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

MINISTERO DELLO SVILUPPO ECONOMICO

Ricerca di Sistema elettrico

Anomaly detection system per smart street: Studio dei principali strumenti presenti in ambito europeo e progettazione di un sistema di supporto per l'operatore

Giuseppe Bernieri, Federica Pascucci

ROMA TRE
UNIVERSITÀ DEGLI STUDI

Report RdS/PAR2017/058

ANOMALY DETECTION SYSTEM PER SMARTSTREET: STUDIO DEI PRINCIPALI STRUMENTI PRESENTI IN AMBITO EUROPEO E PROGETTAZIONE DI UN SISTEMA DI SUPPORTO PER L'OPERATORE

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

Luglio 2018

Report Ricerca di Sistema Elettrico

Accordo di Programma Ministero dello Sviluppo Economico - ENEA
Piano Annuale di Realizzazione 2017
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: Controllo e valutazione delle infrastrutture pubbliche energivore. Sistema di smart service integrato nell'ambiente urbano.
Responsabile del Progetto: Claudia Meloni, ENEA

Il presente documento descrive le attività di ricerca svolte all'interno dell'Accordo di collaborazione *"AnomalyDetection System per smart service illuminazione pubblica"*

Responsabile scientifico ENEA: Francesco Pieroni
Responsabile scientifico Università Roma Tre: prof.ssa Federica Pascucci

Indice

Sommario

Il presente documento è la descrizione delle attività svolte dal Dipartimento di Ingegneria, Università degli Studi Roma concernenti l'accordo. Il documento, nello stato attuale, è completo, per quanto riguarda la consegna intermedia, ma conformemente all'accordo, rappresenta solo un documento preliminare rispetto alla consegna finale.

In particolare esso riporta

1. Analisi preliminare dei sistemi di anomaly detection per reti di calcolatori e infrastrutture di controllo

2. Linee guida per l'analisi dei requisiti per l'anomaly detection system per smart service di illuminazione pubblica.

3. Presentazione della metodologia di progetto di un semplice sistema di anomaly detection system.

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 da un attacco cyber. Per tale motivo, si vuole progettare un sistema di anomaly detection che sia in grado di identificare situazioni di fault o di attacco del sistema. Allo stesso modo si possono.

1 Introduzione

Questo documento rappresenta il report delle attività richieste dal progetto “Ricerca Sistema Elettrico – PAR 2017 – Progetto D6 – Accordo di Collaborazione ENEA – Dipartimento Ingegneria, Università degli Studi Roma Tre”. Le attività previste dall’accordo consistono in:

1. **Analisi degli anomalydetectionsystem**: in questa report sono proposti i classici sistemi di IDS presenti in letterature per le reti informatiche, che allo stato attuale sono anche quelli maggiormente utilizzati nei set up di smartstreet.

2. **Analisi dei requisiti per gli anomalydetectionsystem per smart service di illuminazione pubblica:** il presente report contiene la metodologia di analisi che si vuole effettuare sulla rete della Smart Street presente nello Smart Village nella sede di ENEA – Casaccia e del test-bed basato su concentratore UVAX presente presso il Dipartimento di Ingegneria dell’Università degli Studi Roma Tre. Tali set-up sono analoghi allo smartstreet realizzata nella città di Potenza (Viale Unicef).

3. **Progettazione di un anomalydetectionsystem per smart service di illuminazione pubblica:** in questo report è indicata la metodologia di progettazione che si intende seguire per quanto concerne lo sviluppo di un semplice anomalydetectionsystem per lo Smart Village.

   L’organizzazione del presente documento ricalca le attività svolte, pertanto esso è organizzato in 3 macro-sezione e completato da commenti conclusivi.

2 Analisi degli Anomaly Detection System

2.1 Smart street come Cyber Physical Systems

I Cyber Physical Systems (CPS) sono sistemi che controllano un sistema fisico integrando capacità di computazione e capacità di comunicazione.
A tale scopo i CPS sono formati da un insieme di dispositivi connessi in rete come sensori, attuatori, unità di controllo. I CPS hanno alcune proprietà che li accomunano, quali la tolleranza ai guasti, la scalabilità e l'autonomia. Come sistemi di rete, devono essere organizzati e controllati in maniera distribuita. Infine, i CPS, come tutti i sistemi di controllo, devono rispettare vincoli temporali molto stringenti.

La rapida crescita di sistemi fisici al cui interno sono contenute capacità di connessione alla rete e capacità di calcolo ha promosso lo sviluppo di diversi CPS come dispositivi medici, sistemi per il controllo del traffico, controllo di processo, conservazione dell'energia, controllo dell'ambiente, controllo dei sistemi aerei, controllo delle infrastrutture critiche, sistemi robotici, sistemi di difesa, fabbriche intelligenti e smartcities.

La maggioranza delle applicazioni dei CPS sono safety-critical: un qualsivoglia malfunzionamento causato da un fault o da un attacco informatico può causare danni alla parte fisica del sistema e alle persone che dipendono da esso.

Proteggere i CPS da attacchi informatici e da fault casuali è, pertanto, di grande importanza, ma presenta alcune caratteristiche particolari. Dal punto di vista cyber, meccanismi di prevenzione basati su crittografie e autenticazione sono stati integrati in molti sistemi CPS composti da una grande quantità di nodi distribuiti. Tuttavia, un difetto molto comune di questi meccanismi di protezione è che risultano deboli quando l'attaccante riesce a guadagnare alcuni privilegi di accesso al sistema. Dal punto di vista fisico, in letteratura sono stati presentati diversi algoritmi per identificare fault ed implementare algoritmi di controllo in grado di mantenere in funzione in caso di guasti. Tali algoritmi non sono adeguati per identificare attacchi informatici in quanto progettati per prevedere e guasti fisici occorsi occasionalmente e non provocati intenzionalmente al fine di danneggiare il sistema.
In tale contesto vanno adottate delle soluzioni ibride che comprendano sistemi di identificazione delle intrusioni in grado di identificare minacce a livello fisico e a livello cyber e che tengano conto degli ambienti fortemente dinamici e dei vincoli temporali. Questi sistemi dovranno di necessità utilizzare diverse tecniche. Nei componenti dei CPS caratterizzati da limitate risorse di calcolo saranno implementati maggiormente sistemi di intrusioni semplici e veloci. Nei sistemi più complessi, in cui il flusso di dati è preponderante, si potranno implementare tecniche più sofisticate e accurate

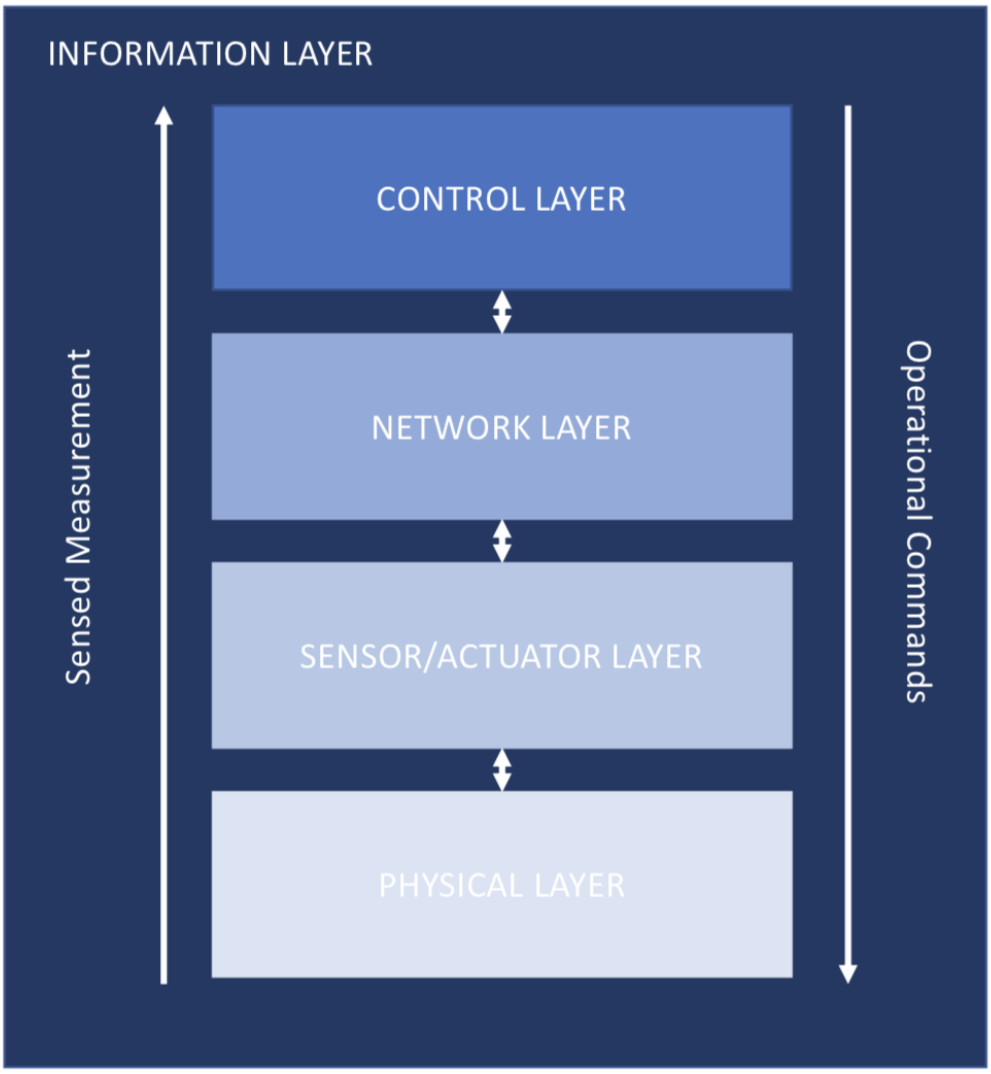

Figura 2.1 Architettura CPS

2.2 Architettura CPS

Una generica architettura per i CPS è rappresentata in Figura 2.1: essa include il sistema fisico, i sensori ed attuatori, le connessioni di rete, il sistema di controllo e il sistema informatico. In particolare

- **Livello fisico:** comprende gli oggetti fisici e i processi del CPS che devono essere monitorati e controllati. Ad esempio, nei sistemi di distribuzione dell'energia questo livello è rappresentato dalla rete di distribuzione. Nei sistemi di illuminazione di smartstreet questo livello è composto dai corpi illuminanti e dalle connessioni fisiche tra questi

- **Livello sensori/attuatori:** comprende tutti i sensori ed attuatori connessi al livello fisico e, pertanto, è strettamente correlato ad esso. I sensori misurano le grandezze di interesse del sistema, mentre gli attuatori agiscono sul sistema per modificarne l'andamento, secondo i comandi elaborati dal controllore. In una rete di distribuzione il livello sensori/attuatori è composto dai sistemi di misura della corrente, della tensione e della fase. Nelle smartstreet, questo livello è composto dai sensori di luminosità, sensori di corrente, sistemi in grado di accendere e spegnere i corpi illuminanti e regolarne la luminosità.

- **Livello di rete:**comprende tutti i dispositivi che garantiscono lo scambio di dati tra livello sensori/attuatori e livello di controllo, pertanto, può essere visto come un ponte tra questi livelli. La comunicazione di questo livello può essere realizzata mediante differenti protocolli. Nei sistemi di distribuzione dell'energia si può utilizzare la comunicazione PLC, come i classici protocolli industriali (MODBUS, DNP, etc) o lo stack di Internet (TCP/IP). Nei sistemi di smartstreet, tipicamente vengono utilizzate comunicazioni PLC oppure wireless, basate su protocolli proprietari o aperti [1].

- **Livello di controllo:**comprende l'insieme dei dispositivi che monitorano la parte fisica del CPS e ne forzano il comportamento. Esso può essere, a sua volta, organizzato in maniera gerarchica nel seguente modo
    - **Sistema di controllo locale:** chiude dei loop localmente ed è localizzato nel sistema fisico e realizza il controllo distribuita. Esso si basa su *programmablelogic computer* o su *remote terminal unit*.
    - **Sistema di supervisione di basso livello:** colleziona i dati del sistema di controllo locale e ne supervisiona il comportamento. Esso realizza anelli di controllo che prendono decisioni a livello di sistema
    - **Sistema di supervisione di alto livello:** contiene l'interfaccia operatore (Human Machine Interface) e pertanto è il mezzo con cui l'operatore umano può agire sul sistema (*human-assisted control*). In generale l'operatore supervisiona il sistema, prendendo decisioni solo in caso di emergenza.

  Nei nostri esempi il livello di controllo è dato del sistema SCADA che governa il funzionamento del sistema di distribuzione dell'energia o dal sistema di supervisione implementato a bordo della controlunit di un sistema di smartstreet[1].

- **Livello di informazione:**è un livello astratto che penetra tutti i livelli del CPS e ne caratterizza il flusso di informazione. In particolare possiamo identificare due differenti flussi di informazione:
    - **Misure dei sensori:** è il flusso di informazioni relativo ai dati raccolti dal sistema sensoriale e inviati al sistema di controllo
    - **Comandi operativi:** è il flusso di informazioni relativo ai comandi che il livello di controllo invia agli attuatori affinché questi agiscano sul sistema fisico.

I CPS possono essere visti come l'evoluzione e la confluenza di sistemi esistenti, quali i sistemi embedded in tempo reale, i sistemi di controllo digitali, le reti di sensori. Come tali, essi hanno ereditato diverse caratteristiche, quali l'essere sistemi

- **distribuiti:** sistemi complessi di grandi dimensioni, distribuiti geograficamente e funzionalmente, in grado di prendere decisione e reagire ad eventi in maniera coordinata e distribuita;

- **real-time:** sistemi in grado di reagire agli stimoli nei tempi previsti e soddisfare vincoli temporali stringenti la cui violazione porterebbe alla distruzione del sistema stesso;

- **autonomi:** sistemi complessi che interagiscono tra di loro in maniera indipendente per portare a termine un compito comuno sotto la guida di controlli automatici e la supervisione umana;

- **confidenziali:** sistemi estesi, appartenenti a differenti organizzazioni in grado di condividere in maniera sicura le informazioni

- **resilienti:** sistemi in grado di riconfigurarsi per mantenere alcuni livelli di servizio. A tale scopo devono essere tali che un fault occasionale non comprometta la capacità di individuazione dei guasti; devono essere in grado di prendere decisioni in caso di informazione parziale e di incertezza;

devono essere in grado di valutare gli impatti sul livello fisico sul livello fisico di un attacco informatico.

Un classico esempio di CPS è costituito dai sistemi di controllo industriali, i cui componenti fondamentali sono rappresentati in Figura 2.2

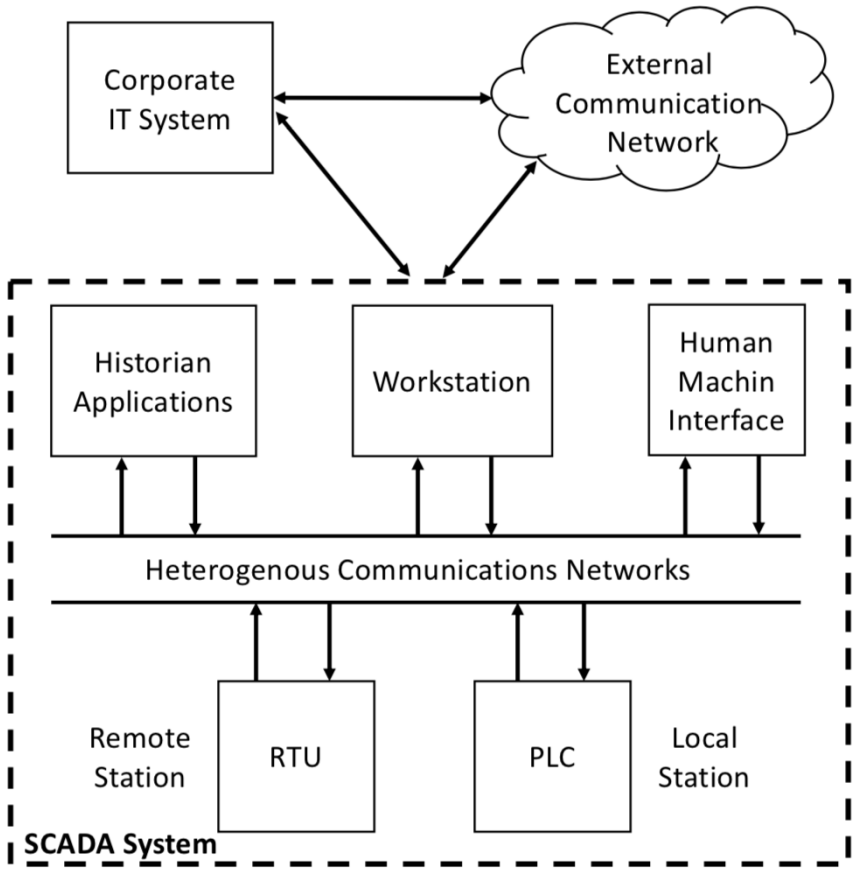

Figura 2.2 Sistema di Controllo Industriale

I sistemi di controllo industriali sono composti da un

- impianto da controllare che rappresenta il livello fisico del CPS;
- sensori ed attuatori: che rappresentano l'omonimo livello dei CPS
- rete che connette i sensori e gli attuattori alle remote terminal unit o ai programmablelogic controller, la rete che connette il sistema di controllo di basso livello al sistema di supervisione;
- il sistema di controllo (livello di controllo) che si compone di un sistema di basso livello composto dai programmablelogic computer chiudono i loop di basso livello e dalle remote terminal unit che concentrano i dati. Un sistema SCADA (Supervisory Control And Data Acquisition) che consente la supervisione automatica e l'interazione tra il sistema e l'uomo;

- l'infrastruttura IT degli operatori che consentono rendere remote alcune procedure.

