L'obiettivo di questa tesi è l'analisi, la progettazione e l'implementazione di un protocollo di puzzle in un sistema client-server al fine di mitigare l'effetto di attacchi DoS. In un protocollo di puzzle, un client è tenuto a risolvere un problema computazionale di difficoltà variabile denominato puzzle e deve presentare la soluzione come proof of work prima che la sua richiesta venga gestita dal server.

I protocolli *proof-of-work* sono protocolli in cui un'entità richiede ad un'altra di svolgere un determinato compito e, una volta svolto, ne controlla il risultato ricevuto per verificarne la correttezza. La particolarità di questi protocolli è l'asimmetria, in quanto il carico computazionale richiesto dalle entità che richiedono i proof-of-work è nettamente inferiore a quello delle entità che devono svolgere il lavoro richiesto.

In un protocollo di puzzle un server consegna ai client delle funzioni hash da risolvere quando percepisce che si sta verificando un attacco in corso, in modo da tardare il loro accesso. In breve, un puzzle è formato dal risultato di una funzione hash e una parte dell'input della funzione, e i client dovranno trovare i bit mancanti per poter accedere al server. Un protocollo di puzzle può essere posto a vari livelli dell'architettura OSI (ad esempio rete o trasporto); in questo caso esso verrà collocato a livello applicazione al fine di proteggere un programma che fa accesso ad un database.

Lo scopo principale è quello di creare un protocollo di comunicazione che comprenda la risoluzione di puzzle. In particolare, il protocollo progettato è costituito da sei messaggi: l'invio della richiesta iniziale, l'assegnazione di un puzzle, l'invio della soluzione, l'accettazione o il rifiuto della richiesta, la richiesta di una risorsa e il suo invio al client.

Per capire quando il server è sotto attacco, viene monitorato il traffico di entrata nel server e si manterrà lo stato dei client per tenere le informazioni dei loro accessi. Quando il numero di accessi supera una soglia di richieste massime accettate impostata all'avvio del server, si attiverà il protocollo di puzzle, alleviando così il carico di lavoro sul server.

Per valutare le prestazioni del sistema si effettueranno dei test con un numero elevato di client in modo da simulare attacchi con molti utenti. Gli attacchi considerati saranno quello classico del flooding e quello di replay, ovvero quando un client invia una stessa soluzione valida già trovata.

Le metriche di valutazione comprendono i principali parametri che sono oggetto di studio nella difesa di attacchi DoS: tempo di accesso, richieste legittime accettate, utilizzo del server. I risultati ottenuti si sono rivelati in linea con quelli previsti e confermano la validità della soluzione proposta.