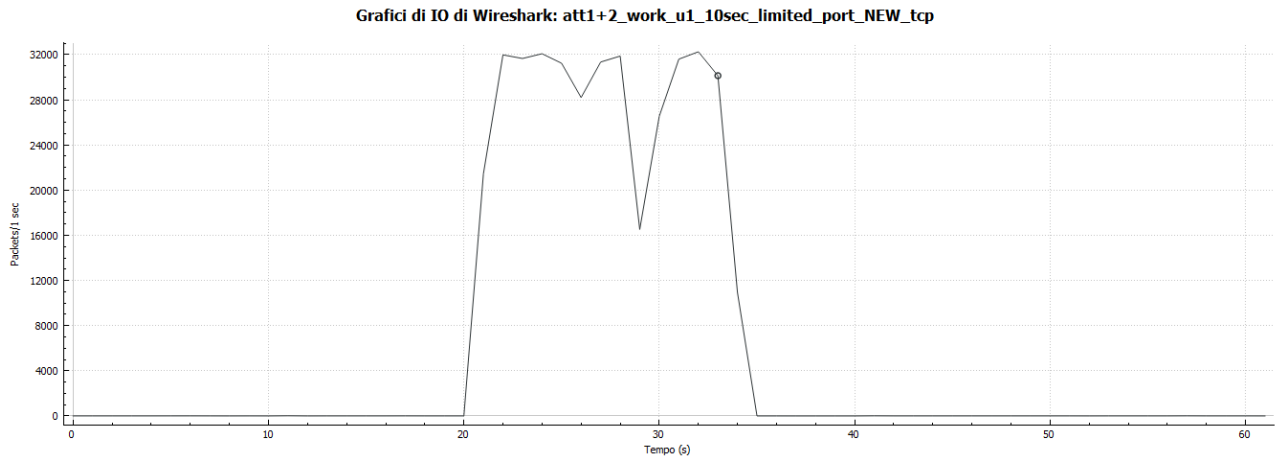

Figura 4.23: Analisi traffico TCP.

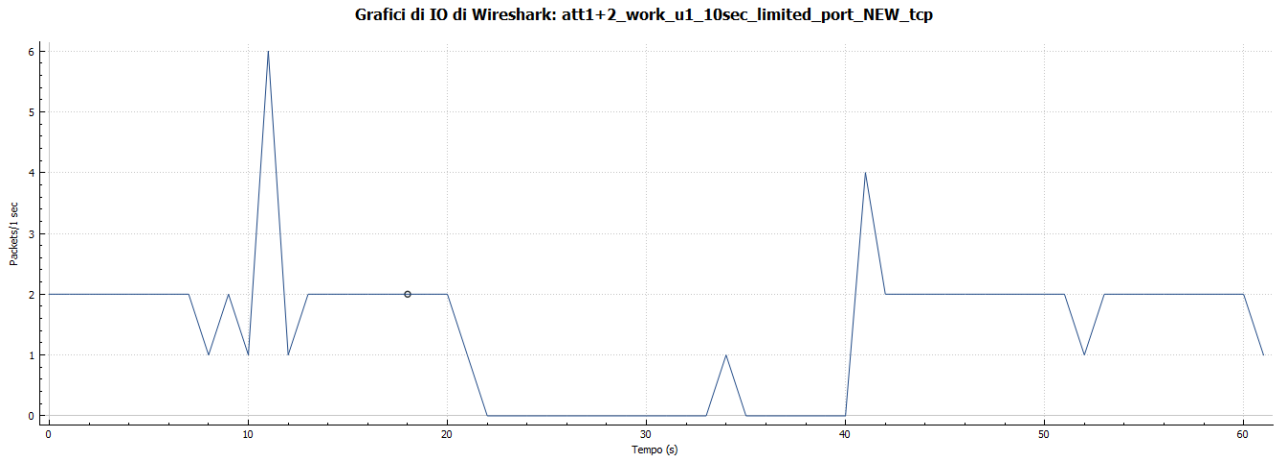

Figura 4.24: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest workstation	Pkts TCP src workstation	Pkts http dest workstation	Pkt http src workstation
387952	87	387846	106	43	44

Tabella 4.20Analisi specifica traffico

4.13 Denial of Service tramite Random Packet Drop

Descrizione:in questo test il nodo malevolo effettua un attacco di tipo *Man In The Middle (MITM)* utilizzando la tecnica *ARP Poisoning*. Successivamente, l'attaccante effettua un *Random Packet Drop*, ovvero una eliminazione random di pacchetti che transitano attraverso di lui sulla rete provocando una degradazione delle comunicazioni di rete tra le due vittime. In questo caso i pacchetti eliminati hanno come destinazione il concentratore. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittime: concentratore.