Anche i sistemi di illuminazione per smartstreet possono essere considerati dei CPS. Considerando il sistema UVAX installato preso ENEA-Casaccia, possiamo osservare come possa essere ricondotto ai livelli architetturali introdotti in precedenza. In particolare

- livello fisico: è composto da una serie di corpi illuminanti equipaggiati con nodi di telecontrollo che attribuiscono a questo livello capacità di connessione;

- livello sensori e attuatori è composto da una serie di nodi collegati tra loro per realizzare la strada intelligente

- livello di rete è composto da una parte basata su reti ad onde convogliate (rete PLC – Power Line Communication) che connette sensori ed attuatori con il sistema di controllo, e una parte costituita dai protocolli di Internet (TCP/IP) che serve a connettere i concentratori con l'operatore

- livello di controllo è costituito da una serie di nodi concentratori dotato di modem PLC e collegamento Ethernet su cavo. Grazie al collegamento PLC possono chiudere i loop di basso livello, mentre il collegamento Ethernet può essere utilizzato dall'utente per accedere al 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.

2.3 Vulnerabilità e minacce dei CPS

I CPS sono sistemi distribuiti complessi, spesso dispiegati in un ambiente non controllato: è quindi molto facile che essi siano soggetti a guasti casuali o ad attacchi mirati. Considerando la superficie di attacco, le vulnerabilità vengono normalmente classificate come

- **Vulnerabilità interne:**il sistema è soggetto a malfunzionamenti dovuti a difetti di progettazione, implementazione o errori umani. Alcuni guasti possono essere causati dalla presenza dell'operatore umano nel loop di supervisione controllo (cattiva scelta dei valori di alcuni parametri come set-points o valori soglia). Ulteriori vulnerabilità interne possono essere costituite da specifiche non corrette sul flusso informativo, flusso di controllo, inconsistenza dei protocolli di comunicazione, errori di configurazione nei dispositivi e bug nel software.

- **Vulnerabilità esterne:** il sistema fisico può essere soggetto a continui transitori causa di comandi non corretti. I sensori sono normalmente costituiti da risorse limitate e possono essere soggetti a failure di vario tipo.

Nella Tabella 2.1sono riportate le vulnerabilità dei CPS.

Vulnerabilities	
External	**Internal**
Large Scale	Internet Specification
Wide Distribution	InconsistentProtocols
PhysicalInteraction	Device Errors
Resource Limitation	Software Bugs
	Human-Made Errrors

Tabella 2.1 Vulnerabilità dei CPS[2]

Le potenziali minacce contro i CPS possono essere individuate esplorando i vari livelli introdotti dall'architettura astratta proposta inFigura 2.1. In generale una minaccia è definita come la possibilità di tentare o di eseguire un accesso non autorizzato al sistema o ai suoi componenti al fine di rendere il sistema stesso non affidabile o non utilizzabile [3].

A livello fisico, una minaccia è rappresentata dalla distruzione parziale o totale della parte fisica del CPS. In questo caso, le misure percepite dai sensori risulteranno inaccurate e produrranno decisioni di controllo non appropriate.

A livello di sensori ed attuatori le minacce sono simili a quelle che si hanno nelle reti di sensori [4]. Un sensore può essere catturato per comprendere il funzionamento della rete e sferrare attacchi agli altri sensori/attuatori. Un attaccante può lavorare direttamente sul nodo dal punto di vista fisico o da quello software al fine di estrarre dati sensibili (come ad esempio chiavi, certificati, etc). Infine, se il nodo ha una fonte di energia limitata, l'attaccante potrebbe far in modo di consumarla velocemente (ossia provocare un *powercomsumptionattack*) aumentando il carico di connessioni effettuate.

Le minacce alla sicurezza del livello di rete dipendono dalle comunicazioni. Il *replay attack* consiste nel inviare ad un destinatario sbagliato delle informazioni oppure nel inviarle/reinviarle con un certo ritardo. L'attacco più semplice da effettuare e, al contempo, più efficace è rappresentato dal *Denial of Service (DoS)* che è definito come qualsiasi evento che riduce o elimina la capacità di comunicazione rendendo di fatto alcuni dispositivi/servizi non disponibili. Il DoS può essere classificato in base alla sua implementazione. Gli attacchi più comuni che lo realizzano sono:

- *Jammingattack:* viene eseguito interferendo con i segnali di comunicazione di un nodo o di un gruppo di nodi;

- *Collisionattack:* viene eseguito violando il protocollo di comunicazione, trasmettendo sul canale in continuazione informazioni in modo da saturarlo e generare collisioni;

- *Routing ill-diretctingattack:* viene eseguito non instradando i pacchetti che richiedono comunicazioni multi-hop;

- *Floodingattack:* viene eseguito generando una quantità ragguardevole di richiesta di connessione al nodo che viene attaccato;

- *Wormholeattack:* viene eseguito mediante l'inserimento di wormhole che compromettono il normale routing dei pacchetti;

- *Selectiveforwardingattack:* viene eseguito attaccando i nodi di una rete permettendo la trasmissione selettiva di alcuni messaggi, compromettendo le trasmissioni dei dati.

Le minacce legate al livello di controllo sono principalmente quelle che mirano a compromettere la capacità di risposta entro i vincoli temporali del sistema, de-sincronizzandolo. Altre tipologie di attacco più sofisticate sono che utilizzano la logica del controllore per destabilizzare il sistema. In questo caso l'attaccante conosce il sistema di controllo e compromette le misure al fine generare comandi di attuazioni capaci di rompere il sistema. Allo stesso modo i dati visualizzati dall'operatore possono essere compromessi per attivare delle procedure di emergenza che potrebbero compromettere o degradare il funzionamento del sistema.

Le minacce del livello informazione sono legate alla possibilità, da parte di un avversario, di collezionare le i dati dei sensori o i comandi agli attuatori. In questo contesto, gli attacchi principali sono

- *Eavesdroppingattack:* consiste nel catturare i pacchetti di rete per studiarne il payload;

- *Trafficanalysis:* consiste nel catturare il traffico di rete per analizzarne le caratteristiche, come ad esempio, numero medio di pacchetti scambiato in un determinato intervallo temporale, sequenze caratteristiche di pacchetti, etc.

In Tabella 2.2sono riportati le minacce più comuni secondo la divisione in livelli presentata.

Layers	Threats	Details
PhysicalLayer	Direct interventions and damages	Immediate damages for hardware
Sensor/ ActuatorLayer	Nodecapture	An instrument for mounting counterattacks
	Nodedestruction	Destruct, extract, or modify node physically
	Powerconusmption	Quickly derain out limited power of sensor
	Cryptographicattacks	Crack secret keys wih brute force, dictionary, or monitoring
Network Layer	Replay	Forward message to an incorrect destination or with delay
	DoS	Result in jamming, colluding, and flooding: ill-redirect routing
	Sybil	An adversary illegitimately takes on multiple identities
	Spoofing and altering routing information	Change routing information illegitimately
	Wormhole	Disrupting routing
	Selective forwarding	Disruptive continuity of transmission
Control Layer	Desynchronization	Break timeliness
Information Layer	Privacy	Steal information by eavesdropping and traffic analisys
	Policy	Breach policy by excuse attack and newbie picking

Tabella 2.2 Minacce per CPS[2]

La classificazione proposta non cattura la complessità dei sistemi CPS, i cui livelli sono tra loro fortemente accoppiati. Un malfunzionamento o un attacco informatico su un livello ha un effetto anche sugli altri in maniera interdipendente. Per meglio cogliere questa complessità, in letteratura è stato introdotto [5]l'*attackspace*: esso è uno strumento che permette di valutare le conoscenze del sistema che un attaccante deve avere e il danno che un attacco può arrecare.

L'attackspace si visualizza in maniera grafica mediante un sistema di riferimento cartesiano, i cui assi assumono i seguenti significati:

- **DisclosureResources(asse x):** indica i dati che l'attaccante deve scoprire per realizzare un attacco;
- **System Knowledge (asse y):** indica la conoscenza a priori del sistema che l'attaccante possiede;
- **DisruptionResources (asse z):** indica le risorse il cui funzionamento verrà compromesso a valle dell'attacco.

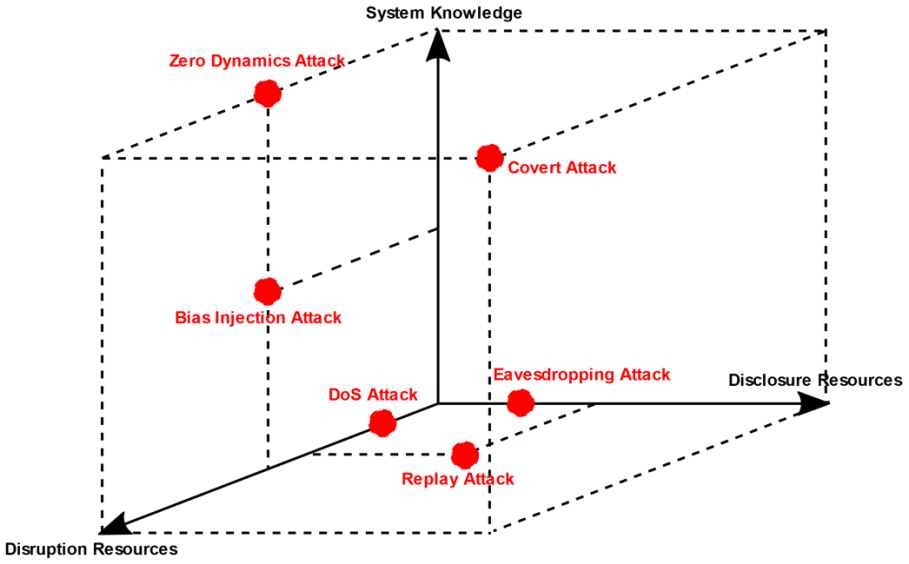

Figura 2.3 Attack Space

All'interno dello spazio tridimensionale è possibile inserire i vari tipi di attacco, come mostrato in Figura 2.3. In particolare, un eavesdroppingattack non mira a compromettere alcuna risorsa e non richiede alcuna conoscenza del sistema, pertanto assumerà valori solo sull'asse x. Un replay attack, invece, richiederà la scoperta di alcuni dati, mirerà a compromettere le performance del sistema, ma può essere eseguito senza avere dettagli sul funzionamento del sistema stesso. Pertanto, esso può essere identificato come un punto sul piano formato dagli assi (x-z). Al contrario, un attacco che modifica i valori dei sensori inserendo un valore costante (*biasinjectionattack*), richiede la conoscenza del sistema per identificare le misure ed ha come obiettivo il malfunzionamento del sistema stesso. Esso non prevede alcuna conoscenza appressa online, pertanto può essere rappresentato come un punto sul piano formato dagli assi (y-z).

2.4 IDS per CPS

La sicurezza dei sistemi di smartstreet è fortemente legata alla duplice natura del sistema stesso. Esso, infatti, è composto da una parte fisica che realizza la struttura di illuminazione ed una parte software che ne controlla il corretto funzionamento. Il mantenimento della sicurezza di questo sistema, quindi, deve abbracciare categorie diverse, prevedendo la protezione dell'infrastruttura fisica, il corretto funzionamento dei processi, la salvaguardia delle comunicazioni e la gestione del ciclo di vita sia dell'hardware che del software del sistema. Questo rende, ovviamente, la gestione della sicurezza di un tale sistema più complessa della normale gestione di un sistema informatico e, per alcuni aspetti, più vicina a quella di un sistema di controllo industriale (ICS) o di un sistema SCADA.

Riguardo la prevenzione e la protezione dei sistemi SCADA e dei ICS da attacchi informatici, in letteratura sono presenti diversi studi. Questi sono in genere limitati ad aspetti particolari di un sistema di controllo applicato in un particolare ambito, tuttavia è radicata la convinzione che, al fine di proteggere adeguatamente tali sistemi, è necessario tenere sotto controllo sia la parte cyber che quella fisica contemporaneamente.

A tale riguardo, pertanto, le tecniche di protezione più efficienti si rivelano quelle basate su IntrusionDetection System (IDS): queste, infatti, sono in grado di rilevare comportamenti non regolari del sistema a partire dal traffico dei dati scambiati all'interno di esso e dare un allarme all'operatore. Questo aspetto di coinvolgimento dell'operatore è fondamentale quando si gestiscono sistemi fisici, il cui malfunzionamento può avere delle ripercussioni a cascata difficilmente controllabili con azioni automatiche: si pensi, a esempio, ad un sistema di semafori intelligenti, il cui blocco automatico potrebbe avere ripercussioni sul traffico, se non gestito adeguatamente.

In linea generale, un IDS è un sistema che analizza il traffico di una rete per identificarne eventuali malfunzionamenti. A tale fine, l'IDS deve essere in grado di raccogliere i pacchetti che viaggiano all'interno della rete e di estrarre le opportune informazioni riguardanti lo stato del sistema, mediante l'estrazione di dati contenuti nell'header del pacchetto o nel payload. Differenti tipologie di IDS possono essere implementate a seconda dei parametri che vengono considerati per analizzare il traffico di rete.

Questa tipologia di sistemi è nota nella letteratura riguardante la sicurezza nel campo dell'*information technology*(IT) e vengono utilizzati anche in quello dell'*operationaltechnology*(OT), più vicino all'ambito dei CPS. Gli approcci utilizzati nell'uno e nell'altro ambito sono simili sotto alcuni punti di vista, tuttavia presentano delle peculiarità legate ai sistemi che vengono protetti.

Per quanto riguarda i CPS alcuni requisiti degli IDS sono collegati alle caratteristiche specifiche di questa tipologia di sistemi. In particolare, un IDS per CPS dovrà essere distribuito: ci si aspetta che un IDS possa collezionare e processare i dati in punti diversi del sistema in maniera distribuita e non in maniera centralizzata. In questo modo ogni componente della rete partecipa al processo e l'onere computazionale è suddiviso tra i vari nodi: questo approccio è particolarmente interessante quando i nodi hanno limitate capacità di calcolo.

Gli IDS devono soddisfare i vincoli di tempo del sistema, in maniera da non introdurre ritardi nell'identificazione di situazioni critiche.

Gli IDS devono avere una certa autonomia e capacità di auto-organizzarsi per identificare sia minacce note che nuove.

Gli IDS devono essere in grado di identificare i guasti casuali, prendere decisioni in caso di conoscenza parziale e/o incerta e capire gli effetti che un attacco ad un livello può causare negli altri.

Infine, nella letteratura dei sistemi di sicurezza in ambito IT, tre ulteriori caratteristiche sono importanti:

- **Confidentiality (C):** è la caratteristica di mantenere le informazioni sensibili o le risorse riservate. La necessità di preservare tali informazioni è evidente quando si considerano sensori sensibili come quello industriale o governativo. Considerando sistemi in rete, anche la protezione dei dati degli utenti riveste molta importanza. Gli IDS devono mantenere la confidenzialità dei dati, quando operano su grandi infrastrutture gestite da diversi operatori. Questo permette mantenere la privacy sui dati critici per l'operatività dell'infrastruttura nel mercato.

- **Integrity (I):**si riferisce all'integrità dei dati (cyber integrity) e all'affidabilità delle risorse (physicalintegrity). Questa caratteristica mette in evidenza il bisogno di prevenire cambiamenti impropri o non autorizzati attraverso attori malevoli. L'integrità è considerata in ogni suo aspetto, sia per quanto riguarda il contenuto dell'informazione, sia per quello che riguarda la fonte dell'informazione. Per i CPS l'integrità è riferita ai dati e alle sorgenti di essi, ossia i sensori, gli attuatori ed i controllori di ogni livello ed è importante che essa sia mantenuta nel passaggio dei dati attraverso il canale di comunicazione.

- **Availability (A):**si riferisce alla capacità di poter sfruttare le risorse del sistema. Se il sistema non è disponibile, non può provvedere ad alcun servizio verso l'utente. Il problema della disponibilità del sistema è rilevante per la sicurezza in quanto un attore malevolo potrebbe intenzionalmente voler limitare l'accesso ad una o più problema. Per i CPS l'availability riguarda la possibilità di poter effettivamente disporre di ogni suo componente. Se un sensore non è più raggiungibile, questo diventa un problema di availability.

