Abstract

Con la sempre più rapida crescita in termini di dimensioni e complessità delle moderne infrastrutture di rete, l'attività di individuazione e prevenzione di abusi e violazioni nell'uso di tali infrastrutture sta diventando sempre più strategica per garantire alle stesse un adeguato grado di protezione sia dall'esterno che da possibili minacce interne. In questo particolare scenario stanno emergendo prepotentemente molte tecniche per il controllo automatizzato del traffico di rete e basate sulla formulazione di modelli di comportamento normali o anomali del traffico stesso, al fine di rilevare la presenza di attività indesiderate o quantomeno sospette. Innanzitutto va considerato che, la definizione del concetto di andamento normale o anomalo del traffico dipende da diversi fattori legati alle attività giornaliere e all'utilizzo le delle risorse ad esse associate. Infatti, il profilo di normalità del traffico può essere determinato solo attraverso l'acquisizione e l'attenta analisi di informazioni storiche relative allo stesso, seguite dalla formulazione di scenari di previsione basati sull'esperienza passata, ma ovviamente tali analisi di solito richiedono tempo e pertanto pregiudicano la possibilità di rilevare la presenza di fenomeni anomali in tempo reale.

Questo problema può essere risolto provando a modellare il comportamento futuro del traffico basandosi sull'idealizzazione statistica degli eventi passati e l'osservazione di quelli presenti e specificamente analizzando ed osservando alcune proprietà statistiche particolarmente discriminanti, in grado di caratterizzare i fenomeni evolutivi e osservabili nel traffico di rete. Dato che gli eventi anomali vanno ormai considerati una parte strutturale irrinunciabile del traffico di rete globale, diventa sempre più importante poter rilevare automaticamente, classificare e identificare gli stessi al fine di reagire prontamente e adeguatamente ad eventuali minacce o malfunzionamenti. Di conseguenza l'obiettivo principale di questa tesi è lo sviluppo di un nuovo approccio per il rilevare in tempo reale anomalie di traffico in rete basandosi sull'analisi di proprietà e meccanismi di associazione complessi nonchè modelli di ricorrenza e dinamiche non

immediatamente "apparenti" riscontrabili nei flussi aggregati di traffico. Nello studiare ed analizzare tali proprietà al fine di modellizzare e rilevare comportamenti anomali, sono state adottate diverse tecniche che hanno dimostrato la loro efficacia nell'esplorare dinamiche meno apparenti e correlazioni temporali di serie storiche statistiche, come l'analisi multi-risoluzione basata su wavelets e l'analisi di quantificazione dei fenomeni ricorrenti. Sulla base di tali presupposti è stato realizzato un modello adattativo per la classificazione di eventi anomali basato su metodologie di machine learning che ha dimostrato di essere alquanto efficace nell'interpretazione deterministica dei fenomeni non lineari e delle complesse dinamiche di traffico osservabili durante il verificarsi di eventi anomali caratterizzati da variazioni apprezzabili nelle proprietà statistiche del traffico di rete. Pertanto tale modello si è rivelato estremamente utile per sviluppare e osservazioni qualitative e quantitative che possono essere utilizzate in modo affidabile per rilevare tali eventi anomali.