Identificativo	**Indirizzo IP**
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.21Descrizione nodi di rete utilizzati

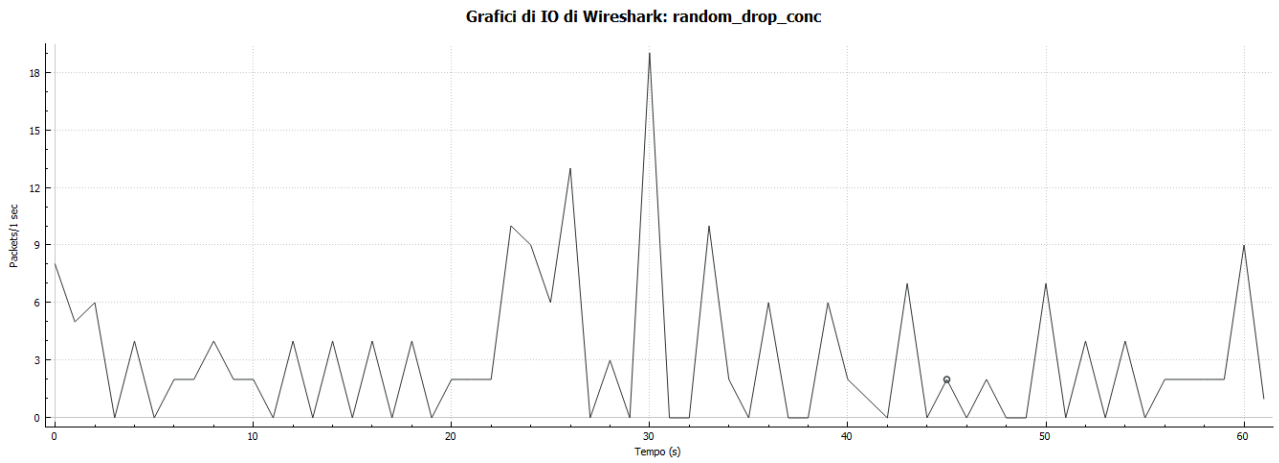

Figura 4.25: Analisi traffico TCP

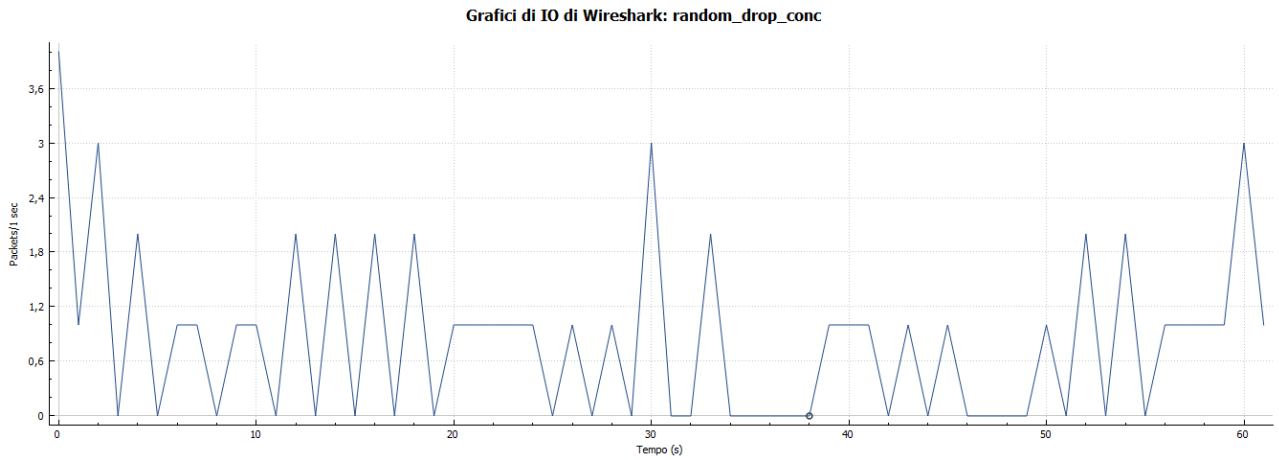

Figura 4.26: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest concentratore	Pkts TCP src concentratore	Pkts http dest concentratore	Pkt http src concentratore
188	52	110	96	26	26