Per quanto riguarda la sicurezza in ambito IT, l'ordine di priorità delle caratteristiche appena descritte è CIA [6]: la confidenzialità assume un'importanza maggiore, seguita dall'integrità e dalla disponibilità del sistema. Per i CPS, invece, viene considerato l'ordine inverso AIC, dove la disponibilità dei dati e delle risorse gioca un ruolo centrale in quanto la mancanza di dati o risorse può causare seri danni al sistema, alle persone e all'ambiente.

2.5 Tassonomia degli IDS per CPS

In letteratura sono molteplici le tassonomie che vengono usate per classificare gli IDS. In particolare questi sono gli elementi che comunemente vengono presi in considerazione sono

- **Posizionamento dell'IDS;**
- **Tecniche di osservazione del traffico;**
- **Tipologia di flussi analizzati;**
- **Tipologia di dati elaborati dagli IDS;**
- **Metodologie di detection.**

2.5.1 Posizionamento dell'IDS

Una classificazione per gli IDS può essere fatta in base al posizionamento del dispositivo. In particolare si possono riconoscere due diverse configurazioni:

- **Host-based IDS:** il sistema di identificazione viene utilizzato per monitorare lo stato interno di un host e le sue connessioni di rete. Esso è in grado di monitorare il comportamento dinamico dell'host ed il suo stato. Questa configurazione veniva utilizzata per diagnosticare i malfunzionamenti dei mainframe, che avevano limitate interazioni con l'esterno.

- **Network-based IDS:**è collocato sulla rete ed è posto a guardia di essa. Il suo compito è quello di monitorare ed analizzare il traffico della rete al fine di rilevare pattern di comunicazioni sospetti, che potrebbero rappresentare una minaccia per i sistemi connessi alla rete.

- **Distributed IDS:** è un componente software separato, detto agente o probe. Sono distribuiti nella rete e negli host al fine di monitorare specifici component. Generalmente riportano i risultati ad un IDS centralizzato in grado di derivare lo stato del sistema nel suo complesso.

2.5.2 Tecniche di osservazione del traffico

Una classificazione per gli IDS può essere fatta in base alle tecniche utilizzate per osservare il traffico, ossia raccogliere i pacchetti dalla rete. In letteratura [7] vengono distinti due approcci differenti, detti, rispettivamente, *passivo* e *attivo*.

Le misure passive sfruttano dispositivi che osservano il traffico di rete senza interferire con esso. Esse vengono effettuate mediante monitor inseriti nella rete per osservare passivamente il traffico di rete e collezionare misure attraverso statistiche sui pacchetti e attraverso il tracciamento di particolari pacchetti già presenti nella rete. Le tecniche che vengono utilizzate per effettuare misure passive sulla rete possono dividersi in due categorie, sulla base della quantità di dati analizzati:

- **online inspection:** considera solo statistiche sui pacchetti e sui flussi nella rete. Esempi di queste statistiche sono il conteggio dei pacchetti, il conteggio del numero di byte, etc

- **offline trace filesanalysis:** effettua un'analisi più specifica dei pacchetti, copiandoli parzialmente (ad esempio solo l'header) o totalmente. Le copie dei pacchetti vengono organizzate in file (trace files) che successivamente vengono analizzate offline.

Gli operatori di rete dispiegano nell'infrastrutture i monitor passivi, come trappole realizzato con Simple Network Management Protocol (SNMP), analisi di flusso effettuate con Netflow e syslog posizionati sui dispositivi di rete. Questi consentono di misurare passivamente i parametri di funzionamento della rete effettuando diagnosi e localizzando eventuali malfunzionamenti.

Le misure attive, invece, vengono effettuate mediante dei pacchetti di saggio (*probe packets*) che vengono immessi sulla rete da analizzare al fine di effettuare statistiche. Ad esempio, un eventuale ritardo o una perdita di pacchetti può essere individuata inviando i probe packets tra due nodi di interesse.

Le misure attive vengono realizzate mediante strumenti quali i comandi ping o traceroute. Questi sono in grado di fornire informazioni sulla latenza della rete, il percorso di routing eseguito, la capacità delle connessioni che compongono il percorso.

Quando si considera un sistema di controllo, l'approccio attivo non è comunemente utilizzato, in quanto i pacchetti di saggio possono alterare il funzionamento nominale del sistema introducendo ritardi e portando il sistema verso l'instabilità. Ancora, le statistiche elaborate tramite i probepackets all'interno di un sistema di controllo non sono così interessanti: per le caratteristiche di ripetitività, infatti, le statistiche di un sistema di controllo possono essere facilmente ricavate osservando in maniera passiva il sistema stesso.

2.5.3 Tipologia di flussianalizzati

Un'altra classificazione che può essere fatta è quella in base alla modalità con cui il traffico di rete è catturato e analizzato. Le modalità più utilizzate sono

- **Switched Port Analyzer (SPAN):** considera tutti i flussi esistenti sulla rete;
- **Statistical probes**: considera in maniera selettiva solo alcuni flussi.

Lo SPAN o porta di mirroring è un elemento che si trova abbastanza comunemente negli switch di rete e ad essa può essere connesso un IDS. Come si vede dalla Figura 2.4, lo switch esegue un portmirroring, ossia replica il traffico di rete che passa attraverso lo switch e lo invia ad una specifica porta (SPAN). Tre computer sono connessi ad uno switch e comunicano sulla rete (traffico giallo, blu e verde), tutto il traffico viene copiato e riproposto sulla porta SPAN.

È possibile selezionare le porte da monitorare: in tal caso il traffico collezionato dalla SPAN sarà quello relativo alle connessioni in entrata ed in uscita da tali porte.Un sistema di analisi procederà poi ad analizzare tutto il traffico per identificare attività malevole [3].

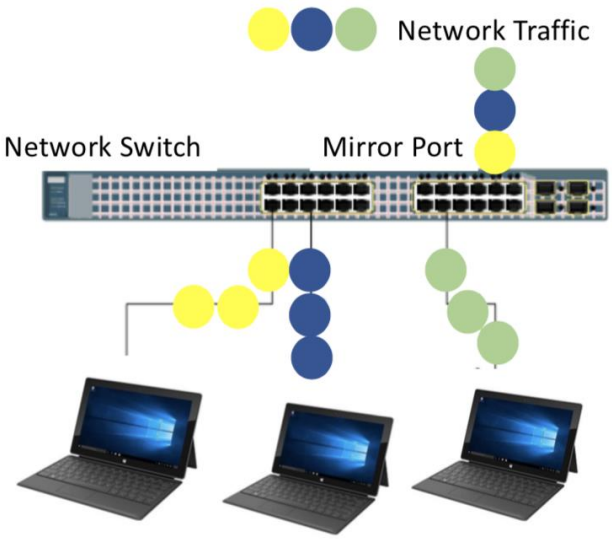

Figura 2.4Mirroring

Il maggior svantaggio relativo a questa modalità è la quantità di dati da analizzare. Se si procede ad un'identificazione online, l'IDS deve essere sufficientemente potente per processare tutti i dati. Se si procede ad un'identificazione offline, la memoria utilizzata per raccogliere i dati diventa rilevante.

Con l'avvento delle reti ad alta velocità sia l'identificazione online che quella offline risultano difficili per l'alta quantità di dati generata in tempi brevi. Per questo motivo si preferisce utilizzare strumenti selettivi, in grado di analizzare solo alcuni set di dati. In particolare vengono considerati i cosidetti*statisticalprobles*: essi sono flussi di dati i cui parametri statistici possono rivelare guasti o malfunzionamenti. Un flusso di dati è definito come una sequenza di pacchetti di rete che hanno lo stesso mittente e lo stesso destinatario. La scelta dei flussi è cruciale per l'efficacia dell'IDS: i nodi monitorati dovranno essere quelli che statisticamente sono soggetti ad essere attaccati, rappresentando l'anello debole del sistema. L'attività malevola, quindi, può essere identificata comparando i pattern nominali con quelli attuali del sistema: ogni deviazione della baseline viene considerata come un attacco. I maggiori produttori di switch hanno proposto architetture per la cattura di flussi, come verrà illustrato in seguito.

2.5.4 Tipologia di dati elaborati dagli IDS

Un'altra classificazione riguarda il tipo di dati che vengono elaborati dall'IDS. Anche in questo caso, si hanno due categorie:

- **Dati di rete:** riguardano il calcolo di parametri statistici della rete;
- **Dati di sistema:** riguardano il calcolo di parametri statistici del sistema.

La prima categoria definisce i comportamenti anomali considerando alcuni parametri statistici della rete e dei pacchetti, come ad esempio il numero di pacchetti scambiati, il numero di byte, la lunghezza media dei pacchetti, etc. Questi dati possono essere ricavati considerando il traffico dei dati e l'header del pacchetto. In particolare, le informazioni sulle statistiche della rete si possono ottenere considerando il livello 2 e 3 della pila ISO/OSI[17]. Questa tipologia di analisi può essere facilmente effettuata on-line nei sistemi di controllo in quanto il traffico è limitato e ripetitivo. In tali condizioni è molto semplice rilevare anomalie. Nelle reti ad alta velocità, come già osservato, l'analisi dell'intera rete potrebbe divenire onerosa.

L'analisi dei parametri statistici del sistema necessita l'estrazione del payload del pacchetto. Questo tipo di analisi, infatti, opera a livello semantico ed è nota in letteratura con il termine di *DeepPacketInspection*(DPI). Dal punto di vista operativo viene effettuata un filtraggio a livello 7 della pila ISO/OSI. Questo significa che l'IDS ispeziona livelli oltre il 3 della pila ISO/OSI: tale analisi non può essere pertanto effettuata da router, che normalmente operano sui livelli 2 e 3 del modello ISO/OSI (ad esempio analizzano la sorgente IP, la destinazione IP, la porta sorgente e la porta target).

Essa verifica la consistenza dei pattern contenuti nei payload con il corretto funzionamento del sistema. Il maggior svantaggio della DPI risiede nella complessità degli algoritmi di ricerca di pattern, sulla cardinalità dell'insieme dei pattern ammissibili, sul possibile overlapping di pattern differenti. Per risolvere parzialmente questi problemi, non ci si può affidare ad algoritmi software per la comparazione delle stringhe, ma si devono considerare soluzioni hardware. Per implementare la DPI, infatti, si utilizzano dispositivi specializzati come Field-Programmable Gate Arrays, Content Addressable Memory o Network Processors. Questi sono in grado di ridurre i ritardi introdotti dalla DPI riducendo al minimo l'impatto sulle prestazioni del sistema.

Nel campo dei CPS, gli svantaggi di questo approccio sono legati alla complessità, ai tempi di esecuzione e al tipo ricerca. Se la DPI non rispetta i vincoli temporali, il funzionamento del CPS potrebbe essere compromesso.Per i sistemi di controllo, tuttavia, un'analisi più approfondita del contenuto dei pacchetti potrebbe rivelarsi più interessante. L'analisi statistica, infatti, ci fornisce i parametri entro cui il traffico di una rete può essere considerato sintatticamente corretto.

2.5.5 Metodologie di detection

In base alle metodologie di detection, gli IDS possono essere classificato in tre categorie come

- **Basatisu signature;**
- **Basati su regole (rule-based);**
- **Statistici;**
- **Metodicomputazionali;**
- **Metodibasatisulmodello.**

I sistemi di identificazioni basati su signature rilevano la presenza di pattern tipici. I pattern tipici si riferiscono a situazioni di attacco ben specifiche e sono collezionati in una base di conoscenza a priori. Quando un pattern viene rilevato nel flusso di dati, allora viene segnalato un allarme. La presenza di una conoscenza a priori non legata a fasi di learning rende questi sistemi facilmente implementabili, tuttavia sono scarsamente efficaci rispetto a nuovi attacchi.

I sistemi di identificazione ruled-based confrontano i dati ottenuti a diversi livello con una base di conoscenza a priori. Se i dati sono consistenti rispetto alla conoscenza a priori, il sistema sta funzionando correttamente, altrimenti viene riscontrata una violazione. Se l'insieme di regole può essere provato in maniera computazionalmente poco costosa, questa tipologia di IDS risulta molto veloce ed efficiente. Essendo la conoscenza a priori definita nell'implementazione, non richiede fasi di learning e può essere facilmente implementato in forma distribuita. Il lato negativo è rappresentato dalla scarsa capacità di far fronte a situazioni in cui la conoscenza è parziale o il rumore risulta rilevante.

I sistemi signature-based e basati su regole sono molto simili nel meccanismo di detection, ma differiscono nella modalità con cui viene definita la conoscenza: gli IDS signature-based sono fortemente legati a degli attacchi specifici, mentre gli IDS rule-based sono risultano più flessibili.

Gli approcci di tipo statistico sono molto utilizzati per gli IDS: essi assumono che il comportamento nominale del sistema occorra con una probabilità più alta delle anomalie. Si possono distinguere due tipi di IDS statistici

- **Approcci parametrici:** la distribuzione di probabilità che descrive lo stato del sistema è supposta nota (non ci sono fasi di learning). I parametri di tale distribuzioni vengono comparati con quella del flusso di dati che si sta analizzando.

- **Approcci non parametrici:** la distribuzione non è nota a priori, ma viene appresa dal sistema analizzando il suo comportamento.

Gli approcci parametrici fanno delle assunzioni sul comportamento del sistema molto forti e risultano molto veloci non dovendo effettuare alcuna fase di learning. Questa, invece, è necessaria agli approcci non parametrici che devono apprendere la distribuzione di probabilità. I primi risultano meno flessibili nella gestione di scarsa informazioni, mentre gli ultimi risultano più flessibili. Gli approcci parametrici possono applicarsi ad un ristretto numero di casi, mentre quelli non parametrici scontano come svantaggio un overhead computazionale ragguardevole.

Le tecniche computazionali sono basate su data mining e/o machine learning. Esse apprendono il profilo della rete mediante una procedura di learning, che può essere supervisionata, semi-supervisionata o non supervisionata. La detection viene effettuata mediante algoritmi di classificazione o di ottimizzazione.
Riguardo l'analisi semantica del contenuto dei pacchetti di rete (cioè l'analisi a livello 7 della pila ISO/OSI), differenti tecniche si possono applicare per identificare pattern che non dovrebbero accadere (i.e., outliers, eccezioni, faults, etc). In [3], gli approcci che maggiormente vengono utilizzati sono divisi nelle seguenti categorie:

- Approcci basati sulla classificazione: consistono nel creare dei pattern analizzando la rete durante il suo funzionamento nominale (fase di learning) per poi classificarne il comportamento. Utilizzano tecniche come le reti neurali, le reti bayesiane o le supportvectormachines.

- Approcci basati sul nearestneighbour: assumono che istanze di dati con caratteristiche simili rappresentano la situazione normale, mentre situazioni anomali presentano caratteristiche diverse.

- Approcci basati sul clustering: dividono istanze di dati in cluster e identificano l'anomalia come l'impossibilità di assegnare ad un cluster un'istanza di dati.

- Approcci statistici:

    - Approcci basati sulla teoria dell'informazione: assumono che le anomalie inducono dati irregolari

    - Approcci basati su analisi spettrale: riducono il set dei dati in un sottospazio più piccolo dove è più facile identificare le anomalie.

I metodi basati sul modello, infine, sono mutati dal contesto dei controlli automatici tolleranti ai guasti. Esso è implementato per identificare attacchi sulla rete o sul livello di controllo analizzando il comportamento del layer fisico [21].

A tale scopo all'interno dell'IDS viene implementato un *digital twin* del sistema, ossia una copia sintetica di esso. Lo schema del modello di detection è proposto in Figura 2.5.

