La complessità, il grado di sofisticazione ed il tasso di crescita delle reti moderne, in congiunzione con la profondità, continuità e imprescindibilità del loro ruolo nelle nostre attività quotidiane, sottolineano l'importanza di identificare possibili utilizzi inappropriati o minacce che ne possono pregiudicare l'operatività.

Al fine di assicurare una reazione rapida ed adeguata, le anomalie nel traffico di rete devono essere scoperte, classificate ed identificate nel modo più corretto e veloce possibile.

Molti approcci sono concentrati sull'ispezione del contenuto dei pacchetti in transito sulla rete, mentre altre tecniche mirano ad individuare le attività sospette attraverso la quantificazione dello stato della rete ed il confront con il livello normalmente atteso.

La formalizzazione di un modello per il comportamento normale richiede la raccolta e l'analisi del traffico, allo scopo di isolare un insieme di caratteristiche in grado di descriverlo in modo completo e conciso.

L'argomento principale di questa dissertazione è la ricerca di rappresentazioni efficaci per il traffico di rete, rappresentazioni astratte che sappiano descrivere con semplicità molta dell'intricata struttura esibita dai dati osservati.

In tal modo, alcuni dei fattori e delle variabili nascoste che governano il processo di generazione dei dati possono essere disvelati e isolati, così da individuare eventi anomali con maggiore affidabilità.

Abbiamo usato più metodi per raggiungere tali rappresentazioni semplificate; tra essi l'Analisi delle Componenti Indipendenti e le architetture profonde di apprendimento.

Ci si è avvalsi di tecniche di apprendimento automatico per verificare l'incremento nella capacità di classificazione ottenibile attraverso le rappresentazioni proposte.