Tabella 4.22Tabella 21: Analisi specifica traffico

4.14 Denial of Service tramite Random Packet Drop

Descrizione:in questo test il nodo malevolo effettua un attacco di tipo *Man In The Middle (MITM)* utilizzando la tecnica *ARP Poisoning*. Successivamente, l'attaccante effettua un *Random Packet Drop*, ovvero una eliminazione random di pacchetti che transitano attraverso di lui sulla rete provocando una degradazione delle comunicazioni di rete tra le due vittime. In questo caso i pacchetti eliminati hanno come destinazione la workstation. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87

Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.23Descrizione nodi di rete utilizzati

Figura 4.27: Analisi traffico TCP

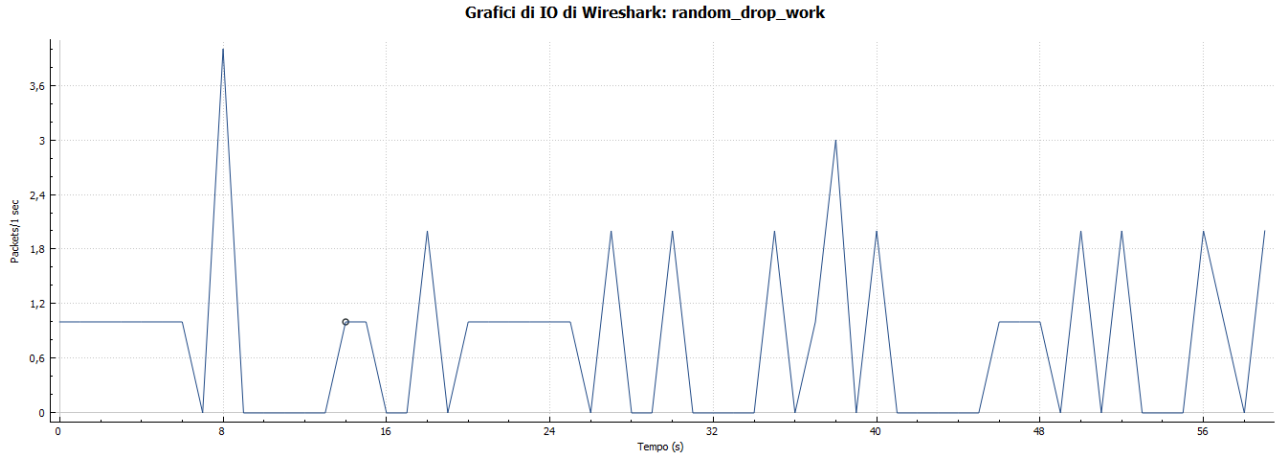

Figura 4.28: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest workstation	Pkts TCP src workstation	Pkts http dest workstation	Pkt http src workstation
221	65	113	126	41	24

Tabella 4.24Analisi specifica traffico

4.15 Denial of Service tramite Packet Time Delay

Descrizione: in questo test il nodo malevolo effettua un attacco di tipo *Man In The Middle (MITM)* utilizzando la tecnica *ARP Poisoning*. Successivamente, l'attaccante inserisce ritardi trasmissivi ai pacchetti che transitano attraverso di lui sulla rete provocando una degradazione delle comunicazioni tra nodi legittimi. In questo caso i pacchetti ritardati hanno come destinazione il concentratore. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.