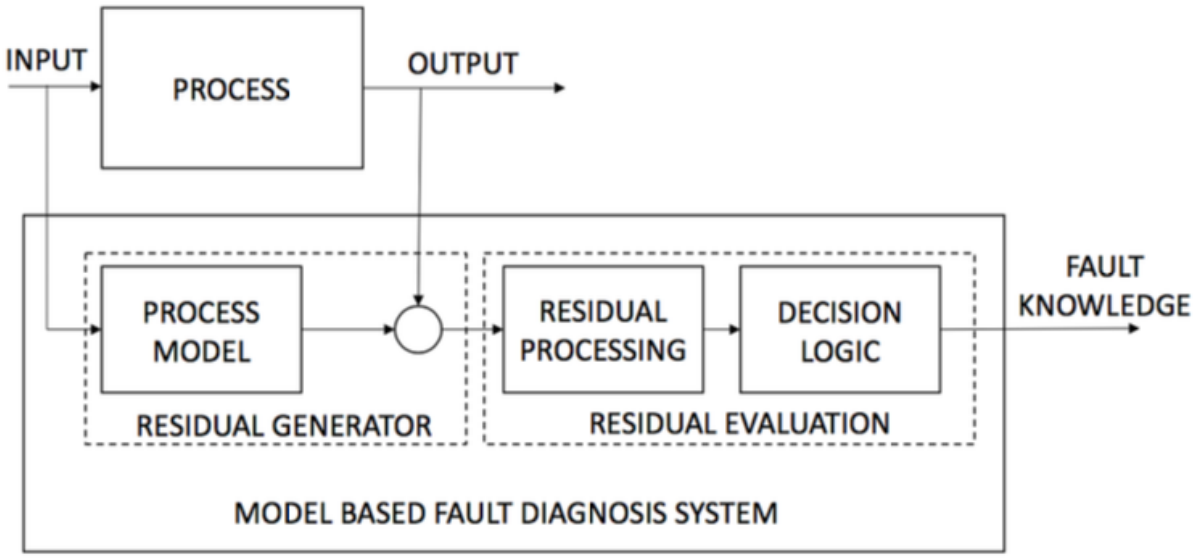

Figura 2.5 IDS basati sul modello

Il digital twin riproduce il comportamento del sistema fisico ricevendo i medesimi input del sistema reale. Mediante algoritmi di stima e filtraggio il digital twin è in grado di calcolare le misure che il sistema reale, sottoposto a quell'ingresso, produce. Queste vengono confrontate con le misure reali provenienti dal sistema per calcolarne il residuo, ossia lo scostamento tra le misure del digital twin e le misure reali. Tale scostamento è tanto più piccolo, quanto più il digital twin è in grado di imitare il comportamento del sistema. Il residuo viene ulteriormente elaborato in vari modi (calcolo della media, calcolo della norma di Mahalanobis, etc) e comparato con dei valori soglia che permettono di identificare se il sistema funziona in maniera corretta o meno.

Questo approccio, sebbene preveda la conoscenza a priori del modello del sistema, risulta più robusto perché è in grado di catturare la dinamica del sistema e le condizioni al contorno di esso. Ancora, se l'elaborazione dei residui e la regola di decisione sono ben strutturate, è possibile utilizzare questa tipologia di IDS anche quando il rumore sui segnali è alto e la conoscenza del modello è scarsa. Questa tipologia di IDS, infine, può identificare con successo gran parte degli attacchi che si possono effettuare a livello di controllo e che sono più difficile da interpretare da parte degli altri approcci.

2.6 Strumenti per l'implementazione di IDS

Gli strumenti che concorrono all'implementazione di un IDS sono molteplici e si possono dividere in protocolli per il mantenimento della rete (come ad esempio il SNMP), standard per l'analisi di flussi dati e strumenti che implementano l'analisi dei dati. Di seguito verranno analizzati gli strumenti più comunemente utilizzati.

2.6.1 Simple Network Management Protocol

Il Simple Network Management Protocol è un protocollo applicativo della suite TCP/IP. Esso consente di monitorare in maniera passiva il traffico di rete, collezionando il traffico prodotto dai sensori e dagli attuatori della rete target. Il SMNP ha tre componenti principali, come si vede in Figura2.6.

- I dispositivi monitorati (ad esempio, router, switches, bridges, hubs, computer, etc.) che contiene un agente SNMP e sono connessi alla rete da mantenere al fine di collezionare e registrare informazioni;

- Gli agenti SNMP, ossia moduli software all'interno dei dispositivi da mantenere. Le operazioni che compiono sono locali, quindi mantengono informazioni locali nel formato del protocollo;

- Il Network management System (NMS), il sistema che effettua il monitoraggio dei dispositivi basandosi sui dati collezionati dagli agenti.

I comandi di SNMO sono quattro:

- *read*lettura delle variabili,
- *write* scritturadell variabili,
- *traversal* richiesta di specifiche variabili,
- *trap* utilizzato per riportare particolari eventi.

SNMP facilita la manutenzione della rete in termini di capacità, ma non può fornire dettagli sul pattern di traffico. Ancora, SNMP non è un protocollo autenticato, pertanto il suo utilizzo può creare ulteriori vulnerabilità nella rete.

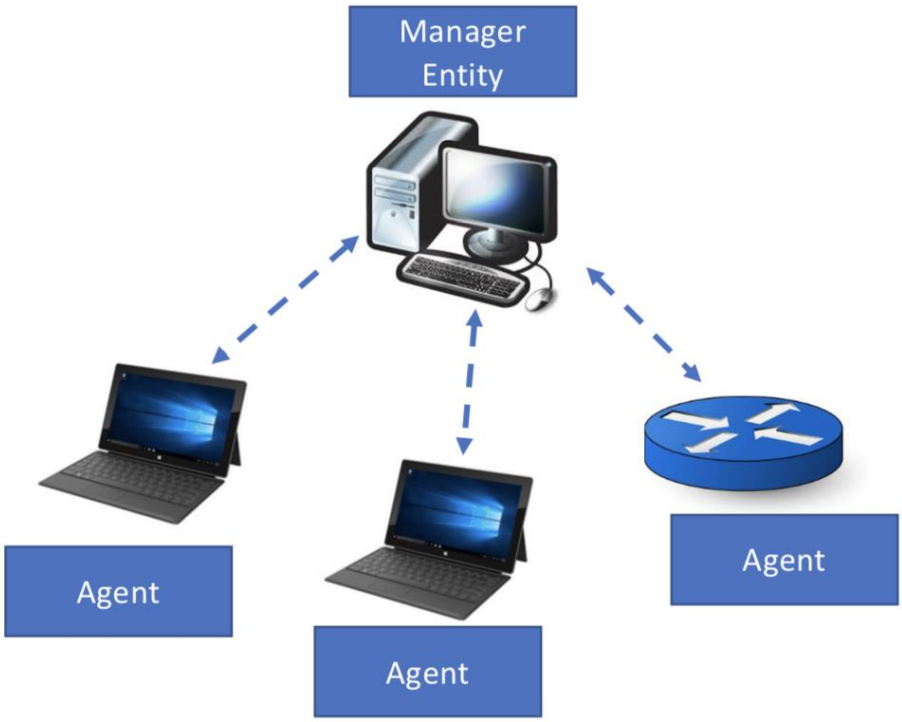

Figura2.6Simple Network Management Protocol

2.6.2 Strumenti per l'estrazione dei flussi.

L'input di un qualsiasi IDS sono le misure del traffico della rete rilevate da vari dispositivi. I dati possono essere forniti a livello di pacchetto oppure a livello di flusso.Con l'avvento delle reti ad alta velocità, un IDS efficace deve basarsi su dati aggregati e i dispositivi di rete devono essere in grado di organizzare il traffico in flussi.

Diversi vendors propongono prodotti con supporti per l'estrazione e l'analisi di flussi di comunicazione. Cisco ha proposto NetFlow, uno standard aperto per l'estrazione e l'esportazione di flussi di dati con l'obiettivo di diminuire il quantitativo di dati registrati. NetFlow registra il traffico a livello IP dai router e dagli switch. La versione 5 di NetFlow definisce un flusso come una sequenza unidirezionale di pacchetti che ha almeno 7 campi dei pacchetti in comune: interfaccia di ingresso, indirizzo IP del mittente, indirizzo IP del destinatario, la porta del mittente, la porta del destinatario e il tipo di servizio IP.

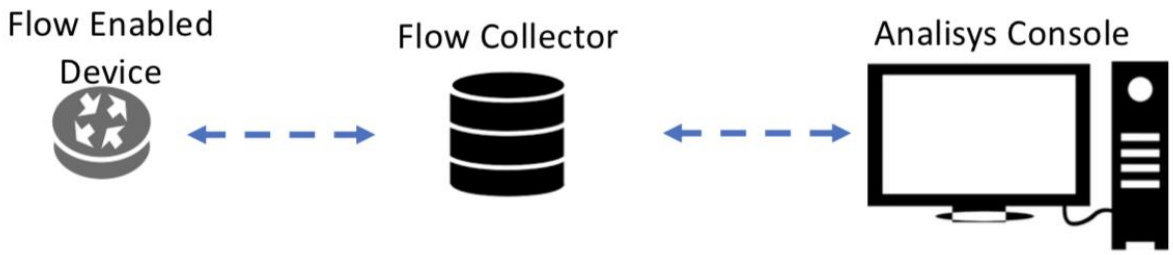

Figura 2.7 Componenti NetFlow

L'architettura di NetFlow è composta da (si veda Figura 2.7):

1. *NetFlowExporter*: raccoglie e decodifica i pacchetti della rete, aggrega i pacchetti in flussi utilizzando una chiave per ogni flusso e li inserisce nel *NetFlowCollector;*

2. *NetFlowCollector*: colleziona i record dei flussi per ulteriori analisi e li rende disponibili all'*Analysis Console;*

3. *Analysis Console*: elabora i flussi per identificare eventi malevoli e valutare le prestazioni della rete individuare problemi di sicurezza (ad esempio DoS, worns, eventi indesiderati). Essa è in grado di visualizzare le analisi prodotte.

Dal 2003, l'Internet Engineering Task Force (IETF) ha accettato come standard industrial NetFlow introdotto da Cisco ed ha propostol'Internet Protocol Flow Information eXport (IPFIX) [16].Questa definisce l'informazioni del flusso IP che verranno trasferite dal router che contiene l'applicazione di analisi dei dati.Dalla version 9 NetFlow è in grado di analizzare anche il traffico UPv6 e il riconoscimento di flusso è limitato ai protocollo TCP e UDP.

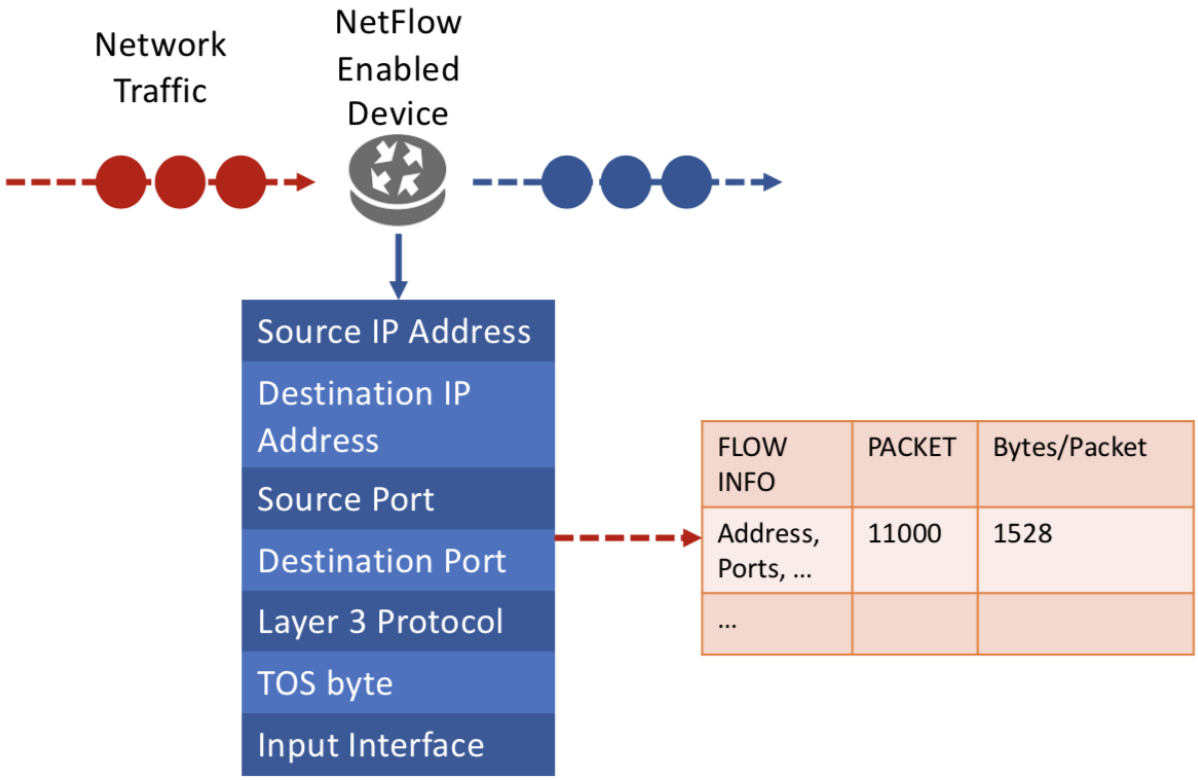

Figura 2.8 Parametri di flusso

Un router che gioca il ruolo di un probe deve mantenere un tabella dei flussi esistenti ed aggiungere nuovi elementi ad essa ogniqualvolta un nuovo indirizzo IP inizia una connessione con un nodo (si veda Figura 2.8). Esso dovrà, per ogni flusso, mantenere dei contatori relativi al numero di pacchetto e alle dimensioni del flusso. Questi contatori sono utili per aggregare i dati catturati ed identificare i flussi spuri che causano colli di bottiglia e potrebbero essere causati da potenziali attacchi.

Un'altra tecnologia importante per l'acquisizione ed il monitoraggio dei dati di rete che si trova all'interno di router e switch è SFlow, rilasciata per la prima volta nel 2001 e la cui architettura è proposta in Figura 2.9. L'obiettivo principale di un agente SFlow è quello di fornire flussi campionati in all'interno di una rete ad alta velocità. SFlow adotta la stessa struttura di NetFlow ad agenti e collector.

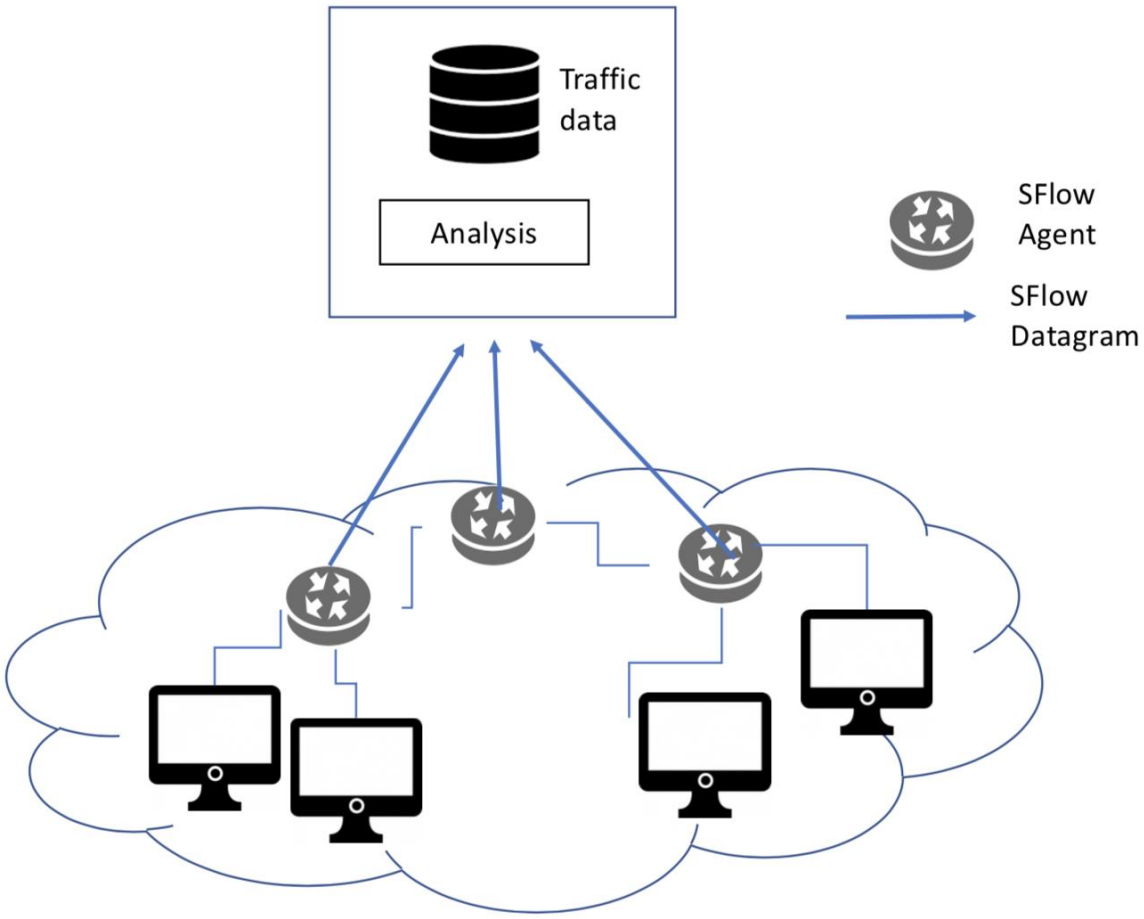

Figura 2.9Architettura SFlow

SFlow utilizza MIB, un'entità che controlla gli agenti sFLOW da remoto per mezzo di un amministratore di rete e definisce il formato dei dati campionati. Quest'ultimo viene utilizzato quando i dati sono inviati al componente che colleziona i dati o a quello che lo analizza.

La maggiore differenza tra NetFlow e SFlow risiede nella scalabilità. NetFlow, infatti, ha capacità limitate quando la rete da analizzare diventa grande e/o produce una quantità di dati rilevante. L'implementazione di un agente che analizza tutto il flusso è impensabile nelle reti ad alta velocità, pertanto SFlow considera solo dati campionati. In particolare invia solo informazioni aggregate sul flusso e non registra il flusso completo all'interno del router o dello switch. In questo modo, il caching non è effettuato a livello di router e questo rende la loro progettazione più semplice e meno complessa, aumentandone la scalabilità.

