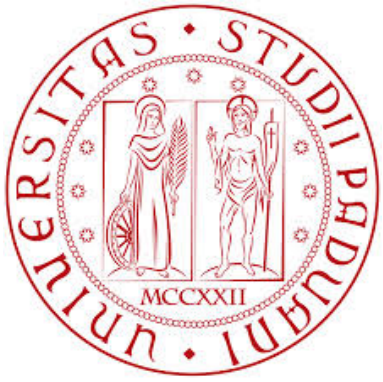
Università degli studi di Padova

Dipartimento di ingegneria dell'informazione



Corso di laurea in Ingegneria Informatica

Visibilità del traffico di altri utenti nelle reti a pacchetto GPRS: analisi quantitativa e classificazione.

Laureando: *Giorgio Zambon*
Matricola: *611511*

Relatore: *Chia.mo Prof. Ing. Nicola Zingirian*

Anno Accademico 2012/2013

Ringraziamenti

Ringrazio innanzitutto il relatore Prof. Ing. Nicola Zingirian per avermi dato la possibilità di condurre e portare a termine quest'esperienza formativa fornendomi strumentazioni e spunti nel momento del bisogno.
Un ringraziamento speciale va ai miei familiari per avermi permesso di svolgere la fase sperimentale e la redazione di questa tesi nel silenzio e nella tranquillità di cui necessitavo.
Un sincero grazie a Silvia, la mia ragazza, la quale mi ha saputo sopportare nei momenti difficili sostenendomi e stimolandomi a proseguire e porgendomi quel valido aiuto che ha contribuito a farmi arrivare fino a qui.
Un ringraziamento finale a tutti coloro che, seppure non citati di persona, hanno contribuito al raggiungimento del primo traguardo al quale sono appena giunto.

Indice

Sommario

L'intento di questa tesi è quello di instaurare nel lettore la conoscenza di una falla che interessa le reti a pacchetto GPRS.
Tale falla presenta un problema sia dal punto di vista economico che della sicurezza, tuttavia nei capitoli successivi si concentrerà l'attenzione sui risvolti economici che questa implica.
L'analisi del problema è corroborata da risultati sperimentali ottenuti con metodi e conoscenze che verranno introdotte nei prossimi capitoli.
Segue una breve introduzione ai punti che questo elaborato esamina o approfondisce:

- inizialmente vengono presentati i concetti che sono alla base dell'elaborato. Ogni concetto è descritto esaustivamente per consentire al lettore una comprensione immediata del contenuto e delle finalità dell'esperimento;
- successivamente si procede con l'esporre l'esperimento eseguito. Verranno presi in esame gli strumenti necessari e le modalità di svolgimento della prova;
- reso noto il modo in cui è stato svolto l'esperimento, si procede con l'analisi dei risultati ottenuti classificandoli per tipologia e quantità;
- i risultati delle analisi permetteranno di dare delle conclusioni sull'entità del problema;
- si conclude accennando a conseguenze in termini di sicurezza.

Capitolo 1

Introduzione ai concetti utilizzati

In questa sezione si mira a spiegare il significato dei termini che verranno utilizzati nei successivi capitoli. Una conoscenza di questi termini rende più agevole capire lo sviluppo dell'esperimento anche a chi non ha mai manipolato la tecnologia utilizzata nella prova.

1.1 Indirizzi IP: pubblici, privati, statici e dinamici

Un indirizzo IP ("Internet Protocol address") è un'etichetta numerica che identifica univocamente un dispositivo collegato ad una rete informatica che utilizza tale protocollo al livello di rete (livello 3 del modello ISO-OSI). A differenza della maggior parte dei protocolli a livello di rete più vecchi, IP è stato progettato fin dall'inizio pensando alla comunicazione tra reti. Il suo compito è quello di fornire un servizio best effort (quindi non garantito) per trasportare i datagrammi (pacchetti di livello 3) inviati da una sorgente ad una destinazione senza curarsi di dove siano posizionate le macchine, le quali potrebbero trovarsi su reti diverse, non considerando quindi eventuali reti intermedie presenti nel percorso di comunicazione.
In questo elaborato verranno presi in esame indirizzi IP di tipo IPv4. Questa versione del protocollo IP prevede indirizzi di lunghezza pari a 32 bit rappresentati solitamente in notazione decimale puntata[1]; l'indirizzo è diviso in 4byte, ognuna delle 4 parti può quindi assumere un valore da 0 a 255.
Gli indirizzi IP sono gerarchici; ogni indirizzo è composto da un gruppo di bit di rete iniziali e dalla restante parte che rappresenta i bit di host. All'interno di una stessa rete ogni elemento connesso ha un indirizzo IP che varia

[1] in ambito web l'indirizzo può essere convertito da notazione numerica a testuale perché più semplice da memorizzare. Il servizio che si occupa della conversione nei due sensi è chiamato DNS ed è implementato sui server web attraverso l'omonimo protocollo.

solo per la parte di host[2]; solitamente all'indirizzo IP è affiancato un altro numero, separato da uno slash, il quale rappresenta il numero di bit riservati alla rete o sottorete a cui l'host è connesso.
Un altro parametro rilevante negli indirizzi IP è la maschera di rete, ovvero un'etichetta numerica con la stessa forma degli indirizzi IP; tale etichetta presenta i bit di rete impostati ad "1" ed i restanti a "0".
Un'operazione di "and" logico tra un indirizzo IP e la sua maschera produce come risultato l'indirizzo della rete o sottorete nella quale ci si trova. In Figura 1.1 si può notare la struttura degli indirizzi IP sopra descritta nel caso di più sottoreti.
Ogni host o router nella rete Internet ha un indirizzo IP che identifica la scheda di rete. Quando un host è collegato a più reti, gli vengono assegnati più indirizzi IP; solitamente gli host sono collegati ad una singola rete e perciò necessitano di un solo indirizzo IP, al contrario dei router che per interfacciarsi con la rete esterna necessitano di più di un indirizzo.

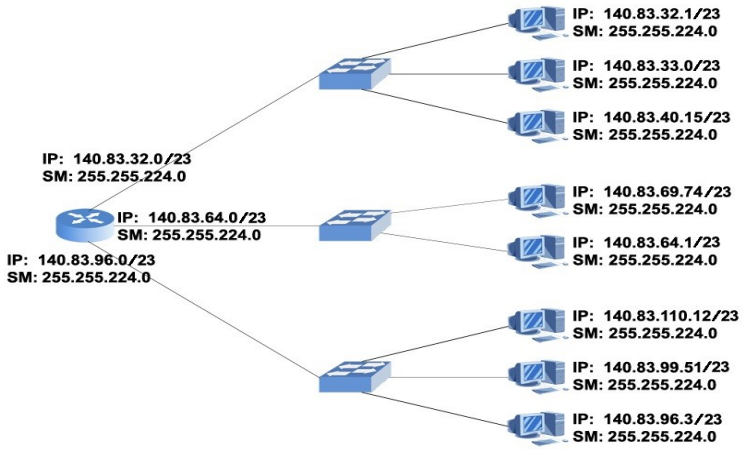


Figura 1.1: Esempio di indirizzi IP e maschere in un insieme di sottoreti

1.1.1 Indirizzi IP pubblici

Si dice pubblico, un indirizzo IP nello spazio di indirizzamento della rete internet che è allocato univocamente ed è potenzialmente accessibile da qualsiasi altro indirizzo IP pubblico, cioè utilizzabile per l'indirizzamento e l'instradamento tramite protocollo IP.