Vittima: concentratore.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.25Descrizione nodi di rete utilizzati

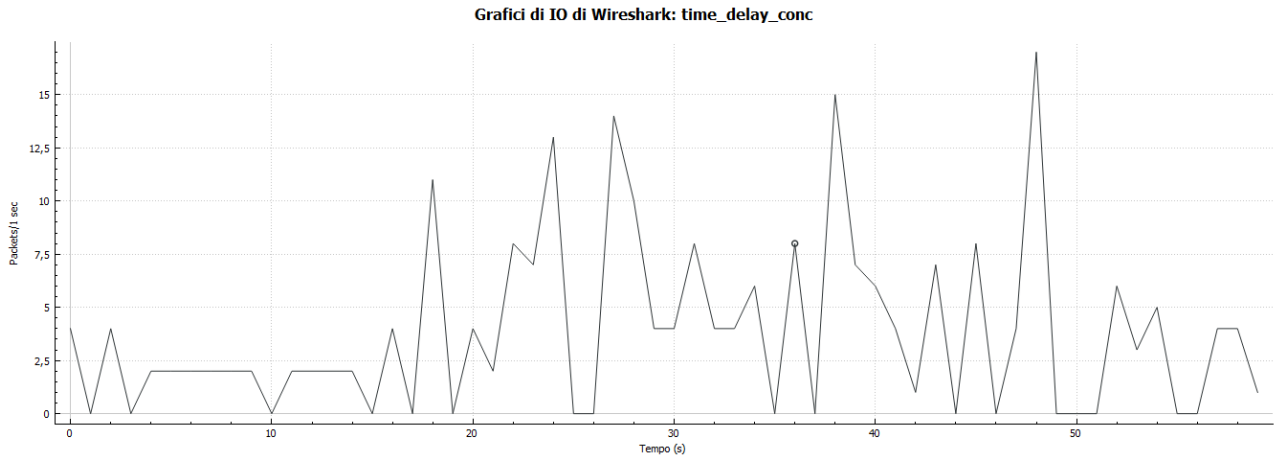

Figura 4.29: Analisi traffico TCP

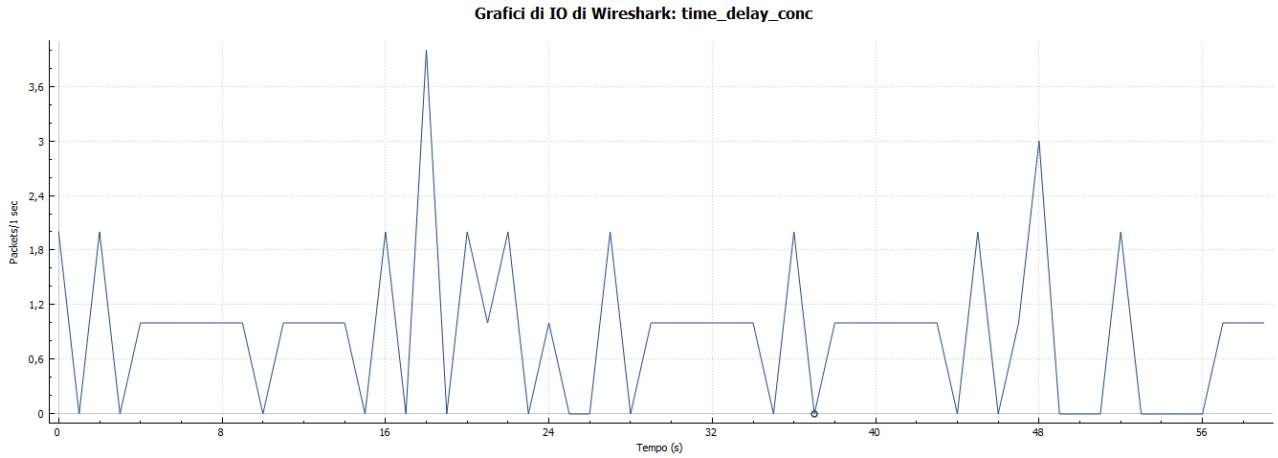

Figura 4.30: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest concentratore	Pkts TCP src concentratore	Pkts http dest concentratore	Pkt http src concentratore
249	53	142	107	26	27

Tabella 4.26Analisi specifica traffico

4.16 Denial of Service tramite Packet Time Delay

Descrizione: in questo test il nodo malevolo effettua un attacco di tipo *Man In The Middle (MITM)* utilizzando la tecnica *ARP Poisoning*. Successivamente, l'attaccante inserisce ritardi trasmissivi ai pacchetti che transitano attraverso di lui sulla rete provocando una degradazione delle comunicazioni tra nodi

legittimi. In questo caso i pacchetti ritardati hanno come destinazione la workstation. L'analisi dei risultati viene effettuata dall'analizzatore di rete collegato in *mirroring*.
Vittima: workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.27Descrizione nodi di rete utilizzati