Il tempo di campionamento per la registrazione del flusso può essere definite dall'utente.
L'architettura del sistema di monitoraggio SFlowè basata su due entità :

1. Agente sFlowimplementato nel router che invia il flusso campionato e i contatori;

2. SFlowcollector: un punto di aggregazione/analisi centralizzato.

2.6.3 Strumenti software per l'implementazione di IDS

NetFlow è uno strumento per analizzare il traffico di una rete in tempo reale a livello macroscopico. Un IDS che sia in grado di identificare azioni malevole deve, tuttavia, analizzare i pacchetti anche ad un livello microscopico. A tale scopo diversi strumenti software sono stati sviluppati.

Il pacchetto software open source più popolare per questo scopo è sicuramente Snort [14]. Nato come sniffer e logger, è costantemente aggiornato e sviluppato come IDS [15]. Snort si configura come un IDS basato su regole: la sua caratteristica base, infatti, è quella di poter definire semplice regole che possano essere utilizzate per identificare un grande insieme di attacchi malevoli, come, ad esempio, bug per corrompere la memoria, scan delle porte, attacchi web, etc). Snort fornisce funzionalità per inviare file di log del sistema mediante mail o syslog. Esso è disponibile per molte piattaforme e sfrutta il paradigma di community [15] per aggiornare continuamente le signature degli attacchi distinguibili.

Un sistema simile è lo strumento software Suricata []: quest'ultimo supporta la sintassi delle signature di Snort, tuttavia, la sua architettura di basso livello è completamente differente.

Un altro strumento software per l'analisi della sicurezza delle reti è Bro [17], anch'esso open-source. Lo strumento Bro converte il traffico di rete in una serie di eventi che possono essere analizzati tramite script appositi, sviluppati dagli amministratori di sistema in base alle specifiche di monitoraggio della rete. La piattaforma Linux fornisce degli strumenti integrati nel kernel del sistema per il filtraggio dei pacchetti di rete dalla versione 2.4.x, mentre L7-filter [18] rappresenta una potente classificatore a livello applicazione.

Sempre per l'analisi a livello applicazione dei pacchetti di rete, un altro strumento molto efficace è la libreria nDPI [19]. Tale pacchetto ha un supporto cross-platform per l'ispezione di pacchetti di rete a livello applicazione ed è progettata per identificare i protocolli di rete senza basarsi sulle porte utilizzate.

3 Analisi dei requisiti per gli anomalydetectionsystem per smart service di illuminazione pubblica

In questa sezione viene descritta la metodologia di analisi che si vuole effettuare sulla rete della Smart Street presente nello Smart Village nella sede di ENEA – Casaccia e del testbed basato su concentratore UVAX presente presso il Dipartimento di Ingegneria dell'Università degli Studi Roma Tre.

Lo smart service di illuminazione pubblica si presenta come un CPS dove i processi fisici, in questo caso inerenti all'illuminazione intelligenteinabienti esterni, vengono gestiti attraverso comunicazioni di rete TCP/IP e Power Line Communication (PLC).

3.1 Descrizione della topologia di rete in ENEA Casaccia

Figura 3.1 Smartstreet ENEA - Casaccia

Come descritto nel documento [1], il progetto Smart Street di ENEA realizza un sistema di strada intelligente all'interno dello Smart Village nella sede di ENEA – Casaccia (Figura 3.1).
Il sistema è costituito da venti lampioni con armature LED Ampera Midi Schreder, equipaggiate con nodi di telecontrollo BPLC UVAX.

Gli obiettivi implementativi del progetto Smart Street prevedono i seguenti punti:

- Telecontrollo dell'illuminazione illuminazione punto-punto con regolazione del flusso in tempo reale;
- Videosorveglianza analisi video;
- Illuminazione adattiva (traffico, meteo, emergenza);
- Servizio WiFi.

L'architettura di rete del sistema è composta da concentratori, nodi e workstations.

I concentratori sono installati all'interno delle cabine elettriche e controllano i nodi (i lampioni intelligenti) direttamente tramite comunicazione PLC.

Le workstation permettono di gestire attraverso interfaccia web il funzionamento dei sistemi implementati per lo Smart Village.

Dal punto di vista informatico, la comunicazione tra concentratore e workstation è esposta a possibili vulnerabilità. È per questo motivo che verranno analizzati possibili implementazioni di sistemi di IntrusionDetection per l'architettura di rete dello Smart Village Enea - Casaccia.

3.2 Configurazioni di IntrusionDetection Systems per smart service di illuminazione pubblica in ENEA Casaccia

Al fine di poter analizzare i sistemi di AnomalyDetection per scenari smartstreet, si presentano due possibili approcci implementativi con relativi requisiti:

- **Host-BasedAnomalyDetection System:** il prototipo di AnomalyDetection System viene implementato direttamente all'interno del nodo concentratore. In questo modo è possibile monitorare il traffico su un nodo appartenente alla rete di comunicazione principale. Il vantaggio di questo approccio risulta nel poter applicare meccanismi difensivi attivi ed automatizzati direttamente sul concentratore interrompendo potenziali flussi dati malevoli. Possibili criticità di questa tipologia di AnomalyDetection System potrebbero essere rappresentate dal carico computazionale derivante dall'analisi del traffico sul nodo concentratore. Il totale accesso al sistema operativo implementato all'interno del concentratore rappresenta il requisito principale per lo studio ed implementazione del prototipo di Host-BasedAnomalyDetection System.

- **Mirrored-BasedAnomalyDetection System:** il prototipo di AnomalyDetection System viene implementato su un sistema ad hoc predisposto all'analisi passiva del traffico di rete sfruttando la tecnologia del Port Mirroring. In questo modo, il sistema di monitoraggio implementato analizza il traffico di rete senza interagire attivamente con esso. Il vantaggio di tale approccio risulta nel poter identificare anomalie sul traffico senza congestionare a livello computazionale le operazioni effettuate dal concentratore, ma sfruttando un sistema predisposto appositamente per l'analisi di sicurezza. Per poter implementare tale sistema è necessario che lo switch di rete al quale è collegato il concentratore sia predisposto per la funzionalità di Port Mirroring. Ulteriore requisito specifico per il Mirrored-BasedAnomalyDetection è la disponibilità di una workstation dedicata predisposta per l'analisi passiva del traffico di rete.

I requisiti per l'analisi ed implementazione di sistemi di AnomalyDetection per smart service di illuminazione pubblica che sono comuni ai due approcci presentati sono:

1. l'identificazione delle caratteristiche principali dei flussi di dati per generare un profilo base per AnomalyDetection;

2. la disponibilità di un Training Set caratterizzato dall'assenza di azioni malevoli;

3. la presenza di uno o più attori malevoli connessi alla rete dello smart service di illuminazione pubblica per la generazione di attacchi cyber controllati.

Considerando lo stato attuale dei sistemi a disposizione e avendo identificato la minaccia alla disponibilità delle risorse come rilevante per lo studio scientifico, in questo lavoro si opterà per analizzare la possibile implementazione di IDS per attacchi informatici volti a ledere la disponibilità delle risorse di sistema.

Per la valutazione dell'efficacia di uno strumento di security è necessaria la presenza di azione (singola o multipla) malevola sulla network in esame. Avendo identificato l'azione malevola sulla disponibilità delle risorse particolarmente problematica per i sistemi implementati per smart service di illuminazione pubblica, si effettueranno specifici esperimenti il cui scopo finale sarà quello di identificare attacchi alla "Availability" delle risorse interconnesse.

Data la natura invasiva delle sperimentazioni, si utilizzerà un testbed appositamente sviluppato per valutare gli attacchi informatici ai sistemi. Il testbed, in maniera semplificata, permette di replicare in ambiente sicuro e controllato il sistema installato presso lo Smart Village nella sede di ENEA – Casaccia.

Verrà quindi effettuato uno studio di prototipo di AnomalyDetectionsystem per l'identificazione di minacce informatiche relative alla disponibilità delle risorse dei sistemi nello scenario di smartstreet. Tale sistema verrà implementato come Mirrored-BasedAnomalyBased e testato sul traffico di rete generato utilizzando il testbed realizzato in laboratorio. Tuttavia, il prototipo di AnomalyDetectionsystem sarà compatibile con entrambi gli approcci implementativi (Host-Based e Mirrored-Based) descritti in precedenza.

3.3 Valutazione Single and Side Points of Failure

Il concentratore implementato all'interno delle cabine rappresenta un possibile target per attori malevoli. Considerando che il concentratore permette la gestione da remoto dei sistemi di smartstreet questo rappresenta un Single Point of Failure, ovvero un componente dell'architettura il cui malfunzionamento può portare ad anomalie e/o alla cessazione del servizio offerto dai sistemi di smartstreet.

Nel capitolo 4 verranno analizzate le implementazioni di sistemi di sicurezza che permettano la detectionhost-based o mirrored-based di anomalie sulla rete del concentratore.
Lo scopo ultimo di questo studio è quello di implementare strumenti di sicurezza modulari che possano essere adattati sia direttamente all'interno del concentratore, sia su un sistema ad hoc predisposto sulla porta di mirroring dello switch a cui risulta connesso il concentratore.

Oltre alle considerazioni effettuate riguardanti il concentratore, è necessario evidenziare che anche le workstation di controllo remoto possono essere vittime di attacchi informatici. Considerando che queste ultime sono spesso collegate anche a reti IT corporate dove è possibile l'accesso ad internet, le workstation rappresentano a tutti gli effetti dei possibili entry points per vulnerabilità è di fondamentale importanza.

Per l'oggetto di studio di questo lavoro, possiamo definire le workstation di gestione remota dei concentratori come Side Point of Failure, in quanto una loro compromissione potrebbe causare disconnessione del canale di comunicazione diretto per la gestione del sistema ma non una possibile compromissione di funzionamento del sistema di smartstreet.

In questo lavoro verranno quindi presentati dei moduli di detection che permetteranno di aumentare la postura di sicurezza informatica per i concentratori, per le workstation e per i sistemi di smartstreet in generale.

4 Progettazione di un anomalydetectionsystem per smart service di illuminazione pubblica

In questa sezione verrà illustrata la metodologia di progettazione che si intende seguire per quanto concerne lo sviluppo di un semplice AnomalyDetectionsystem per lo scenario di Smart Street presente nello Smart Village nella sede di ENEA – Casaccia.

La progettazione di un AnomalyDetectionsystem per smart service di illuminazione pubblica proposta in questo lavoro si basa su un approccio ampiamente validato nell'ambiente delle reti industriali in [17]. Secondo questo approccio, il sistema viene considerato come un Cyber-Physical System (CPS) e le caratteristiche ibride di tale sistema vengono utilizzate per realizzare un AnomalyDetectionsystem.

Come già evidenziato, i sistemi IDS vengono utilizzati per identificare eventuali attacchi sulla rete. Nel contesto Smart Street verranno utilizzati sia gli strumenti classici, opportunamente adattati al caso di studio, sia strumenti creati appositamente per lo scenario in esame. In particolare, si farà riferimento alla creazione di profili specifici di rete per il set up considerato e strumenti di AnomalyDetection basati sul behavior.

4.1 Metodologia di AnomalyDetection per availabilityattacks

Esistono molteplici strumenti che permettono l'implementazione di soluzioni di sicurezza sulle reti. Tuttavia, le metodologie classiche di sicurezza informatica utilizzate nel mondo dell'Information and Communication Technology (ICT) non rappresentano soluzioni ideali per valutare la sicurezza delle reti di sistemi industriali.

L'esempio più evidente riguarda i classici sistemi IDS basati su signatures predefinite. Tali sistemi effettuano una verifica di sicurezza del traffico basata su regole statiche, non permettendo un'analisi dinamica del comportamento della rete e non rappresentano una effettiva soluzione per attacchi di tipo zero day. Questi ultimi sono degli attacchi che sfruttano vulnerabilità non identificate delle reti informatiche, di conseguenza non è possibile sfruttare meccanismi di sicurezza basati su regole predefinite. Gli zero day quindi rappresentano la minaccia più grande per i sistemi industriali e le infrastrutture critiche ma rappresentano allo stesso tempo una minaccia di notevole importanza anche per le implementazioni di smart service di illuminazione pubblica.

A differenza delle operazioni sulle normali reti ICT, le reti delle infrastrutture critiche, così come quelle per l'illuminazione intelligente, presentano un comportamento ripetitivo: in base ai processi che vengono effettuati, le operazioni di lettura dei sensori sul campo e di scrittura degli attuatori avvengono generalmente ad intervalli regolari e ciclicamente. Si pensi infatti al ciclo giornaliero che deve seguire il sistema di illuminazione intelligente: quest'ultimo si attiverà seguendo dei comportamenti ripetitivi e quindi di possibile profilazione.

Dal punto di vista operativo, questo rappresenta un vantaggio in termini di analisi delle anomalie sulla rete. Il motivo è che procedendo all'analisi del traffico di rete in situazioni di normalità, è possibile costruire un profilo di rete. Eseguendo quindi l'analisi del comportamento della rete Smart Street in situazioni normali, è possibile costruire un profilo di traffico di rete sul normale comportamento e successivamente sfruttarlo per il rilevamento di anomalie.

Partendo da questo principio, è stato sviluppato uno specifico IDS anomaly-based per l'analisi del comportamento della rete di comunicazione dello Smart Village nella sede di ENEA – Casaccia.

A differenza dei sistemi IDS classici che integrano l'intero sistema di identificazione in un singolo modulo, il sistema di AnomalyDetection presentato in questo lavoro prevede i seguenti componenti: Modulo di Analisi di Rete (MAR); Modulo di Estrazione Profilo (MEP); Modulo di Detection (MD).

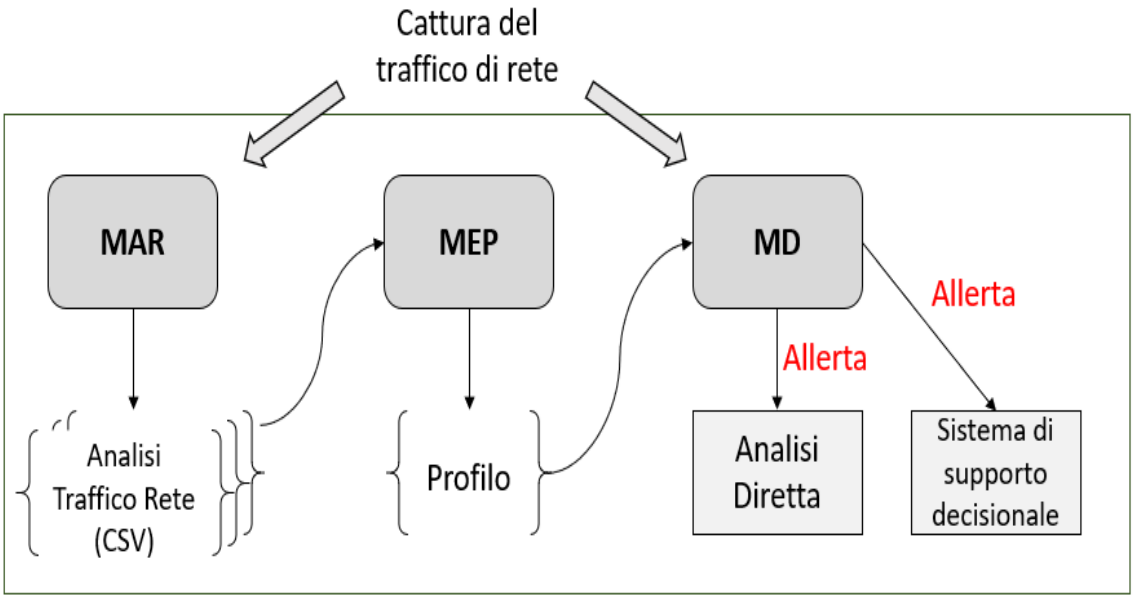

Figura 4.1 Architettura del sistema di AnomalyDetection

Lo schema dell'architettura è rappresentato in Figura 4.1ed è composta dai seguenti moduli:

- **Modulo di Analisi di Rete (MAR)**: questo componente analizza il traffico di rete e salva in un file Comma-SeparatedValues (CSV) le informazioni su tutti i pacchetti in transito sulla rete in un intervallo predefinito di analisi. La durata dell'analisi dipende dal comportamento ripetitivo del sistema. A titolo di esempio, si considerino le operazioni di accensione/spegnimento dei lampioni in un sistema di illuminazione intelligente. In base agli orari di luce solare, tali operazioni si ripetono giornalmente, quindi sarà necessario salvare il comportamento di rete di 24 ore. Nel caso in cui venisse identificato un comportamento di monitoraggio e gestione che si ripete durante una settimana, sarà necessario salvare il traffico di rete di una settimana per poter valutare il comportamento normale. Il periodo di training identificato per generare il profilo di normalità può essere modificato a piacimento effettuando una nuova acquisizione di traffico di rete del sistema in analisi.