[2]in base al numero di bit riservati alla rete sono state definite classi di indirizzamento con diverso numero massimo di host possibili per rete.

Gli indirizzi IP pubblici sono rilasciati e regolamentati dall'ICANN[3] tramite una serie di organizzazioni delegate. Tuttavia è da tener presente che a livello mondiale e nazionale i primi provider di connessione Internet si sono accaparrati un numero sproporzionato di indirizzi IP, spesso molto superiore alle loro reali esigenze, portando ad una scarsità di indirizzi IP disponibili a favore di altri operatori.
Gli indirizzi IP pubblici sono teoricamente intorno ai 4 miliardi (precisamente 2^32), ma la modalità della loro allocazione e le necessità pratiche dovute all'instradamento dei dati stanno rapidamente terminando la loro disponibilità; per questo motivo si è optato per lo sviluppo e l'uso di soluzioni diverse.
Per ragioni di scalabilità della tabella di routing globale di internet, gli indirizzi IP pubblici vengono assegnati a grandi blocchi ai provider, i quali poi provvedono ad assegnare sotto blocchi o anche singoli indirizzi ai propri clienti.

1.1.2 Indirizzi IP privati

Questa tipologia di indirizzi è utilizzabile da chiunque per la propria rete locale. I pacchetti con questi indirizzi non vengono utilizzati per l'indirizzamento e l'instradamento tramite protocollo IP dai router verso la rete di trasporto. Il loro riutilizzo, oltre a ridurre il numero di indirizzi IP utilizzati, non genera conflitti con analoghi indirizzi posti su altre reti locali in quanto non sono visibili dall'esterno della rete locale.
Nel caso occorra connettere ad Internet una rete locale che utilizza queste classi di indirizzi si deve ricorrere al "Network Address Translation" (NAT), il quale mappa più indirizzi IP privati in un solo indirizzo IP pubblico visibile all'esterno della rete ed utilizzabile per l'instradamento.
I provider che si sono affacciati successivamente sul mercato, hanno ovviato al problema dei pochi indirizzi pubblici rimasti adottando questo tipo di soluzione: considerano gli utenti di una medesima città o area come una rete privata che accede ad Internet mediante un singolo IP pubblico, assegnano quindi ai singoli utenti indirizzi IP privati validi a livello locale.

1.1.3 Indirizzi IP statici

Un indirizzo IP è dichiarato come statico se rimane permanentemente associato ad una stessa interfaccia. A livello locale è possibile associare un dispositivo univocamente ad un indirizzo IP tramite il MAC address; ciò permette di monitorare il traffico dei singoli utenti ma espone al rischio di

[3] L'ICANN ("Internet Corporation for Assigned Names and Numbers") è un ente internazionale no-profit, istituito il 18 settembre 1998, che ha l'incarico di assegnare gli indirizzi IP.

attacchi informatici. Anche all'esterno della rete locale è possibile ottenere IP statici a prescindere dalla natura privata o pubblica dell'indirizzo.

1.1.4 Indirizzi IP dinamici

L'aggettivo dinamico associato ad un indirizzo IP indica che quest'ultimo è assegnato ad un'interfaccia ogni qualvolta il dispositivo che la ospita cerca di connettersi alla rete. Dalla definizione si intuisce che l'indirizzo può variare liberamente ad ogni riconnessione in base al primo che risulta libero[4]. L'assegnazione dinamica permette una riduzione dello spreco degli indirizzi IP in quanto, a differenza del caso statico, quelli inutilizzati possono essere riassegnati ad un altro dispositivo che tenta di connettersi.

1.2 I protocolli TCP, UDP e ICMP

Dopo aver analizzato l'"Internet Protocol", protocollo di livello 3 del modello ISO-OSI, descriviamo i tipici pacchetti di livello 4 che l'IP incapsula:

- TCP: è un protocollo orientato alla connessione, ovvero prima di poter trasmettere dati deve stabilire la comunicazione negoziando una connessione tra mittente e destinatario. Essa rimane attiva anche in assenza di scambio di dati e viene esplicitamente chiusa quando non più necessaria. Il TCP quindi possiede le funzionalità per creare, mantenere e chiudere/abbattere una connessione. Il servizio offerto da TCP è il trasporto di un flusso di byte bidirezionale tra due host. Il protocollo permette alle due interfacce di trasmettere contemporaneamente in entrambe le direzioni $servizioFull - Duplex$.
  Il flusso di byte viene frazionato in blocchi per la trasmissione, tale divisione non è necessariamente la stessa nei diversi passaggi. TCP garantisce che i dati che giungono a destinazione lo facciano in ordine e una volta sola (at most once). Questo è realizzato attraverso vari meccanismi di acknowledgment e di ritrasmissione su timeout.
  TCP offre funzionalità di controllo degli errori sui pacchetti pervenuti grazie al campo checksum contenuto nella sua PDU[5]. TCP possiede funzionalità di controllo del flusso attraverso il meccanismo della finestra scorrevole che permette di ottimizzare l'utilizzo della rete anche in caso di congestione. TCP fornisce un servizio di multiplazione delle connessioni su un host attraverso il meccanismo delle porte.

[4]Il range di indirizzi assegnabili è stabilito in base a quanti bit di rete sono presenti in un indirizzo; il server o router sfrutta quindi questa informazione al momento dell'assegnazione degli indirizzi.

[5]Una Protocol Data Unit (PDU) è l'unità d'informazione o pacchetto scambiata tra due peer entities in un protocollo di comunicazione di un'architettura di rete a strati.

- UDP: a differenza del TCP, è un protocollo di tipo connectionless che non gestisce il riordinamento dei pacchetti né la ritrasmissione di quelli persi; è perciò generalmente considerato di minore affidabilità. L'UDP è invece molto rapido ed efficiente per le applicazioni "leggere" o time-sensitive; è infatti usato spesso per la trasmissione audio-video real-time. Le applicazioni in tempo reale richiedono un bit-rate minimo di trasmissione puntando a non ritardare eccessivamente la trasmissione dei pacchetti, tollerano quindi la perdita di qualche dato. L'UDP fornisce soltanto i servizi basilari del livello di trasporto, ovvero la multiplazione delle connessioni ottenuta attraverso il meccanismo di assegnazione delle porte e la verifica degli errori mediante un checksum (inserita in un campo della PDU).
  L'UDP è un protocollo stateless (non si cura dello stato della connessione) pertanto, rispetto al TCP, ha meno informazioni da memorizzare.

- ICMP: è un protocollo di servizio per reti a pacchetto che si occupa di trasmettere informazioni riguardanti malfunzionamenti, informazioni di controllo o messaggi tra i vari componenti di una rete di calcolatori. ICMP è incapsulato direttamente in IP e non è quindi garantito l'arrivo dei pacchetti. Questo protocollo è utilizzato da molti applicativi di rete, tra i quali ping e traceroute.