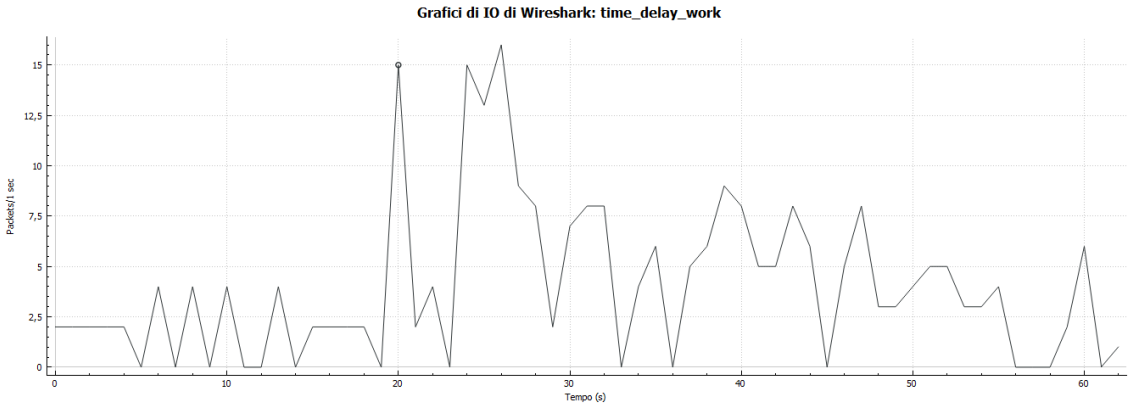

Figura 4.31: Analisi traffico TCP

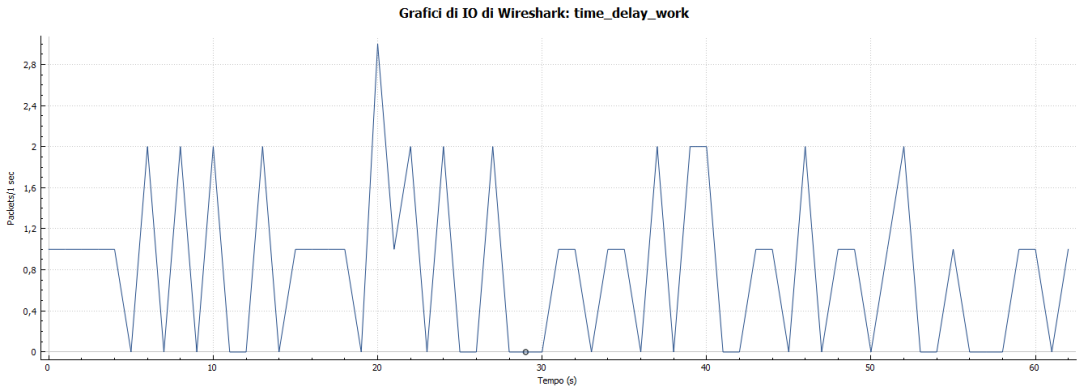

Figura 4.32: Analisi traffico HTTP

Pkts TCP totali	Pkts http totali	Pkts TCP dest workstation	Pkts TCP src workstation	Pkts http dest workstation	Pkt http src workstation
273	50	135	138	25	25

Tabella 4.28Analisi specifica traffico

4.17 Sniffing attack

Descrizione: in questo test il nodo malevolo effettua un attacco di tipo *Man In The Middle (MITM)* utilizzando la tecnica *ARP Poisoning*. Successivamente, l'attaccante analizza in maniera malevola e passiva il traffico di rete al fine di consolidare la propria conoscenza delle vittime e poter perfezionare futuri attacchi più complessi.
Vittime: concentratore e workstation.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102
Attaccante 1	193.204.161.113

Tabella 4.29Descrizione nodi di rete utilizzati

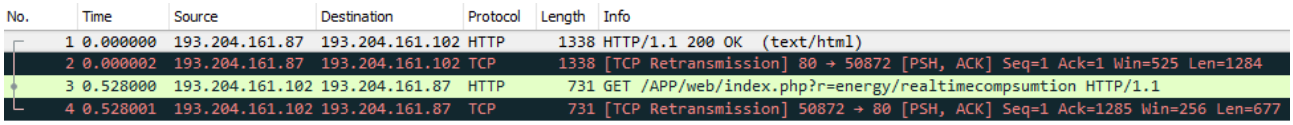

Figura 4.33: Evidenza del traffico che passa attraverso l'attaccante.