- **Modulo di Estrazione Profilo (MEP)**: questo componente sfrutta le informazioni sul traffico di rete salvato dal Modulo di Analisi di Rete per generare un profilo sul comportamento normale della rete. Il modo in cui viene generato il profilo rappresenta l'aspetto fondamentale dell'AnomalyDetection. Più sarà accurato il modello, più sarà possibile identificare le anomalie di sistema presenti sul traffico di rete. A differenza di strumenti di AnomalyDetection presenti in letteratura, il punto di forza che caratterizza il Modulo di Estrazione Profilo è rappresentato dalla elevata possibilità di configurazione. Quest'ultima caratteristica permette di adattare facilmente il sistema proposto a qualsiasi sistema di rete per l'analisi delle anomalie.

- **Modulo di Detection (MD)**: questo componente dell'architettura di detection rappresenta il sistema di allarme capace di verificare la presenza di azioni malevoli sul traffico di rete. Il Modulo di Estrazione Profilo completa la creazione del profilo di rete, permettendo successivamente di far utilizzare tale profilo di normalità per l'operazione attiva di AnomalyDetection. Il Modulo di Detection quindi analizza attivamente il traffico e lo confronta ad intervalli regolari con il set di parametri generati dal Modulo di Estrazione Profilo.

Concretamente, per il caso di studio implementato, il Modulo di Detection genera un'allerta quando:

$$\chi(i) > \chi^*(i) + \delta(i)$$

Dove$\chi(i)$: rappresenta il valore dell'i-esimo parametro considerato per l'AnomalyDetection ricavato dall'analisi attuale del traffico di rete, $\chi^*(i)$ rappresenta il valore dell'i-esimo parametro considerato presente nel file del profilo di comportamento normale di rete, mentre $\delta(i)$ rappresenta un valore di incertezza scelto in maniera accurata da poter generare il minor rate possibile di detection false.

L'aspetto di modularità del sistema di AnomalyDetection presentato permette di modificare agilmente algoritmi e tecniche di analisi utilizzati all'interno dei componenti dell'architettura di sicurezza. Ad esempio, si potrebbero implementare tecniche di Machine Learning o tecniche statistiche più avanzate per l'analisi dei dati sia per il Modulo di Estrazione profilo, sia per lo stesso Modulo di Detection.

Le allerte generate vengono inviate sia direttamente all'analista di sicurezza per una valutazione dello stato di sicurezza della rete, sia ad un sistema di supporto decisionale che verrà presentato in sezione 4.3.

4.2 Risultati e valutazione preliminare implementazione AnomalyDetectionsystem

In questa sezione verrà discusso un case study di scenario di smartstreet riconducibile allo Smart Village nella sede di ENEA – Casaccia. Per l'emulazione degli attacchi informatici in ambiente sicuro verrà utilizzato il testbed di smartstreet configurato presso l'Università degli Studi Roma Tre e verrà introdotto l'utilizzo del sistema di AnomalyDetection per l'analisi delle anomalie presenti in questa rete emulata. Infine verranno valutati i risultati della fase di AnomalyDetection attiva in presenza di varie tipologie di attacco alla disponibilità delle risorse di rete (availabilityattacks).

La topologia di rete con la presenza dell'attaccante è rappresentata in Figura 4.2.

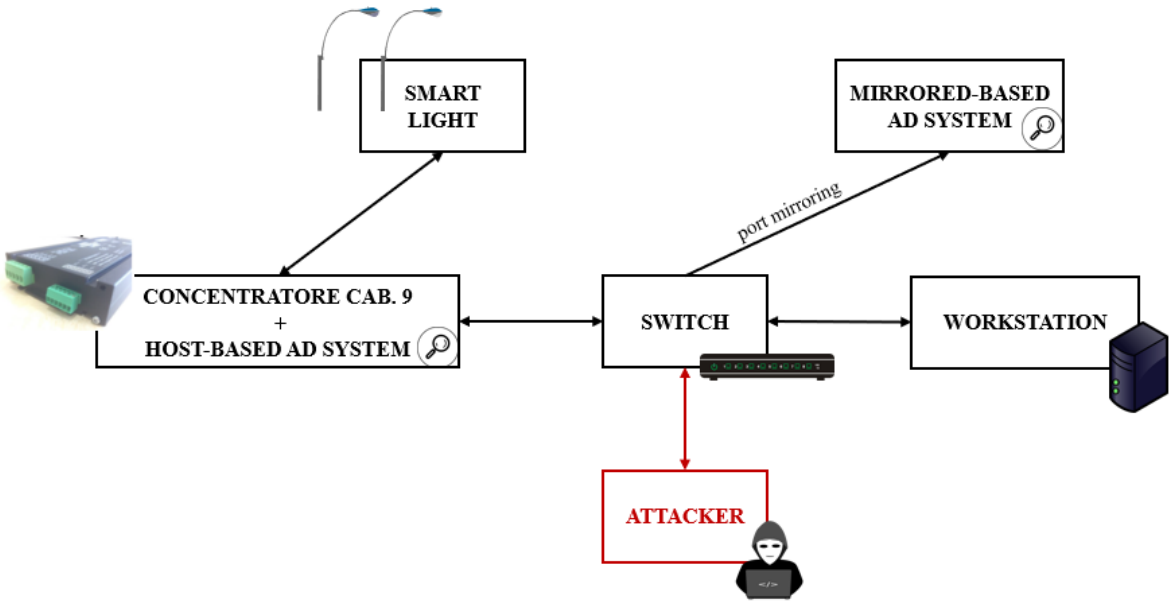

Figura 4.2 Topologia della rete

Tale topologia è caratterizzata da uno switchlegacy, un attaccante, la simulazione del concentratore di Cabina 9 al quale sono connessi via PowerLineCommunication i sistemi di Smart Light e la workstation dalla quale è possibile, tramite interfaccia web, modificare la configurazione del concentratore. Si assume che i link di connessione tra i vari nodi descritti non presentano problematiche fisiche.

Grazie alle caratteristiche di modularità del sistema di AnomalyDetection concepito, quest'ultimo può essere implementato sia come host-based direttamente all'interno del concentratore, sia come mirrored-based su un sistema dedicato per scopi di intrusiondetectionsystem.

Per quanto riguarda le comunicazioni di rete di questi esperimenti, si assume che le operazioni riguardino il monitoraggio di normali operazioni di supervisione e/o modifica delle impostazioni dei sistemi di Smart Light attraverso il concentratore.

Come già detto precedentemente, i moduli del sistema di AnomalyDetection devono essere configurati considerando lo specifico sistema in esame. Per questi esperimenti, visto che si è scelto di riprodurre uno scenario di supervisione e/o modifica delle impostazioni sul concentratore attraverso la web interface, il tempo di analisi impostato per il Modulo di Analisi di Rete è stato scelto pari a t = 60s. Di conseguenza, il Modulo di Analisi di Reteanalizza il traffico di rete e salva i dati di interesse in un file CSV per permettere al Modulo di Estrazione Profilo di generare il profilo di rete in situazione di normalità. Il tempo di analisi è stato selezionato in questo modo per finalità di test di laboratorio.

La configurazione del Modulo di Estrazione Profilo è la parte più delicata dell'implementazione: i parametri da utilizzare per la creazione del profilo devono essere scelti con molta attenzione. Per questo esperimento, sono stati scelti i seguenti parametri: *PacketTimestamp, Total Packets*. Successivamente, è stato scelto di creare un riferimento sul comportamento normale della rete per ogni secondo di analisi del traffico. In questo modo sono state generate n=60 entry per il file di profilo del traffico di rete con le informazioni sui parametri descritti precedentemente.

Una volta completata la generazione del file di profilo, il Modulo di Detection viene attivato: viene analizzato attivamente ogni secondo di traffico di rete e le statistiche riguardanti i parametri presi in considerazione vengono confrontati con quelli del profilo generato dal Modulo di Estrazione Profilo.

Al fine di valutare il comportamento sperimentale del sistema di AnomalyDetection sviluppato, sono stati effettuati attacchi cyber sulla rete in modo tale da verificare l'effettivo funzionamento del sistema di sicurezza (si vedaTabella 4.1). Si assuma che l'attaccante sia riuscito ad avere accesso alla rete e sia connesso come una normale workstation su di essa. Tutti i test effettuati hanno una durata approssimativa di un minuto.

#	Metodologia attacco	Obiettivo attacco
1	*DoSfloodingattack* con singolo nodo malevolo	Concentratore
2	*DoSfloodingattack* con singolo nodo malevolo	Workstation
3	*DoS*tramite*Random Packet Drop*	Concentratore
4	*DoS*tramite*Random Packet Drop*	Workstation
5	*DoS*tramite*Time Packet Drop*	Concentratore
6	*DoS*tramite*Time Packet Drop*	Workstation

Tabella 4.1Attacchi informatici per sperimentazione sistema AnomalyDetection.

Negli esperimenti condotti e descritti nel documento [1], gli attacchi DoSflooding effettuati sono caratterizzati da un invio di SYN packets ogni microsecondo. Tale tipologia di attacco comportava un decadimento delle prestazioni di rete tale da provocare l'impossibilità di interagire con i nodi di rete sotto attacco.

In questo lavoro sono stati effettuati attacchi DoSflooding utilizzando invio di pacchetti SYN ogni 1000 microsecondi che, pur rappresentando una notevole frequenza di invio, non comporta decadimento delle prestazioni tale da comportare disconnessioni o impossibilità di utilizzo dei nodi di rete, in questo caso l'interfaccia web based del concentratore.

Il motivo di ridurre il tempo di invio pacchetti di flooding è giustificato dal fatto che si sono identificate condizioni per le quali il sistema, pur essendo sotto attacco, continua a funzionare normalmente. Questo evidenzia che in assenza di uno strumento di detection basato sulle anomalie del comportamento, come quello sviluppato ad hoc per il sistema smartstreet e descritto in questa sezione, non sarebbe stato possibile effettuare detection dell'attacco informatico che veniva effettuato anche se senza conseguenze.

In Figura 2.1è rappresentato il traffico della rete di smartstreet emulata in condizioni di normalità. Tale condizione di normalità viene rappresentata per gli scopi di questo lavoro in un minuto di analisi di traffico della rete del testbed utilizzando il sistema di AnomalyDetection.

Più precisamente, la linea blu rappresenta il plot del traffico di rete con numero di pacchetti al secondo in situazioni di normalità, ovvero durante questo periodo non sono presenti attacchi informatici verso i nodi di rete connessi.

Il caso di test prende in considerazione l'analisi di traffico tra due nodi di rete legittimi, una workstation ed il concentratore PLC. La situazione di normalità permette di creare il profilo di rete grazie al Modulo di Analisi di Rete e al Modulo di Estrazione Profilo.

Al fine di poter sfruttare nel miglior modo possibile l'AnomalyDetection, è necessario individuare un comportamento ripetitivo delle azioni svolte dal sistema. Come già evidenziato, l'avere come riferimento una rete di smartstreet si dimostra un vantaggio perché considerando le operazioni da svolgere, è possibile identificare un pattern ripetitivo, con il fattore tempo da valutare attentamente.

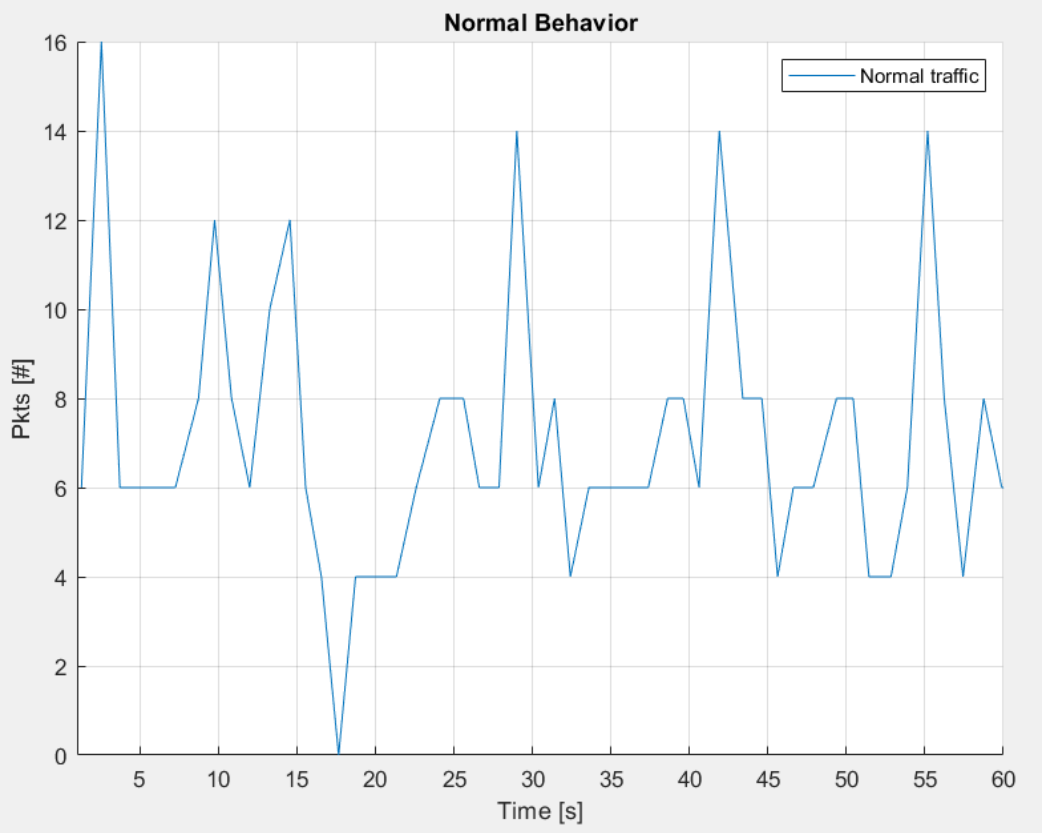

Figura 4.3 Comportamento nominale del sistema

In Tabella 4.2sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet.

Identificativo	Indirizzo IP
Concentratore	193.204.161.87
Workstation	193.204.161.102

Tabella 4.2 Indirizzi IP dei nodi implementati sul testebd di smartstreet

4.2.1 Attacchi informatici alla disponibilità delle risorse

Come descritto nel documento [1], gli attacchi informatici alla disponibilità delle risorse di un sistema hanno come obiettivo quello di rendere problematico o non possibile l'utilizzo di un servizio informatico da parte di un generico utente interessato.
Gli attacchi conosciuti come Denial-of-Service (DoS), rappresentano l'esempio più importante di minaccia alla disponibilità delle risorse si verificano 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. E' per questo motivo che in questo lavoro sono stati sviluppati dei meccanismi modulari di detection pensati per questa tipologia di minaccia.
Al fine di testare i sistemi di detection, sono stati effettuati dei test di attacco informatico utilizzando SYN Flooding. Il SYN Flooding è un attacco di tipo DoS che sfrutta il meccanismo di three way handshake del protocollo TCP per generare problemi alla disponibilità delle risorse di rete.

Gli attacchi DoS tramite tecnica SYN Flooding che si è scelto di implementare sono diversi da quelli presenti in [1],in quanto non sono in grado di provocare una degradazione grave delle comunicazioni di rete tale da generare disservizio.
Questo avviene perché i pacchetti vengono inviati ogni 1000 microsecondi, tempo che si è rivelato essere più gestibile dai sistemi di rete rispetto al SYN Flooding effettuato con invio pacchetti ogni microsecondo.

La scelta di implementare degli attacchi che non provochino impatto grave e conseguenze sui sistemi è giustificata dal fatto che si vuole dimostrare l'efficacia degli strumenti di detection sviluppati proprio in situazioni dove non si ha una evidenza dell'attacco.

4.2.2 DoSfloodingattack con singolo nodo malevolo (vittima concentratore)

- **Descrizione attacco**: SYN Flooding utilizzando un singolo nodo malevolo, vittima il concentratore. 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 1000 microsecondi.

- **Descrizione risultati detection**: InFigura 4.4è possibile osservare i risultati del sistema di AnomalyDetection implementato. Essendo il numero di pacchetti al secondo molto alto durante il periodo di attacco (> 2500 pkts/s), non è possibile graficare il modello creato dal Modulo di Estrazione Profilo. Tuttavia è evidenziato il funzionamento del Modulo di Detection che evidenzia delle allerte ogni secondo che il sistema si trova sotto attacco. Nello specifico, vengono inviati all'operatore di sicurezza allerte nella finestra temporale che va da 22s a 33s.