1.3 Connessioni alla rete: il GPRS

Le connessioni alla rete avvengono essenzialmente attraverso due modalità tra loro distinte: la commutazione di circuito e la commutazione di pacchetto.

1.3.1 Commutazione di circuito

La commutazione di circuito comporta una reale connessione fisica tra due stazioni comunicanti realizzata attraverso la connessione di nodi intermedi sulla rete. Ogni comunicazione effettuata tramite la commutazione di circuito coinvolge tre fasi:

- apertura della connessione;
- trasferimento dei dati;
- chiusura della connessione.

Prima che i dati possano essere trasferiti deve essere stabilito un cammino che collegherà il mittente ed il destinatario per tutto il tempo necessario a trasmettere i dati. L'uso del cammino è esclusivo e continuo. Ciascun utilizzatore ha a disposizione un canale trasmissivo dedicato che garantisce di avere sempre la capacità massima ad ogni richiesta di servizio. Questa modalità di connessione è la stessa utilizzata dalla tecnologia DSL.

La capacità del collegamento può essere suddivisa in circuiti con diversi meccanismi:

- divisione di tempo;
- divisione di frequenza;
- divisione di lunghezza d'onda;
- divisione di codice.

L'eventuale frazione di capacità trasmissiva non utilizzata (arco di tempo in cui non avviene l'invio di dati) è persa; questo è uno dei grossi limiti della commutazione di circuito. Tra i principali vantaggi c'è la garanzia che se la connessione viene stabilita, essa godrà per tutta la sua durata delle prestazioni richieste. La tariffazione di questo tipo di connessioni è dunque basata sull'effettivo durata della connessione[6] in quanto il canale che si instaura tra i dispositivi rimane occupato anche nel caso in cui non ci sia traffico trasmesso.

1.3.2 Commutazione di pacchetto

Nella commutazione di pacchetto l'idea di base consiste nel suddividere l'informazione in entità elementari (i pacchetti) che poi vengono trasmesse e instradate individualmente, ognuna in modo indipendente, per essere poi riassemblate nel punto di destinazione. L'instradamento dei pacchetti avviene usando in ogni nodo della rete apposite tabelle di routing di tipo dinamico che ad ogni pacchetto ricevuto su una interfaccia associano la corrispondente interfaccia di uscita verso il nodo successivo. La determinazione dell'interfaccia di uscita viene stabilita in base a meccanismi di auto-apprendimento oppure tramite appositi protocolli di routing, questo approccio consente un utilizzo più efficiente della capacità trasmissiva di una rete rispetto alla commutazione di circuito. Nella commutazione di pacchetto i circuiti fisici sono utilizzati solo per il tempo strettamente necessario alla trasmissione di un singolo pacchetto e sono subito disponibili per poter trasmetterne un altro appartenente a un segnale diverso. Ciò consente un livello di condivisione del mezzo più elevato. Di contro, nelle reti a commutazione di pacchetto il ritardo di trasferimento complessivo non è fisso e data la natura non continuativa della trasmissione e l'utilizzo condiviso, insorge anche la necessità di controllare la congestione nel caso di concorrenza. Per le sue caratteristiche, la commutazione di pacchetto pone quindi un problema nel caso sia necessaria una disponibilità garantita di banda o nelle trasmissioni real time. I pacchetti, di dimensioni limitate, sono arricchiti con un'intestazione contenente informazioni riguardo la posizione del pacchetto nella lista di quelli

[6] In caso di abbonamento di tipo flat questo non sussiste in quanto il costo della connessione è fatturato senza variazioni dovute al tempo di sfruttamento della rete.

inviati, la priorità, il destinatario e il tipo di contenuto trasportato e con un campo in coda contenente un codice di controllo degli errori, il quale verrà rieseguito dal destinatario per verificare la correttezza del pacchetto ricevuto.
Quando un nodo intermedio (detto commutatore di pacchetto) riceve un pacchetto, esso decide qual'è il percorso migliore che quest'ultimo può prendere per raggiungere la sua destinazione in base alle informazioni presenti nelle tabelle di routing e ai risultati delle elaborazioni da parte dei protocolli di routing. Questa strada può cambiare di pacchetto in pacchetto a seconda delle condizioni della rete, quindi i pacchetti appartenenti ad uno stesso messaggio possono intraprendere percorsi distinti.
La tariffazione della tecnologia a commutazione di pacchetto viene solitamente effettuata in base al volume di traffico generato in ricetrasmissione in quanto è solamente l'istante di invio del pacchetto che occupa il canale, il quale viene poi rilasciato.

1.3.3 Il GPRS

Acronimo di "General Packet Radio Service", rappresenta il sistema di rete wireless successore del GSM[7]. Tale sistema è considerato come la generazione 2.5, transizione tra il GSM e l'UMTS[8]. La tecnologia GPRS viene introdotta per affiancare la rete GSM in tutto ciò che riguarda la commutazione di dati a pacchetto permettendo un'assegnazione più flessibile delle risorse grazie all'uso più efficiente del canale[9]; tutto ciò è consentito da questo tipo di commutazione.
Il GPRS non richiede nessun setup per accedere alla rete velocizzando quindi l'instaurazione del collegamento; il terminale dell'utente è sempre connesso e la tariffazione avviene secondo il volume di dati ricetrasmessi. L'aspetto più apprezzato dalla maggior parte dei consumatori è probabilmente la compatibilità con internet; essendo basata sul protocollo IP, la rete GPRS permette infatti di accedere a tutti i servizi disponibili sulla rete. La rete GPRS può essere considerata la prima estensione wireless della rete Internet.
Come già accennato, il GPRS è nato per affiancare il GSM e non per sostituirlo; esso utilizza, per quanto possibile, gli elementi funzionali (strumentazione e hardware) già presenti. Le maggiori modifiche riguardano gli apparati che erano destinati alla connessione puramente a commutazione di circuito, ora affiancati dai corrispettivi per la commutazione a pacchetto. Tali elementi di innovazione si occupano di connettere i dispositivi, instradare i pacchetti nelle reti esterne rendendoli compatibili attraverso opportuni protocolli

[7] 2^ generazione dei sistemi di reti wireless a commutazione di circuito.
[8] 3^ generazione di sistemi di rete wireless
[9] La rete GPRS consente di arrivare a velocità di picco di 171.2 kb/s rispetto ai 9.6 kb/s di picco della rete GSM.

di tunnelling[10] e viceversa instradare verso i dispositivi della propria rete i pacchetti provenienti da reti esterne. Il roaming deve essere supportato da specifici accordi tra i gestori delle rispettive reti.
La rete GPRS fornisce due differenti topologie di servizio: PTP ("Point To Point") e PTM ("Point To Multipoint"). Il PTP connette due dispositivi e può essere di tipo "Connection Less"[11] oppure "Connection Oriented"[12]. Il PTM prevede invece più di un utente destinatario.
Un terminale che vuole usufruire dei servizi GPRS, una volta sincronizzato con una base ricetrasmittente, chiede di accedere al servizio GPRS inviando alla rete una richiesta "GPRS attach". Con tale richiesta la rete viene informata che l'utente desidera utilizzare un servizio della rete GPRS, senza questa operazione il terminale risulterebbe non raggiungibile. Successivamente la rete svolge alcune funzioni amministrative quali l'autenticazione dell'utente, la memorizzazione del suo profilo e l'assegnazione di un identificativo. Fatto ciò, la rete stabilisce una connessione logica con il dispositivo, il quale si trova in uno stato di attesa (standby) che non impegna risorse fisiche. Il dispositivo è ora pronto per iniziare un eventuale trasferimento di dati. La disconnessione dalla rete GPRS è detta "GPRS detach" e può essere richiesta dal mobile o dalla rete.