4.18 Analisi dei risultati e conclusioni

Come si può evincere dall'analisi dei risultati, effettuando gli attacchi *SYN Flooding* si è constatato un decadimento delle prestazioni di rete ed una conseguente indisponibilità delle risorse.

Nei vari casi, l'attacco ha portato ad un rallentamento delle comunicazioni e nei casi più gravi alla impossibilità di aggiornamento dei dati di *Energy Management*.È possibile affermare che quanto più traffico legittimo è presente sulla rete, tanto più sarà facile per un attore malevolo effettuare con successo un attacco informatico alla disponibilità delle risorse.

In Figura 4.34è possibile visualizzare il messaggio di errore che viene inviato dal webserver del concentratore quando si verifica indisponibilità della risorsa dovuta ad un attacco *SYN Flooding*.Si evidenzia anche la capacità dei nodi di rete legittimi, compreso il concentratore, di ristabilire una situazione di comunicazione normale quando l'attacco si interrompe.

In lavori futuri verranno analizzati i risultati di attacchi informatici alla disponibilità delle risorse utilizzando un test-bed più complesso, inserendo sensori/attuatori PLC che permettano un completo funzionamento dell'impianto sperimentale.

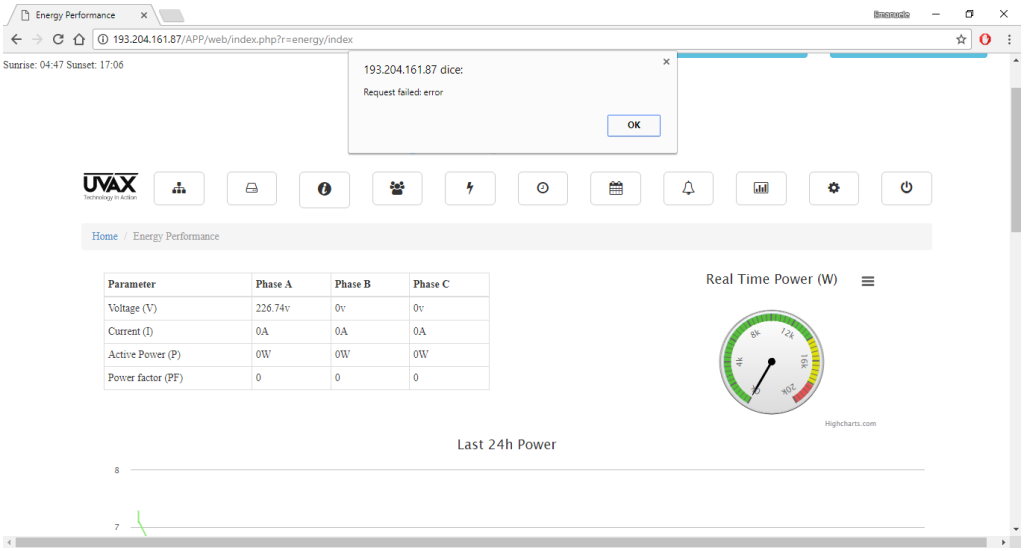

Figura 4.34 Request failed error

5 Riferimenti bibliografici

1. Blasco, C.J.V., Riveiro, I.J.C., Fouren, N.H., Jimenez, M.F.J., Gomez, M.F., Torres, C.L.M., Garcia, S.J.A., Blasco, A.F.J., Pardo, V.C., Badenes, C.A., Communication optimisation method for a multi-user OFDM digital transmission system using the electrical network, CA242453 A1, https://worldwide.espacenet.com/publicationDetails/biblioCC=CA&NR=242453A1&KC=A1&FT=D(29 settembre 2017)
2. Beghelli – Catalogo Reverso Illuminazione 2017https://www.beghelli.it/it/media/download/documents/08a21c3a-564e-4e22-9171-1d53eb4fdc42(29 settembre 2017)
3. Luminibus –Scheda tecnica concentratore M3C-CB200 http://www.apsystems.it/media/2544/m3c-cb200-pds-sh2016v3-it.pdf(29 settembre 2017)
4. Luminibus Scheda tecnica Smar City software M3C-SCS http://www.apsystems.it/media/2547/m3sms-printable-data-sheet-fh2016v2-it.pdf(29 settembre 2017)
5. Telensa – PLANet Systemhttps://www.telensa.com/smart-lighting/(29 settembre 2017)
6. InteliLIGHT – LonWorks Systems https://intelilight.eu/technology/intelilight-lonworks-plc-compatible-street-lighting-remote-management/(29 settembre 2017)
7. Billion –Broadband Powerline Smart Lighting Wireless Bridgehttp://www.billion.com/upload/product/doc/2016120116185912.pdf (29 settembre 2017)
8. Billion - Broadband Powerline Smart Lighting Segment Controller, http://www.billion.com.tw/upload/product/doc/2017011014143612.pdf (29 settembre 2017)