In Tabella 4.3sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

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

Tabella 4.3Indirizzi IP dei nodi implementati sul testebd di smartstreet

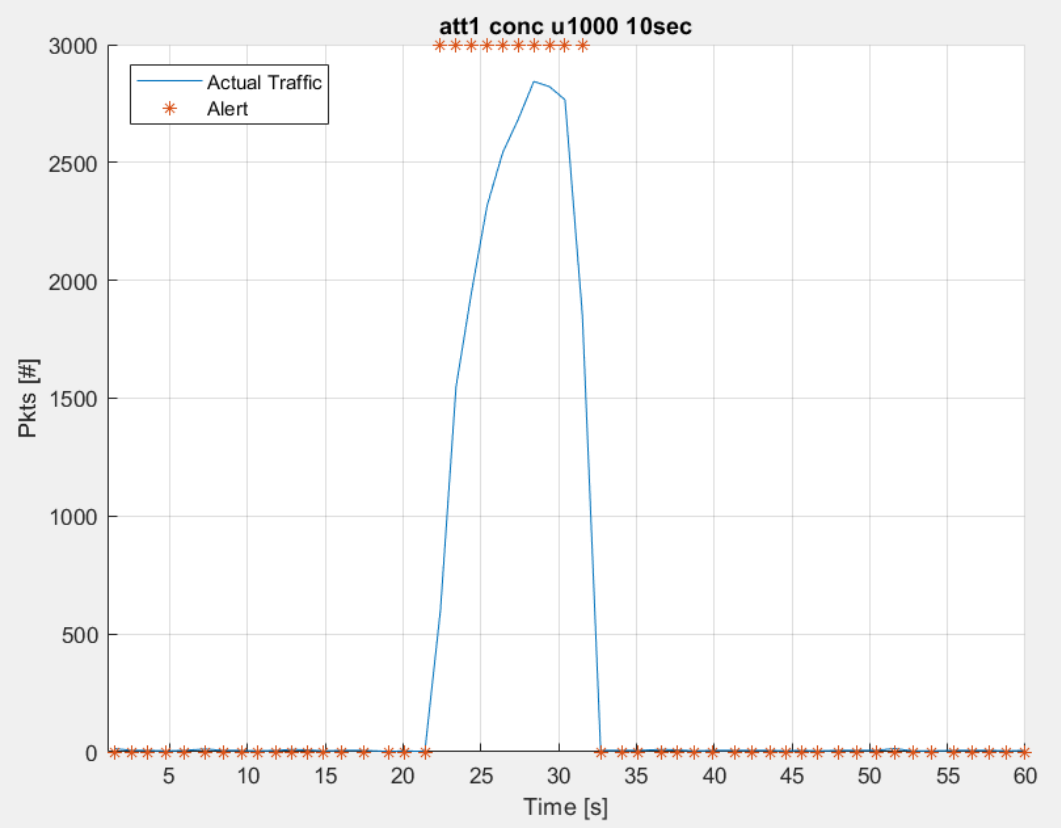

Figura 4.4 Risultati AnomalyDetection

4.2.3 DoSfloodingattack con singolo nodo malevolo (vittima workstation)

- **Descrizione attacco**: SYN Flooding utilizzando un singolo nodo malevolo, vittima il concentratore. 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 1000 microsecondi.

- **Descrizione risultati detection**: In Fig. 4.5 sotto è possibile osservare i risultati del sistema di AnomalyDetection implementato. Essendo il numero di pacchetti al secondo molto alto durante il periodo di attacco (> 2500 pkts/s), non è possibile graficare il modello creato dal Modulo di Estrazione Profilo. Tuttavia è evidenziato il funzionamento del Modulo di Detection che evidenzia delle allerte ogni secondo che il sistema si trova sotto attacco. Nello specifico, vengono inviati all'operatore di sicurezza allerte nella finestra temporale che va da 22s a 33s.

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

Tabella 4.4Indirizzi IP dei nodi implementati sul testebd di smartstreet

In tabella sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

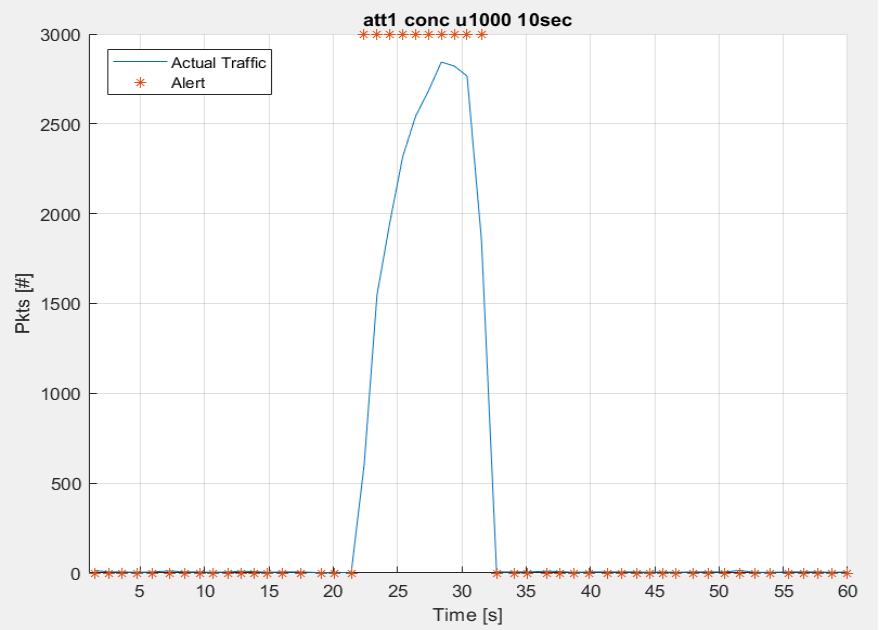

Figura 4.5Risultati AnomalyDetection

4.2.4 DoSfloodingattack con singolo nodo malevolo (vittima workstation)

- **Descrizione attacco**: SYN Flooding utilizzando un singolo nodo malevolo, vittima la workstation. 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 1000 microsecondi.

- **Descrizione risultati detection**: In Figura 4.6è possibile osservare i risultati del sistema di AnomalyDetection implementato. Anche in questo caso come il precedente, essendo il numero di pacchetti al secondo molto alto durante il periodo di attacco (> 1000 pkts/s), non è possibile graficare il modello creato dal Modulo di Estrazione Profilo. Tuttavia è evidenziato il funzionamento del Modulo di Detection che evidenzia delle allerte ogni secondo che il sistema si trova sotto attacco. Nello specifico, vengono inviati all'operatore di sicurezza allerte nella finestra temporale che va da 22s a 33s.

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

Tabella 4.5Indirizzi IP dei nodi implementati sul testebd di smartstreet

In Tabella 4.5sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

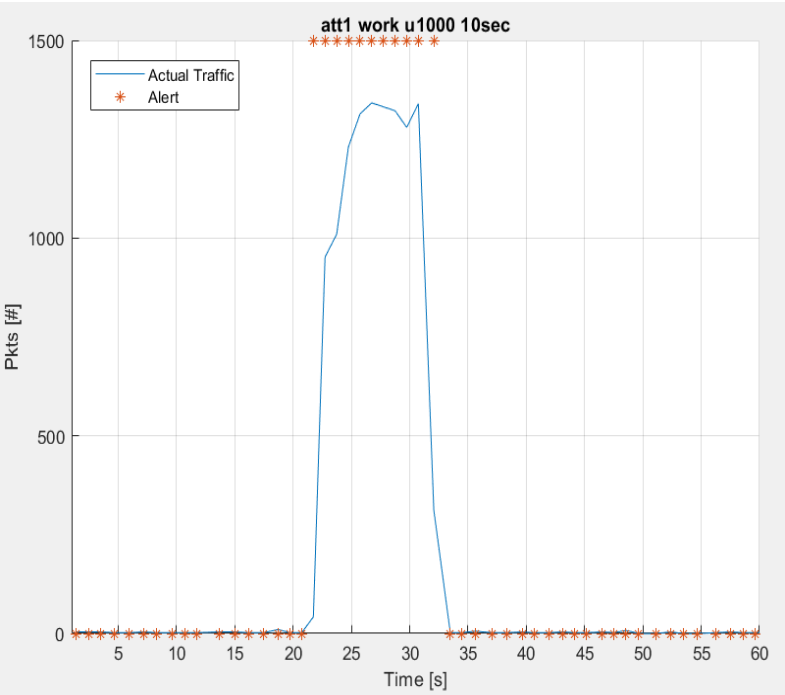

Figura 4.6 Risultati AnomalyDetection

4.2.5 DoS tramite Random PacketDrop (vittima concentratore)

- **Descrizione attacco**: 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 PacketDrop, 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 attacco la vittima del drop è il concentratore. L'attacco ha una durata di circa 30s.

- **Descrizione risultati detection**: al fine di poter gestire problematiche relative ad attacchi di tipo MITM che sfruttano l'*ARP Poisoning*, attraverso l'utilizzo del Modulo di Analisi di Rete e del Modulo di Estrazione Profilo, è stato generato il profilo di normalità dei pacchetti relativi al protocollo ARP presenti in rete in situazione di normalità (Tabella 4.7).
- In Tabella 4.8è possibile identificare il confronto tra il profilo di rete normale con δ= 3 e il traffico di rete attuale dove è presente l'attacco. Durante la finestra di attacco si verifica un aumento anomalo dei pacchetti ARP sulla rete che viene prontamente individuato dal sistema di AnomalyDetection implementato e nello specifico dal Modulo di Detection. Vengono quindi generate delle allerte nella finestra temporale che va dai 22s ai 49s.

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

Tabella 4.6Indirizzi IP dei nodi implementati sul testebd di smartstreet

In Tabella 4.6 sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

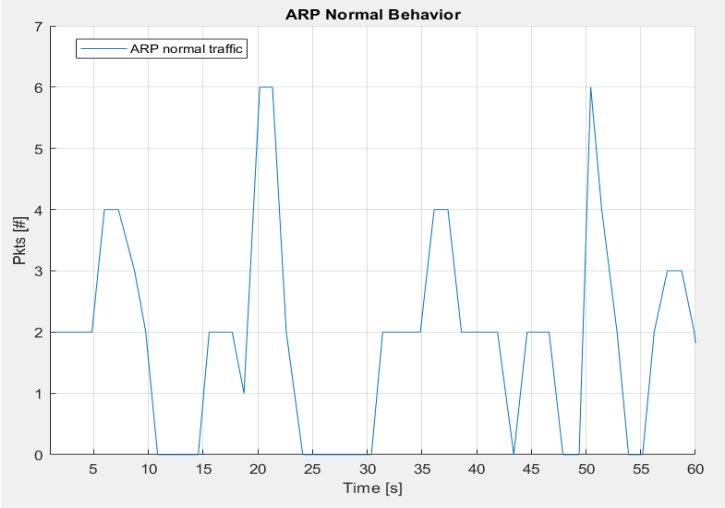

Figura 4.7Profilo nominale ARP

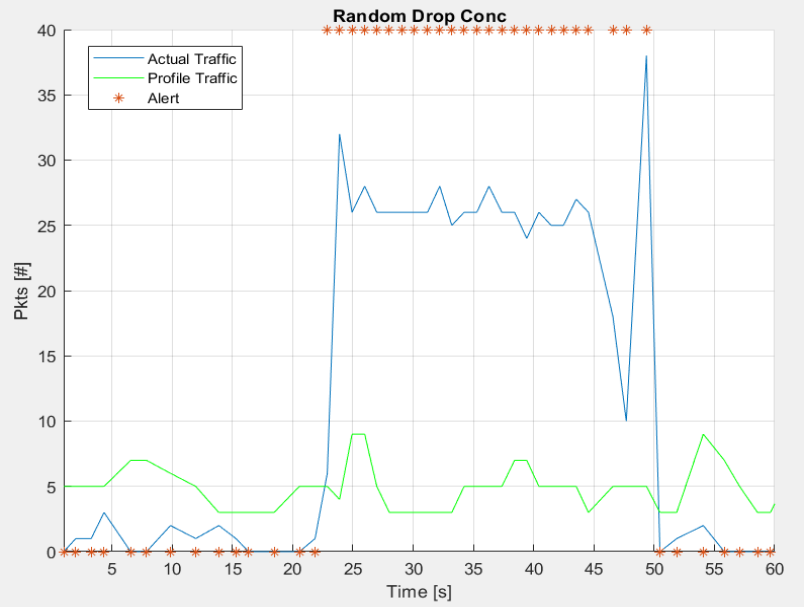

Figura 4.8Risultati AnomalyDetection

4.2.6 DoStramite Random Packet Drop (vittima workstation)

- **Descrizione attacco**: 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 PacketDrop, 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 attacco la vittima del drop è la workstation. L'attacco ha una durata di circa 30s.

- **Descrizione risultati detection**: come per l'esperimento precedente, anche in questo caso è stato utilizzato il profilo di normalità dei pacchetti relativi al protocollo ARP presenti in rete in situazione di normalità (Figura 4.7).
  In Figura 4.9è possibile identificare il confronto tra il profilo di rete normale con δ= 3 e il traffico di rete attuale dove è presente l'attacco. Durante la finestra di attacco si verifica un aumento anomalo dei pacchetti ARP sulla rete che viene prontamente individuato dal sistema di AnomalyDetection implementato e nello specifico dal Modulo di Detection. Vengono quindi generate delle allerte nella finestra temporale che va dai 22s ai 55s con la presenza di un outlier al t=56s.

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

Tabella 4.7Indirizzi IP dei nodi implementati sul testebd di smartstreet

In Tabella 4.7sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

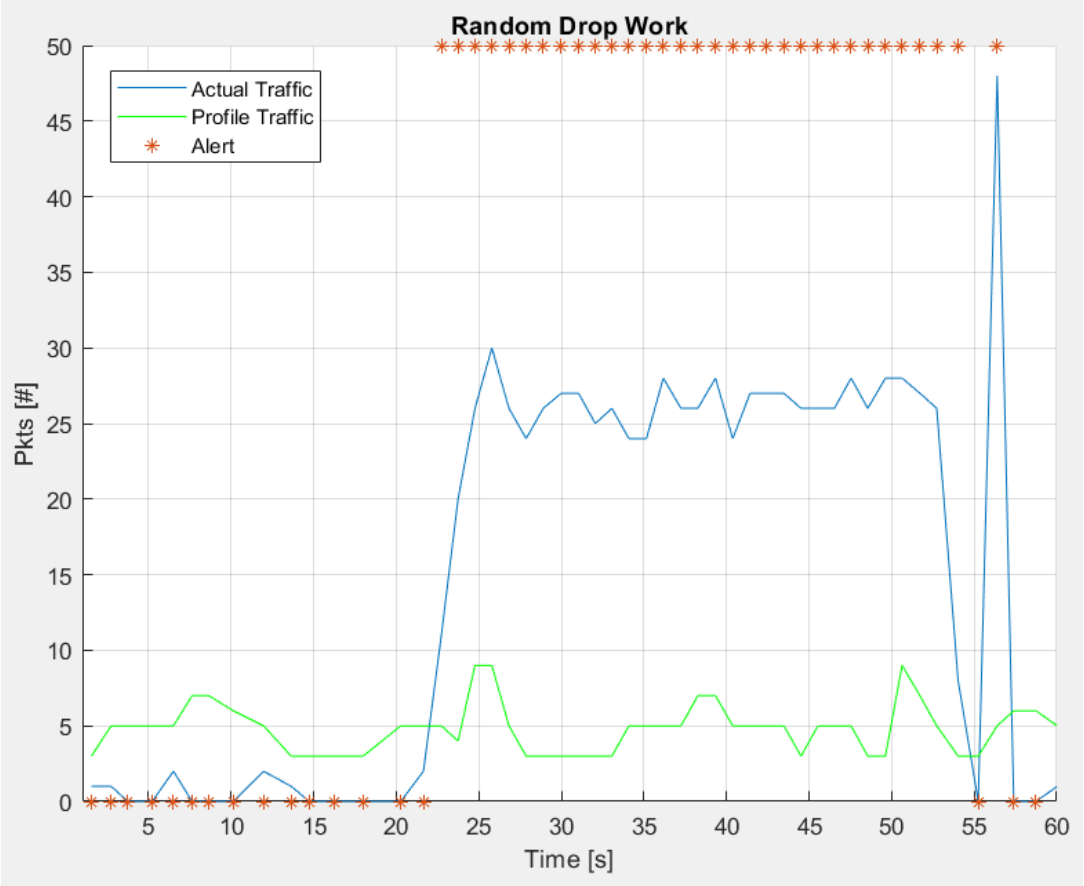

Figura 4.9Risultati AnomalyDetection

4.2.7 DoS tramite Time PacketDrop (vittima concentratore)

- **Descrizione attacco**: in questo test il nodo malevolo effettua un attacco di tipo Man In The Middle (MITM) utilizzando la tecnica ARP Poisoning. 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'attacco ha una durata di circa 40s.

- **Descrizione risultati detection**: come per l'esperimento precedente, anche in questo caso è stato utilizzato il profilo di normalità dei pacchetti relativi al protocollo ARP presenti in rete in situazione di normalità (Figura 4.7).
  In Figura 4.10è possibile identificare il confronto tra il profilo di rete normale con δ= 3 e il traffico di rete attuale dove è presente l'attacco. Durante la finestra di attacco si verifica un aumento anomalo dei pacchetti ARP sulla rete che viene prontamente individuato dalsistema di AnomalyDetection implementato e nello specifico dal Modulo di Detection. Vengono quindi generate delle allerte nella finestra temporale che va dai 22s ai 60s.