1.4 Il PPP

Acronimo di "Point to Point Protocol", il PPP è un protocollo di livello "data link". Oggi viene utilizzato largamente per accedere ad una rete geografica e funziona su un'ampia varietà di link. La funzione di PPP è quella di incapsulare pacchetti IP o di altri protocolli di livello 3 e trasmetterli su un canale punto-punto. PPP svolge altre importanti funzioni come l'autenticazione e la compressione.
PPP comprende tre componenti principali:

- un metodo per incapsulare i pacchetti provenienti dal livello superiore;
- un protocollo LCP ("Link Control Protocol"), il cui compito è stabilire, configurare e controllare lo stato del link durante la sessione di comunicazione ed infine terminare il collegamento;

[10] Tra due nodi della rete il "GPRS Tunneling Protocol" incapsula le PDU di livello rete, all'interno delle quali troviamo i protocolli TCP/UDP e IP utilizzati per il trasporto dei dati sulla dorsale GPRS.

[11] I pacchetti inviati al destinatario sono indipendenti tra loro; è un servizio noto come servizio a datagrammi e può essere utile per supportare applicazioni di tipo non interattivo

[12] stabilisce in fase di setup un circuito virtuale tra sorgente e destinatario dei pacchetti, che resta attiva durante tutta la durata della connessione. La differenza rispetto alla commutazione di circuito è che le risorse vengono rilasciate quando ogni singolo pacchetto è stato trasferito. Questo sevizio di trasporto è più adatto ad applicazioni interattive in tempo reale.

– una famiglia di protocolli, NCP ("Network Control Protocol") per configurare diversi protocolli di livello rete (IP, IPX);

Il pacchetto PPP ha il seguente formato:

Flag	Address	Control	Protocol	Data	FCS	Flag

– Flag= 0x7E serve per marcare l'inizio e la fine del pacchetto;

– Address è sempre uguale a 111111111 perché PPP è un protocollo punto-punto e non assegna perciò indirizzi alle stazioni;

– Control contiene sempre 00000011 che codifica una modalità di trasmissione non connessa;

– Protocol contiene il codice del protocollo incapsulato;

– Data è la trama relativa al protocollo incapsulato. La dimensione max di default è 1500 byte;

– FCS contiene il codice per la correzione degli errori.

Le operazioni effettuate da PPP comprendono le seguenti fasi:

Inizialmente: Stabilimento della connessione e negoziazione dei parametri.

Successivamente: Stima della qualità della connessione (opzionale).

Infine: Negoziazione della configurazione del protocollo di livello 3.

Le opzioni di configurazione negoziate riguardano:

– lunghezza del pacchetto o MTU (default 1500 byte);

– autenticazione;

– compressione (viene negoziata la soppressione di alcuni campi dell'header, per es. protocol, address, control);

– rilevazione degli errori.

LCP svolge il compito di terminare la connessione anche indipendentemente dalla volontà dell'utente. Ciò accade nel caso in cui si verifichi un evento che costringe LCP a chiudere il collegamento[13].

[13]Esempi in cui interviene l'LCP per la chiusura forzata della connessione sono: perdita della portante, mancata autenticazione, timeout su inattività dell'apparato, perdita di qualità del collegamento

Una volta configurato il protocollo, è possibile opzionalmente impostare l'autenticazione. PPP usa due protocolli di autenticazione: PAP[14] e CHAP[15]. Due importanti opzioni di configurazione che seguono l'autenticazione sono la compressione degli header di TCP e IP e l'assegnazione dinamica dell'indirizzo IP. Finita questa fase la comunicazione dei dati può avere inizio[16].

1.5 Sim "Machine to Machine"

Le sim "Machine to Machine" (M2M) sono delle particolari schede sim la cui particolarità è quella di poter effettuare traffico dati, non ammettendo quindi traffico voce o di messaggistica SMS. I piani tariffari che interessano tale tipologia di schede sono pensati ad hoc per il traffico dati. A seconda dell'operatore con cui viene stipulato il contratto per la M2M, si può optare per una tariffazione oraria o per volume di dati. Tale scelta dipende totalmente dall'uso che si intende fare della M2M.
L'utilizzo principale delle M2M è l'installazione in un dispositivo con lo scopo di farlo interagire o funzionare senza l'ausilio dell'uomo, scambiando istruzioni con una base remota.
Le sim M2M trovano impiego in un'infinità di casi, di seguito ne vengono elencati alcuni:

- impianti di condizionamento dell'aria che possono rilevare dati di temperatura;
- impianti di videosorveglianza che inviano segnali d'allarme ad un centro remoto;
- sistemi di geolocalizzazione in grado di inviare informazioni riguardo alla posizione sulla terra;
- sistemi di ristorazione automatica dove si vuole rilevare se un determinato ingrediente è finito;

[14] "Password Authentication Protocol"; il client invia ripetutamente il proprio nome e la propria password al provider aspettando una conferma di autenticazione. La password viene inviata solo nella fase di autenticazione e attraversa le rete in chiaro. Per questo può essere intercettata da terzi e riutilizzata.

[15] "Challenge Authentication Password Protocol"; In questo caso il processo di autenticazione rimane attivo per tutta la durata della sessione di comunicazione. Il meccanismo di autenticazione è più complesso e presuppone che ciascuno dei nodi conosca l'username dell'altro e un'unica password condivisa.

[16] pppd (acronimo di point-to-point protocol daemon) è un demone tipico dei sistemi GNU/Linux e di altri sistemi Unix-like che permette di realizzare connessioni di rete punto-punto mediante il protocollo PPP usando modem analogici o ADSL.

– in un'azienda si può monitorare da remoto i macchinari in cui risulta installata una sim M2M per rilevare eventuali guasti o comunicare automatismi.

Capitolo 2

Preparazione e avvio della fase sperimentale

A questo punto il lettore dovrebbe avere acquisito delle conoscenze adeguate per capire l'intento della fase sperimentale. Si procederà dunque illustrando com'è stato preparato e svolto lo studio terminando con l'analisi dei risultati ottenuti.