9. Eliko – SmartELI Street Lighing Control System (29 settembre 2017)
10. Philips – Piattaforma CityTouch (29 settembre 2017)
11. https://intelilight.eu/intelilight-plc-streetlight-control-solution-and-smart-city-integrations-in-brasov-romania/ (29 settembre 2017)
12. https://intelilight.eu/the-first-lorawan-compatible-streetlight-control-pilot-project-in-moldova-implemented-by-orange-moldova-and-intelilight/(29 settembre 2017)
13. https://intelilight.eu/intelilight-provides-smart-street-lighting-management-dubai-water-canal/(29 settembre 2017)
14. https://intelilight.eu/intelilight-lora-streetlight-control-solution-successfully-passes-field-trials-szada-hungary/ (29 settembre 2017)
15. http://www.billion.com/upload/web/Case/Everlight.pdf(29 settembre 2017)
16. http://www.billion.com/upload/web/Case/MiTAC.pdf(29 settembre 2017)
17. http://www.billion.com/upload/web/Case/Leadray.pdf(29 settembre 2017)
18. http://images.philips.com/is/content/PhilipsConsumer/PDFDownloads/Italy/ODLI20160616_001-UPD-it_IT-CityTouch_ITA_2016.pdf(29 settembre 2017)
19. http://images.philips.com/is/content/PhilipsConsumer/PDFDownloads/Italy/ODLI20160616_001-UPD-it_IT-CityTouch_ITA_2016.pdf(29 settembre 2017)
20. https://www.eliko.ee/smart-street-lighting-system-monitors-environment-traffic-tallinn/ (29 settembre 2017)
21. UVAX – Presentazione Smart Street ENEA
22. IETF Standard RFC 2865 "RADIUS", http://www.rfc-base.org/rfc-2865.html(29 settembre 2017)
23. https://www.kali.org(29 settembre 2017)
24. https://www.wireshark.org(29 settembre 2017)

CV breve del responsabile scientifico del cobeneficiario, Prof. ssa Federica Pascucci

Federica Pascucci ha conseguito la Laurea in Scienze Informatiche presso l'Università di Roma Tre e il Dottorato di Ricerca in Ingegneria dei Sistemi presso l'Università di Roma "La Sapienza" rispettivamente nel 2000 e nel 2004. Docente dal 2005 presso Dipartimento di Informatica e Automazione dell'Università di Roma Tre. I suoi interessi di ricerca sono nel settore dei sistemi di controllo industriale, della robotica, della fusione dei sensori e della protezione delle infrastrutture critiche (CIP). Diversi articoli pubblicati, nel campo della robotica, si trovano nell'ambito della localizzazione robotica mobile in ambienti non strutturati. Molte tecniche derivate da Fuzzy Logic, Stima Bayesiana e Dempster-Shafer Theory sono state sviluppate e applicate al problema della mappatura della costruzione e della localizzazione basata sulla visione. Più di recente, è stata interessata a cercare e salvare la localizzazione in ambienti molto dinamici utilizzando reti di sensori.