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

Tabella 4.8Indirizzi IP dei nodi implementati sul testebd di smartstreet

In Tabella 4.8 sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

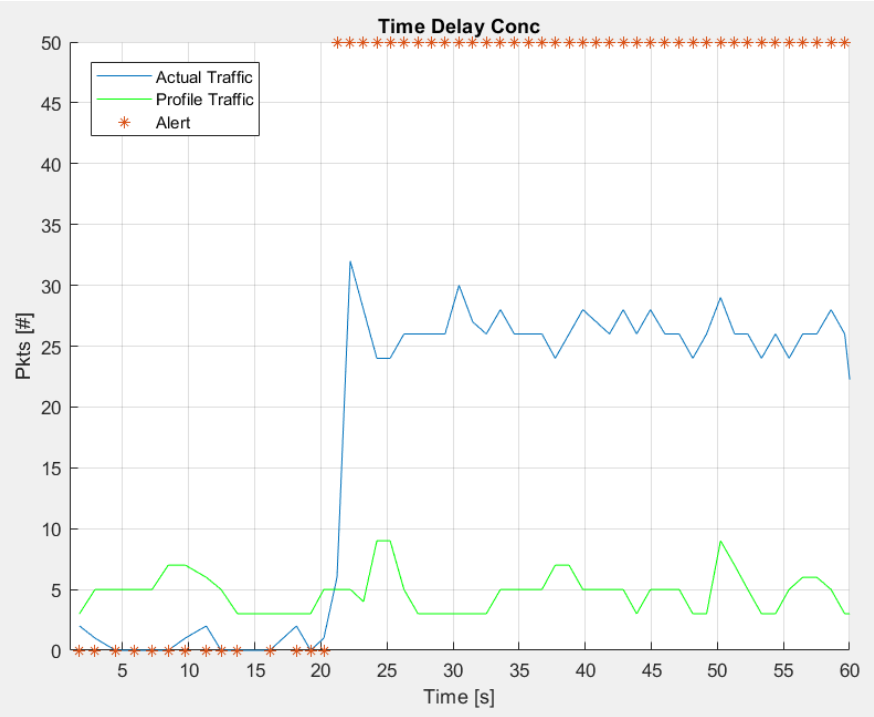

Figura 4.10Risultati AnomalyDetection

4.2.8 DoStramite Time Packet Drop (vittima workstation)

- **Descrizione attacco**: in questo test il nodo malevolo effettua un attacco di tipo Man In The Middle (MITM) utilizzando la tecnica ARP Poisoning. 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'attacco ha una durata di circa 40s.

- **Descrizione risultati detection**: come per l'esperimento precedente, anche in questo caso è stato utilizzato il profilo di normalità dei pacchetti relativi al protocollo ARP presenti in rete in situazione di normalità (Figura 4.7).
  In Figura 4.11è possibile identificare il confronto tra il profilo di rete normale con δ= 3 e il traffico di rete attuale dove è presente l'attacco. Durante la finestra di attacco si verifica un aumento anomalo dei pacchetti ARP sulla rete che viene prontamente individuato dal sistema di Anomaly Detection implementato e nello specifico dal Modulo di Detection. Vengono quindi generate delle allerte nella finestra temporale che va dai 24s ai 60s.

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

Tabella 4.9Indirizzi IP dei nodi implementati sul testebd di smartstreet

In Tabella 4.9 sono presenti gli indirizzi IP dei nodi implementati sul testbed di smartstreet per l'analisi dei risultati di detection in situazione di attacco alla disponibilità delle risorse. In grassetto è evidenziata la vittima dell'esperimento in esame.

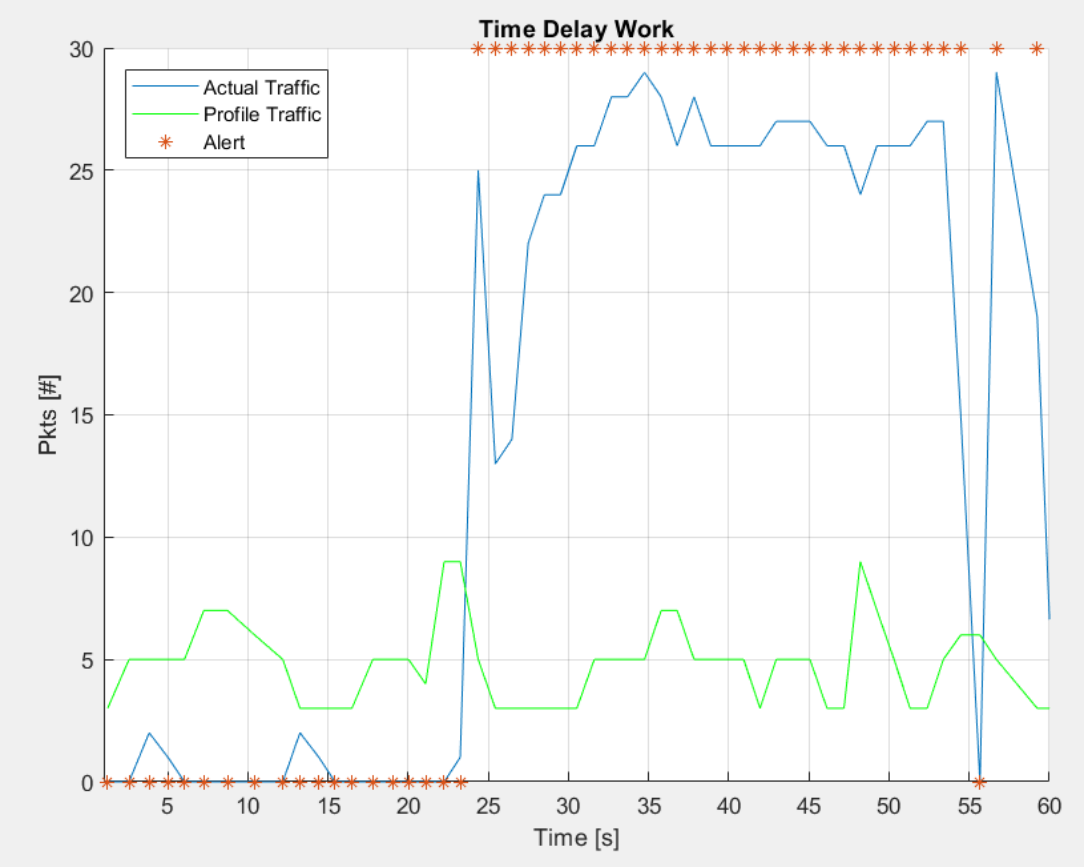

Figura 4.11Risultati AnomalyDetection

4.3 Supporto Decisionale per l'operatore

Durante la fase di analisi della sicurezza, grande importanza è data all'identificazione delle minacce. Allo stesso tempo viene data uguale importanza alle possibili contromisure da implementare in caso di problematiche sui sistemi.

In questo contesto, la rilevanza della figura dell'operatore della sicurezza, ovvero chi deve prendere decisioni in base alle situazioni di pericolo che si verificano all'interno del sistema, viene sottostimata. Nei lavori futuri verrà presentato un nuovo approccio finalizzato a supportare l'operatore di sicurezza informatica di un contesto di cyber-physical security associato allo scenario Smart Street.

Sulla base del lavoro effettuato in [17], verranno implementati dei meccanismi nel processo decisionale che permetteranno di supportare l'operatore nella scelta delle possibili alternative da attuare come contromisura ad un attacco. A tal fine, una fusione innovativa tra i classici approcci di supporto alle decisioni e il sistema di detection presentato in questo lavoro verrà condotto utilizzando l'AnalyticHierarchyProcess (AHP).

5 Conclusioni

Partendo dai sistemi di detection sviluppati, sarà possibile in futuro implementare l'analisi relativa al livello fisico del processo. L'idea principale è quella di creare un modello virtuale di alcune parti del sistema fisico. Questo modello virtuale verrà alimentato con gli stessi input del sistema fisico ed i suoi output verranno comparati con quelli reali per identificare eventuali anomalie. Alcuni attacchi informatici, infatti, sono volti ad indurre malfunzionamenti nei sistemi fisici in modo da provocare disastri. In questo modo, si potrà prevenire anche questa tipologia di attacchi.

La versatilità di questo strumento di AnomalyDetection rappresenta il punto forte dello sviluppo...
Si è evidenziato che anche in mancanza di evidenti problematiche causate dall'attacco alla disponibilità delle risorse di rete, il sistema di AnomalyDetection ha permesso di identificare anomalie e di allertare l'operatore di sicurezza della situazione di pericolo che era in procinto di generarsi.

Inoltre, gli strumenti di simulazione presentati permettono di fare ricerca e sviluppo su scenari di infrastruttura critica simulati consentendo un'accurata valutazione delle implementazioni prima di utilizzi in reali scenari dove la criticità degli scenari potrebbe generare problemi

In lavori futuri sarà possibile prevedere l'implementazione di meccaniscmi più avanzati di virtualizzazione del modello fisico per introdurre tecniche di sicurezza innovative nel contesto degli smart service di illuminazione e compatibili con le tecnologie presentate in questo lavoro.

6 Riferimenti bibliografici

1. Giuseppe Bernieri, Federica Pascucci, “Telecontrollo digitale Smart Street: riproduzione di situazione di degradamento prestazioni ed analisi dei ritardi di servizio e studio dei servizi aggiuntivi”, Report Par2016, ENEA,2017.
2. Song Han, Miao Xie, Hsiao-Hwa Chen, Yun Ling, “Intrusion Detection in Cyber-Physical Systems:Techniques and Challenges”, IEEE Systems Journal, vol.8, no. 4, 2014.
3. J. P. Anderson, Computer Security Threat Monitoring and Surveillance. Fort Washington, PA, USA: James P. Anderson Company, Apr. 1980.
4. S. Han, E. Chang, L. Gao, and T. Dillon, “Taxonomy of attacks on wireless sensor networks,” in Proc. 1st Eur. Conf. Comput. Netw. Defence, 2005, pp. 97–105.
5. A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “A secure control framework for resource-limited adversaries,” Automatica, vol. 51, pp. 135 – 148, 2015.
6. C.-C. Liu, “Cybersecurity for critical infrastructures: Attack and defense modeling,” IEEE Trans. Syst., Man, Cybern. A, Syst., Humans, vol. 40, no. 4, pp. 853–865, Jul. 2010.
7. N. Mahmood, C. Leckie, J. Hu, Z. Tari and M. Atiquzzaman, Network Traffic Analysis and SCADA Security, Springer Berlin Heidelberg, 2010, pp. 383-405.
8. Baskar Zimmermann, OSI Reference Model—The ISO Model of Architecture for Open Systems Interconnection, in IEEE Transactions on Communications, vol. 28, nº 4, aprile 1980, pp. 425–432, DOI:10.1109/TCOM.1980.1094702.
9. D. R. a. E. Sottile, “Sherlock: A framework for P2P traffic analyis,” in IEEE Ninth International Conference on Peer-to-Peer Computing, Seattle, WA, 2009.
10. Cisco Systems, “RFC 5153:IP Flow Information Export (IPFIX) Implementation Guidelines,”IETF, 2008.
11. L. HUAWEI TECHNOLOGIES CO., “NetStream (Integrated) Technology White paper,” 06 09 2012. [Online]. Available: http://enterprise.huawei.com/ilink/enenterprise/download/HW_201022
12. https://www.juniper.net/us/en/local/pdf/app-notes/3500204-en.pdf
13. https://snort.org
14. M. Roesch, “SNORT - Lightweight Intrusion Detection for Networks,” in Proceedings of LISA '99: 13th System Administration Conference, Seattle, Washington, USA, 1999.
15. “The Bro Network Security Monitor,” [Online]. Available: https://www.bro.org/
16. https://suricata-ids.org
17. “The Bro Network Security Monitor,” [Online]. Available: https://www.bro.org/
18. “Application Layer Packet Classifier for Linux,” 7 01 2009. [Online]. Available: http://l7-filter.sourceforge.net/
19. https://www.ntop.org/products/deep-packet-inspection/ndpi/
20. C. Köhnen, C. Überall, F. Adamsky, V. Rakocevic, M. Rajarajan and R. Jäger, “Enhancements to Statistical Protocol IDentification (SPID) for Self-Organised QoS in LANs,” in International Conference on Computer Communications and Networks (ICCCN), Zürich, 2010.
21. D. I. Urbina, J. A. Giraldo, A. A. Cárdenas, N. O. Tippenhauer, J. Valente, M. Faisal, J. Ruths, R. Candell, and H. Sandberg, “Limiting the impact of stealthy attacks on industrial control systems,” in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, ser. CCS ’16. New York, NY, USA: ACM, 2016, pp. 1092–1105.
22. Bernieri, Giuseppe, et al. "Monitoring system reaction in cyber-physical testbed under cyber-attacks." Computers & Electrical Engineering 59 (2017): 86-98

Curriculum scientifico Prof.ssa. F.Pascucci.

PASCUCCI Federica
Indirizzo/i via della Vasca Navale 79, 00146, Roma (RM), Italy
Telefono/i +39 06 5733 3227
Fax +39 06 573030
Email pascucci@dia.uniroma3.it
Nazionalità Italiana
Data di nascita 8 ottobre 1975
Sesso F

Posizione attuale
Date Ottobre 2006 – Funzione Ricercatore Universitario
Istituzione Facoltà di Ingegneria, Università degli Studi Roma Tre

Esperienza professionale
Date 2005 – 2006 Funzione o posto occupato Ricercatore Universitario a tempo determinato
Dipartimento di Informatica e Automazione, Università degli Studi Roma Tre
Date 2004 –2005 Funzione o posto occupato *Innovation Promoter*
Dipartimento di Informatica e Automazione, Università degli Studi Roma Tre
Date 2004 Funzione o posto occupato Consulente Dipartimento di Informatica e Automazione, Università degli Studi Roma Tre
Date 2003 Funzione o posto occupato *Guest Researcher* AASS Institutionen för Teknik, Örebro Universitet
Date 2000 – 2003 Dottoranda

Esperienza didattica
Date 2007 – Funzione o posto occupato Professore a Contratto Facoltà di Ingegneria, Università degli Studi Roma Tre
Date 2003 – Funzione o posto occupato Docente di Master Dipartimento di Informatica e Automazione, Università degli Studi Roma Tre
Date 2003 – 2007 Funzione o posto occupato Tutor Università Campus Bio-Medico
Tipo o settore d'attività Docente di supporto nei corsi di *Fondamenti di Automatica e Modelli di sistemi fisiologici*
Date 2003 – 2005
Funzione o posto occupato Docente Università Campus Bio-Medico
Tipo o settore d'attività Docente del *Corso di introduzione al MatLab*
Date 2001 – 2003
Funzione o posto occupato Docente CNR – Stato Maggiore Difesa, Direzione Corsi Opto–Elettronica
Date 2000 – 2007
Funzione o posto occupato Docente CNR – Stato Maggiore Difesa, Direzione Corsi Opto–Elettronica
Date 2000 –2003 Funzione o posto occupato Docente di supporto Facoltà di Ingegneria, Università degli Studi Roma Tre

Istruzione e formazione
Date 2000 – 2004 Diploma ottenuto Dottorato di ricerca Università degli Studi di Roma La Sapienza
Date Set. 2001 Certificato o diploma ottenuto Compimento Medio di Pianoforte (VIII anno)
Conservatorio di Latina O. Respighi
Date Nov. 2000 Certificato ottenuto Abilitazione alla professione di *Ingegnere*
Date 1994 – 2000 Diploma ottenuto Laurea Università degli Studi Roma Tre 110/110 *cum laude*
Date 1989 – 1994 Certificato o diploma ottenuto Maturità Classica Istituto Massimiliano Massimo 60/60

Capacità e competenze professionali
Madrelingua/e **Italiano** Altra/e lingua/e **Inglese C1 avanzato**

Curriculum scientifico Ing. G.Bernieri

Ing. Giusebbe Bernieri, PhD
lavora come Postdoctoral Researcher presso l'Università degli Studi di Padova. Ha completato il Dottorato in Informatica e Automazione presso il Dipartimento di Ingegneria dell'Università degli Studi Roma Tre.
I suoi interessi di ricerca riguardano la sicurezza informatica applicata ai contesti di Cyber-Physical Systems, Industrial Control Systems, Critical Infrastructures.
Lavora allo sviluppo ed implementazione di soluzioni innovative per il rilevamento di minacce Cyber-Physical.
Ha lavorato come Cyber Security Consultant presso Deloitte, avvicinandosi ai bisogni concreti dello scenario industriale nel campo della sicurezza informatica.
Collabora attivamente con il "Network, Information and Computer Security (NICS) Lab" of Malaga (Spain), con il "Network Security Lab" presso University of Washington, con il "CISPA Helmholtz Center for Information Security" e con "iTrust Research Centre" presso Singapore University of Technology and Design (SUTD).