2.1 Presentazione del problema

Nella maggior parte dei casi, quando ci connettiamo alla rete sfruttando una connessione GPRS, dopo una fase di negoziazione riguardo i parametri del canale comunicativo, ci viene assegnato un indirizzo IP.
Prestando attenzione a quest'ultimo passaggio, ci si può facilmente accorgere che ogni volta che effettuiamo una connessione alla rete GPRS l'indirizzo IP che ci viene assegnato è diverso. Questo accade perché la modalità di assegnazione degli indirizzi IP da parte di quasi tutti i provider è di tipo dinamico. A causa del numero limitato di indirizzi IP disponibili, probabilmente quello che ci è appena stato assegnato poco prima apparteneva ad un altro host che ha terminato la connessione o che è stato disconnesso dal server. Non esiste nessun tipo di controllo da parte degli operatori telefonici sul traffico residuo che continua a fluire da una connessione appena terminata, perciò sorge il dubbio che si possa ricevere del traffico non di nostra proprietà.
I pacchetti che potremmo ricevere dovrebbero essere per la maggior parte di tipo IP.
Un calcolatore connesso alla rete GPRS, al rilevamento di un pacchetto IP che ne incapsula uno TCP è in grado di rilavare se il pacchetto in questione non è a lui destinato, in caso affermativo risponde al mittente con un pacchetto dello stesso tipo avente un flag di reset impostato a "1". Questo indica al mittente che deve essere interrotto il precedente flusso di informazione. In

caso di ricezione di pacchetto UDP invece il calcolatore non è in grado di resettare la connessione a causa della natura di questo protocollo (capitolo 1.2).
Nei sistemi embedded che vengono utilizzati semplicemente per la connessione alla rete GPRS, mancano i meccanismi di reset che caratterizzano i calcolatori più evoluti, il rischio è quindi di continuare a ricevere anche i pacchetti TCP a noi non destinati. La ricezione in tal caso avviene finché il mittente non lascia cadere la connessione alla scadenza dei timeout di attesa di risposta.
L'utenza media si appoggia ad operatori telefonici che offrono piani tariffari comprendenti traffico internet, voce e di messaggistica con limitazioni quantitative in base al costo mensile di tale traffico. Il prezzo di questi piani tariffari risulta vantaggioso per il singolo, che può usufruire del piano scelto in base alle proprie esigenze.
Poniamoci ora nell'ottica aziendale; nel nostro caso ipotizziamo che un'azienda media abbia l'esigenza di gestire un numero rilevante di dispositivi che svolgono attività delle più disparate[1]. Questa azienda, per abbattere i costi di gestione decide di sostituire il supervisore umano addetto ad ogni macchinario con un sistema di gestione remoto, perciò necessita di collegamenti alla rete che possano inviare informazioni ad una base operativa che monitorizza il tutto.
Questo genere di trasmissioni di dati sono generalmente di due tipi:

- relativamente frequenti trasmissioni di piccoli volumi di dati;
- trasmissioni sporadiche di una mole più consistente di dati.

Queste due modalità di sfruttamento della rete prevedono sostanzialmente il medesimo consumo medio mensile di megabyte. Un'azienda che intende intraprendere lo sfruttamento remoto delle sue attrezzature con queste modalità di traffico, non ha la possibilità di usufruire delle medesime tariffe dedicate all'utenza media in quanto moltiplicare i piani tariffari per ogni sim attiva risulterebbe troppo oneroso.
La soluzione per tali aziende proviene da alcuni operatori di telefonia sotto forma delle sim "Machine to Machine" (M2M). Queste schede sono adibite solamente al traffico dati e su di esse gli operatori applicano delle tariffe ad hoc in base al volume di traffico ricetrasmesso sulla rete GPRS[2]. In tal modo un'azienda in possesso di avariate M2M non incorre in spese eccessivamente onerose. Alcuni operatori telefonici non contemplano un canone mensile nelle M2M, il che consente di pagare solo ed esclusivamente il traffico che viene

[1] Con tali dispositivi si possono intendere sistemi di videosorveglianza, congelatori, caldaie, robot, distributori di bevande o alimenti.

[2] Alcuni operatori utilizzano anche piani tariffari relazionati al tempo di connessione anziché al volume, ma questo diverso approccio non ha interesse ai fini dell'elaborato in questione.

effettuato.
Questa tipologia di utilizzazione della rete GPRS è largamente utilizzata nel mondo ed in continua espansione in quanto si cerca sempre più frequentemente di centrare i controlli aziendali in un'area senza dover disporre di molti operatori umani.
L'elaborato si occupa dell'analisi di questa tecnologia in relazione al problema della ricezione di dati superflui precedentemente introdotta. Quando un dispositivo (A) si connette tramite una sim M2M alla rete per trasmettere i dati necessari, un server assegna alla relativa interfaccia un indirizzo IP dinamico. L'IP dinamico assegnato, come spiegato nel capitolo introduttivo, con molta probabilità era associato all'interfaccia di un altro dispositivo (B). Al verificarsi di questa situazione, il dispositivo (A) riceverà pacchetti indesiderati destinati al dispositivo (B), i quali rappresentano il traffico residuo presente nel canale. Come spiegato nel capitolo 1.3.2 il canale creato di volta in volta al momento dell'invio di ogni pacchetto e subito dopo disattivato. Solitamente i dispositivi che ospitano sim M2M sono semplici sistemi embedded, i quali non hanno nemmeno la possibilità di resettare le connessioni con protocollo TCP. I sistemi remoti finiscono quindi per ricevere un determinato numero di pacchetti, in alcuni casi considerevole, che vengono tariffati come traffico in ricezione anche se non costituiscono informazione utile ricetrasmessa dal dispositivo (A).
L'intento di questa tesi è studiare questo fenomeno per quantificare l'entità del danno economico recato e soprattutto portare alla luce questa falla, della quale pochi (oltre agli operatori telefonici) conoscono l'esistenza.

2.2 Il materiale utilizzato

In questa sezione si presenta la strumentazione utilizzata nella fase sperimentale, così da poter replicare l'esperienza in caso di interesse o curiosità.
Innanzitutto serve un dispositivo in grado di connettersi alla rete GPRS grazie ad un'interfaccia che serve da "end point" del canale comunicativo. In questo esperimento è stato utilizzato un modem come quello nella Figura 2.1.

Per potersi connettere alla rete è necessario, se il dispositivo non la integra come nel nostro caso, di un'antenna esterna in grado di ricevere il segnale GPRS come quella nella Figura 2.2.

Una volta assemblato il modem, abbiamo la necessità di collegarlo ad un calcolatore per poterli mettere in comunicazione e rendere così possibile il trasferimento dei dati. Il collegamento dal lato modem avviene tramite un'interfaccia seriale del tipo RS232 (Figura 2.3), mentre dal lato del calcolatore possiamo scegliere tra un'altra interfaccia seriale RS232 oppure una comune

Figura 2.1: Modem Telit, modello ez863-gps gprs utilizzato per l'esperimento

Figura 2.2: Esempio di antenna esterna per captare il segnale

USB[3] (Figura 2.4) tramite adattatore o cavo dedicato.

Figura 2.3: Cavo RS232< − >RS232

Figura 2.4: Cavo RS232< − >USB

A questo punto abbiamo realizzato tutti i collegamenti fisici necessari per far comunicare i vari elementi della struttura hardware che utilizzeremo. L'ultimo pezzo di cui abbiamo bisogno è una comunissima sim (Figura 2.5).

Figura 2.5: comune sim card fornita da un operatore telefonico

[3]Onde evitare problemi di compatibilità presentati in alcuni casi dall'interfaccia USB, si consiglia dove possibile l'utilizzo della RS232.

2.3 La preparazione

Una volta collegati tutti i componenti, installato la carta sim e avviata l'alimentazione siamo pronti per configurare il modem per agire secondo le nostre istruzioni.
Innanzitutto è necessario conoscere alcuni dettagli del nostro operatore telefonico, in particolare dobbiamo conoscere la rete APN[4] relativa e le credenziali d'accesso[5] che caratterizzano il nostro profilo[6].
Una volta ottenuti i dati, abbiamo tutte le informazioni necessarie alla configurazione del modem.
Per svolgere quest'ultima operazione, dobbiamo poter comunicare con il modem; a questo scopo esistono vari software[7] che forniscono un'interfaccia grafica intuitiva per poter impostare i parametri essenziali del dispositivo, ad esempio minicom[8] o wvdial[9].
Tutti i software disponibili operano alla stessa maniera, differenziandosi grosso modo per funzionalità aggiuntive e/o interfacce grafiche. La prima fase della configurazione consiste nel comunicare al software prescelto quale sia l'interfaccia (in Linux tty) del calcolatore sulla quale deve sintonizzarsi. Fatto questo, siamo in grado di dare le istruzioni necessarie all'interfaccia del modem.
Per comunicare con il modem vengono utilizzati speciali comandi denominati "comandi AT Hayes"[10], sui quali si trovano numerose guide in rete. É necessario prendere un po' di dimestichezza con questi comandi per poter configurare correttamente il modem (per esempio, è utile sapere che il sem-

[4] L'"Access Point Name" o APN è il nome di un punto d'accesso per le reti che permettono il trasferimento dati, come ad esempio GPRS o UMTS.

[5] Molti operatori hanno credenziali d'accesso alla rete nulle quindi non è necessario configurarle, altri come TIM invece necessitano di tali parametri.

[6] Normalmente questi parametri sono trasparenti all'utente in quanto gli smartphone attuali sono autoconfiguranti, tuttavia consultando il web si risale facilmente ai dati necessari.

[7] La prova sperimentale è stata svolta in ambiente Linux, non è quindi assicurato che il software citato sia disponibile in sistemi operativi differenti.

[8] Minicom è un programma che permette la comunicazione con modem seriali al fine di configurarne l'interfaccia; ha un'interfaccia grafica umile, molto simile alla shell. Wvdial può chiamare un modem remoto ma non agisce su pppd ("Point-to-Point Protocol Daemon").

[9] Wvdial è un piccolo programma di utilità che assiste nello stabilire connessioni ad Internet basate su modem. Wvdial, caricate le impostazioni da un file ".conf", ordina al dispositivo di chiamare il numero di un modem remoto e avvia pppd per stabilire il collegamento a Internet.

[10] La maggior parte dei modem fonici utilizza i comandi AT Hayes. La stringa di inizializzazione consiste di una serie di comandi che prepara il modem per la comunicazione, impostando caratteristiche come il tipo di connessione, i tempi di attesa, la rilevazione del segnale di occupato eccetera. Ogni funzione del modem è governata dal relativo comando AT (che sta per ATtention). Per inviare un comando occorre trasmettere sulla porta seriale del modem una stringa ASCII formata da AT seguito da uno o più comandi e da un carattere di ritorno a capo.

plice comando "AT" seguito da un invio, rileva se il modem è correttamente collegato dando risposta "OK" o no, rispondendo "ERROR"). Tramite questi comandi dobbiamo innanzitutto settare la velocità di ricetrasmissione a cui opererà il nostro modem, indicare se consideriamo o no la parità e specificare il numero di bit letti alla volta. Il passo successivo è quello di configurare l'APN e le credenziali che erano state precedentemente recuperate.
Arrivati a questo punto, siamo pronti ad effettuare la chiamata ad un server remoto per la richiesta di connessione. Se tutto è andato a buon fine dovremmo ricevere dal modem la risposta "CONNECT", il che ci indica che il nostro modem è in linea. Finalmente possiamo, a seconda del programma utilizzato, far partire pppd o vederlo partire in automatico, per la fase di negoziazione dei parametri di connessione tra il nostro modem e il remoto. Finita tale fase siamo connessi e assisteremo all'assegnazione di un indirizzo IP.
Con questa procedura abbiamo solamente creato la connessione GPRS e siamo entrati in rete. Tale operazione rende pressoché trasparente il problema che affronta questo elaborato, tuttavia avendo la possibilità di reperire informazioni in tempo reale riguardo il consumo del traffico dati, ci si potrebbe accorgere di aver speso un volume più o meno ampio pur non avendo effettuato nessun tipo di traffico. Questo potrebbe essere un primo campanello d'allarme che prova la veridicità del problema trattato.
Nella prossima sezione ci si occuperà in maniera approfondita del traffico che avviene a nostra insaputa, osservandolo in prima persona.

2.4 Lo svolgimento

Lo svolgimento descritto è testato passo passo su ambiente Linux, si potrebbero quindi riscontrare differenze e/o incompatibilità in caso di differente sistema operativo.
Ai fini dell'esperimento si è presentata l'esigenza di vedere di persona il traffico che viene consumato al momento della connessione. Per poter vedere effettivamente tutto ciò che viene ricevuto, in caso di ricezione di un pacchetto che incapsula il TCP, sorge la necessità di impedire l'invio della risposta con il flag di "RESET" da parte del nostro calcolatore. Per impedire questo automatismo è sufficiente fornire al firewall di sistema nuove regole che obbligano lo scarto di tutti quei pacchetti in uscita che contengono il flag interessato attivo.
Al fine di ascoltare la linea, abbiamo bisogno di creare un socket[11] su di essa,

[11] Con il termine socket si indica un'astrazione software progettata per la trasmissione e la ricezione di dati attraverso una rete. È il punto in cui il codice applicativo di un processo accede al canale di comunicazione per mezzo di una porta, ottenendo una comunicazione tra processi che lavorano su due macchine fisicamente separate. Dal punto di vista di un programmatore, un socket è un particolare oggetto sul quale leggere e scrivere i dati da trasmettere o ricevere.

dandogli le impostazioni che gli consentono di interagire solo sull'interfaccia pppn[12] (dove n è il numero dell'interfaccia) presente una volta connessi alla rete GPRS.
Creato tale canale comunicativo, per poter ascoltare la rete è sufficiente:

1. effettuare la chiamata al server remoto;
2. avviare il pppd;
3. generare il socket sul pppn;
4. leggere il traffico in entrata sul socket tramite la funzione recvfrom()[13].

La funzione recvfrom() ha, tra i vari parametri di ingresso, un buffer sul quale scrive tutto ciò che viene ricevuto.
Svolgendo il procedimento indicato e stampando a schermo o su file ciò che la recvfrom() cattura, si nota che nella maggior parte dei casi, dal momento in cui si instaura la connessione, si cominciano a ricevere molteplici pacchetti che non sono ovviamente stati richiesti. Questo fonda definitivamente l'esistenza del problema trattato.
Si sa che un esperimento, può condurre a risultati unanimamente accettati, solo se risulta ripetibile. Per accumulare dati ai fini di poter effettuare delle stime e classificazioni ci si può servire di uno "script bash". Lo script progettato per questo esperimento ha il compito innanzitutto di avviare la connessione, dopodiché avvia un programma [C] sulla pppn appena creata, il quale rimane in ascolto per 4 minuti scrivendo su file tutto ciò che riceve; a questo punto la connessione viene spenta e dopo un'attesa di un minuto viene ripetuto il procedimento.

[12] L'interfaccia pppn è l'interfaccia sulla quale viaggiano i pacchetti che seguono il protocollo PPP.
[13] Per maggiori informazioni sulla funzione consultare il corrispondente manuale.

Capitolo 3

Analisi quantitativa e qualitativa dei risultati

Come da titolo, questo capitolo si occupa di analizzare i risultati ottenuti dalla fase sperimentale. L'esperimento è stato condotto su circa 400 sessioni di connessione, in ognuna delle quali sono stati catturati i pacchetti ricevuti e inseriti in un file corredato di dati statistici riguardo volume e tipologia dei pacchetti ricevuti.

3.1 Descrizione dei risultati

Durante il corso dell'esperimento, eseguito ininterrottamente per le circa 34 ore necessarie ad effettuare il numero di connessioni indicato, si è potuto notare di volta in volta una marcata diversità di traffico. La tabella 3.1 riporta alcuni dati che sono stati reputati degni di nota. Alcune connessioni non hanno rilevato traffico in ricezione. Con molta probabilità, in questi casi l'indirizzo IP associato all'interfaccia di rete era precedentemente in disuso almeno per un tempo tale da far scadere i timeout delle connessioni attive. A fronte di un modesto numero di connessioni come quelle appena descritte, altre hanno generato moli di traffico di dimensioni interessanti; il valore di picco raggiunto in termini di volume è stato di circa 244kb con un valore medio di circa 16kb.
La classificazione dei pacchetti è stata possibile sfruttando gli RFC[1] dei protocolli interessati. In essi, per ogni protocollo, è possibile consultare struttura e valori dell'intestazione (header) necessari all'identificazione dei vari livelli di incapsulamento del modello ISO/OSI.
Le tipologie di pacchetti ricevuti appartengono tutte, per quanto riguarda il

[1] "Request for Comments", è un documento che riporta informazioni o specifiche riguardanti nuove ricerche, innovazioni e metodologie dell'ambito informatico. Gli RFC una volta vagliati, possono diventare degli standard Internet.

livello 3 ("Network Layer") del suddetto modello, allo standard IP[2]. Quest'ultimo invece, incapsula tipologie differenti di pacchetti di livello 4 ("Transport Layer"), ad esempio: TCP[3], UDP[4], ICMP[5].

3.2 I dati ottenuti

Questa sezione è destinata a riportare uno schema riassuntivo dei dati ottenuti.
Nella tabella 3.1 si possono trovare, come precedentemente accennato, dei dati che sono stati considerati rilevanti.
Il totale dei pacchetti è ripartito tra le varie categorie della tabella; tramite questi valori è stato realizzato il grafico di Figura 3.1 che rappresenta in percentuale il volume di dati suddiviso per tipologia. La categoria "altri pacchetti" presente sia nella tabella che nel grafico contiene ugualmente pacchetti appartenenti alle altre categorie elencate. La differenziazione è sorta a causa di una diversa intestazione di livello 2 ("Data Link") del modello ISO/OSI che ha portato il software a classificarli in una categoria a parte.
Al fine dell'esperimento questa inesattezza non rappresenta fonte di errore in quanto anche questa categoria di pacchetti rappresenta volume di traffico ricevuto.

Parametro Rilevato	**Valore**
Totale pacchetti ricevuti	41283
Media pacchetti per connessione	103
Totale pacchetti TCP ricevuti	24213
Totale pacchetti UDP ricevuti	7302
Totale pacchetti ICMP ricevuti	1144
Totale altri pacchetti ricevuti	8624
Totale volume di traffico in byte	6355584
Volume totale in kb	6206,62
Volume medio di traffico per connessione in kb	15,51
Massimo volume registrato in una connessione in kb	244,22

Tabella 3.1: Alcuni valori degni di nota riguardo i risultati delle connessioni

[2]RFC 791, *"Internet Protocol" (IP)*
[3]RFC 793, *"Transmission Control Protocol" (TCP)*
[4]RFC 768, *"User Datagram Protocol" (UDP)*
[5]RFC 792, *"Internet Control Message Protocol" (ICMP)*

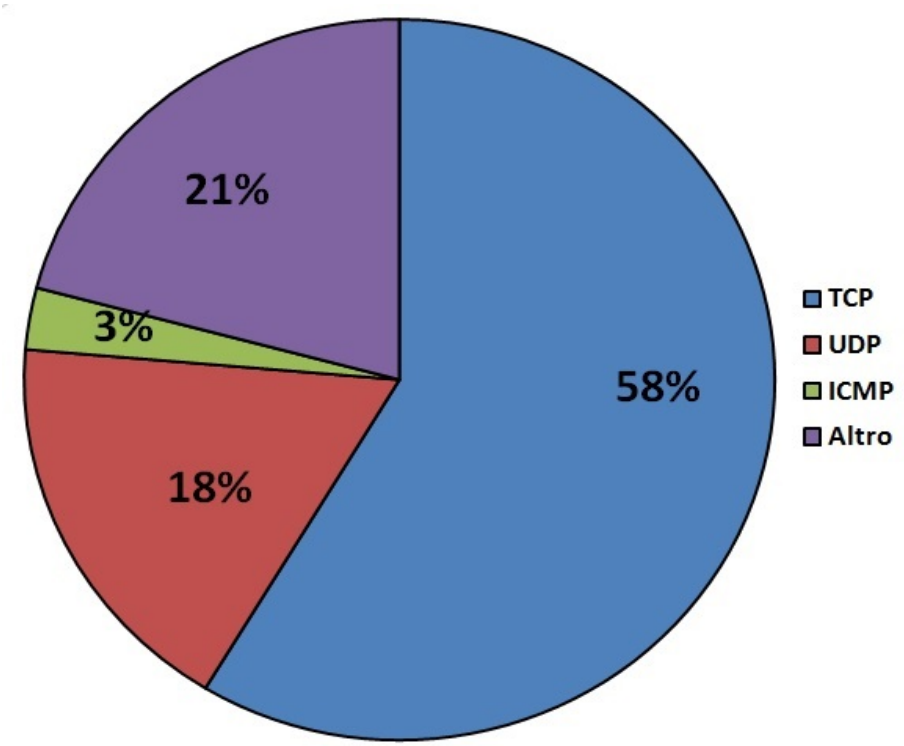


Figura 3.1: Grafico a torta rappresentante le tipologie di pacchetti ricevute.

Le due successive tabelle danno un'idea del tipo di traffico contenuto nei pacchetti analizzati, rispettivamente i pacchetti TCP in Tabella 3.2 e quelli UDP nella Tabella 3.3; esse elencano le porte sulle quali sono stati ricevuti la maggior parte dei pacchetti. Il fatto che IANA gestisca l'assegnazione univoca delle porte permette facilmente di capire la natura di ogni pacchetto, purché la porta di destinazione sia ufficialmente registrata presso tale ente.

Porta TCP	**N° pacchetti ricevuti**
80	8215
443	3913
445	254
59640	169
56820	137
45211	127
22	124
21	17

Tabella 3.2: Alcuni pacchetti di tipo TCP suddivisi in base alla porta ai quali erano destinati

Porta UDP	**N° pacchetti ricevuti**
16401	4312
53	2455
17500	1269
16464	311
16465	271
137	169
43275	106

Tabella 3.3: Alcuni pacchetti di tipo UDP suddivisi in base alla porta ai quali erano destinati

Cercando nel web è possibile trovare la destinazione d'uso di tutte le porte registrate. Sfruttando questa opportunità è stato possibile fare una stima del traffico catturato. Per quanto riguarda il traffico TCP si evince che la metà dei pacchetti ricevuti contenevano informazioni riguardo all'HTTP (porta 80) e all'HTTPS (porta 443). Gli altri pacchetti di questo tipo, in numero

molto minore erano indirizzati a porte dedicate ad altri protocolli noti (ad esempio FTP, SSH, etc.) o ad altre non registrate ufficialmente.
Spostandoci sulla tipologia UDP si può verificare che la grande maggioranza dei pacchetti ricevuti erano destinati a porte occupate dagli streaming audio/video e controlli realtime. Questo fatto non stupisce in quanto, come introdotto all'inizio dell'elaborato, l'UDP viene scelto per assolvere tali compiti data la sua leggerezza che garantisce velocità. Fanno eccezione all'ambito realtime altre porte come la 53 utilizzata dal DNS. Come affermato nel TCP, anche nell'UDP le rimanenti porte utilizzate sono destinate ad altri servizi che possono essere o meno registrati.

3.3 Conclusioni

L'esperimento ha evidenziato la correttezza delle premesse, permettendo di verificare le ipotesi su cui si basava il problema alla base dell'elaborato, ovvero ha provato empiricamente che al momento dell'ingresso in rete, un dispositivo ha molta probabilità di ricevere un addebito di traffico indesiderato, residuo dell'interfaccia a cui era associato precedentemente l'indirizzo IP.
I dati ricavati permettono di trarre delle conclusioni circa la rilevanza del problema presentato.
Un singolo utente medio, che decide di usufruire di una sim "Machine to Machine" per effettuare traffico verso un sistema remoto probabilmente non risentirebbe del carico suppletivo rappresentato dai pacchetti indesiderati ricevuti. Focalizziamoci invece nell'ambito aziendale, dov'è più frequente e intensivo l'uso di questa tipologia di sim. Come descritto nel capitolo 2.1 esistono principalmente due tipi di sfruttamento della rete che si somigliano per volume di traffico generato mensilmente; la differenza fondamentale risiede nel numero di connessioni effettuate.
Nel caso in cui ci si connetta alla rete poche volte per inviare moli rilevanti di dati, non si risentirà in maniera marcata del traffico aggiunto alla tariffazione. Al contrario, nel caso in cui si abbia l'esigenza di connettersi alla rete molte volte per l'invio di pochi pacchetti (per esempio un feedback orario), la maggior parte delle connessioni porterà con se del carico aggiuntivo. Il proprietario della sim si vedrà fatturare tale traffico nonostante non gli appartenga e non lo abbia richiesto. Nel caso in cui, come spesso accade, l'azienda in questione possieda svariate sim di questa tipologia, il fenomeno si moltiplicherà per ognuna di esse. Questo inconveniente fa registrare volumi di traffico non indifferenti che si traducono in una spesa superflua da parte dell'azienda.
Utilizzando i dati ricavati è possibile estrapolare un esempio plausibile per porre il lettore di fronte a risultati numerici che meglio esprimono l'entità del

problema. Supponendo che un dispositivo remoto debba connettersi alla rete per inviare un volume di 200 byte, l'overhead volumetrico medio ricavato dagli esperimenti condotti fa registrare un volume di traffico ricetrasmesso di circa 15,2 kilobyte, in quanto esso si somma al traffico auspicato. Rapportando i due valori in maniera proporzionale, si nota come il volume di traffico sia maggiorato del 7760%.

Capitolo 4

Implicazioni nell'ambito della sicurezza

Il punto debole descritto finora dall'elaborato, costituito dalla visibilità del traffico altrui, è stato considerato da un punto di vista prettamente economico. Lo scopo dell'esperimento era infatti mettere in chiaro e quantificare il danno economico causato dalle tariffe a volume che risultano alterate.
Oltre a questo aspetto, un altro risvolto interessante è rappresentato dalla possibilità di inviare una risposta ad un pacchetto ricevuto.
Il pacchetto deve essere forgiato ad hoc consultando gli RFC per mettere insieme una risposta valida per il destinatario. Esso dovrà rappresentare un acknowledgement; conterrà quindi prima di tutto informazioni riguardo il destinatario (colui che ci ha inviato il primo pacchetto) e racchiuderà le informazioni relative all'ultimo pacchetto ricevuto in modo da poter comunicare al destinatario che può procedere con l'invio dei pacchetti mancanti.
In linea teorica, reiterando nel tempo le risposte di acknowledgement costruite di volta in volta in base ai pacchetti ricevuto, è possibile continuare a leggere il traffico del precedente possessore dell'indirizzo IP che ci è stato assegnato.
Con questo procedimento, senza grosse difficoltà, sarebbe possibile per esempio leggere email e scaricare file altrui.
Anche questo aspetto negativo è da imputare al malfunzionamento che si manifesta all'accesso in rete.

Bibliografia e sitografia

[1] Andrew S. Tannembaum, David J. Wetherall. *Reti di calcolatori, 5ˆ edizione*, 2011 Pearson Italia, Milano-Torino;

[2] RFC 768, *User Datagram Protocol (UDP)*, http://www.ietf.org/rfc/rfc768.txt;

[3] RFC 791, *Internet Protocol (IP)*, http://www.ietf.org/rfc/rfc791.txt;

[4] RFC 792, *Internet Control Message Protocol (ICMP)*, http://www.ietf.org/rfc/rfc792.txt;

[5] RFC 793, *Transmission Control Protocol (TCP)*, http://www.ietf.org/rfc/rfc793.txt;

[6] RFC 1661, *The Point-to-Point Protocol (PPP)*, http://www.ietf.org/rfc/rfc1661.txt;

[7] Wikipedia http://it.wikipedia.org/;

[8] Appunti di reti radiomobili, http://claudiofiandrino.altervista.org/Reti_radiomobili/gprs.pdf;

[9] AT Commands Reference Guide, http://m2m.pp.fi/data/Telit_AT_Commands_Reference_Guide_r5.pdf.

Indice analitico