Università degli Studi dell'Insubria

Dipartimento di Scienze Teoriche Applicate

Corso di Studio Triennale in Informatica

Riassunto

Definizione ed implementazione di protocolli di sicurezza all'interno di un simulatore di reti 5G

Relatore: Dr. Alessandra Rizzardi

Correlatore: Prof.ssa Sabrina Sicari

Tesi di Laurea di: Ferri Matteo

Matr. N. 744234

Anno Accademico 2022/2023

Il lavoro di tesi intende esplorare in dettaglio le potenzialità del 5G e concentrarsi sulla definizione ed implementazione dei protocolli di sicurezza all'interno di un simulatore di rete basato sul protocollo 5G.
In particolare, sono stati sviluppati dei sistemi di crittografia avanzata come AES e ZUC, insieme al protocollo Diffie-Hellman. Inoltre, vengono presentati dei test che simulano situazioni di comunicazione sicura e vengono analizzati gli effetti della sicurezza sulla performance complessiva della rete.

Prima di esaminare i dettagli dei protocolli di sicurezza implementati, è importante comprendere il significato di crittografia. Essa rappresenta la scienza volta a proteggere le informazioni rendendole incomprensibili senza le chiavi necessarie per decifrarle. Questo processo coinvolge la cifratura, che trasforma i dati leggibili in una forma incomprensibile, e la decifratura, che converte il testo cifrato nel testo originale. Le chiavi segrete e condivise sono generate dai protocolli di scambio chiave.

Per sviluppare i protocolli di sicurezza e acquisire i dati riguardanti le loro performance, è stato utilizzato 5G-air-simulator, ossia uno strumento open source e basato sugli eventi che modella gli elementi principali dell'interfaccia aerea 5G da una prospettiva a livello di sistema.
Non esiste un sistema crittografico specifico per il simulatore. È consigliato tuttavia utilizzare algoritmi standardizzati e riconosciuti come sicuri dalla comunità scientifica, che offrono una lunghezza di chiave adeguata al livello di sicurezza richiesto e una complessità computazionale bassa o moderata per blocco.

Degli esempi di algoritmi che soddisfano questi requisiti sono AES e ZUC.

AES, Advanced Encryption Standard, è un algoritmo di cifratura a blocchi ampiamente utilizzato per proteggere dati sensibili tramite crittografia.
AES esegue iterativamente un numero di "rounds" che varia da 10 a 14 a seconda della lunghezza della chiave. In ogni round, vengono svolte diverse procedure, tra cui la sostituzione e la permutazione dei byte, operazioni di shift e altre trasformazioni matematiche. AES utilizza chiavi di diverse lunghezze, tra cui 128, 192 o 256 bit. Per la decifratura, l'AES utilizza funzioni inverse alle operazioni di cifratura per ripristinare i dati originali.
L'algoritmo AES è generalmente considerato molto robusto e resistente contro una vasta gamma di attacchi crittografici. Tuttavia, è importante considerare le sue vulnerabilità e minacce potenziali, tra cui gli attacchi a forza bruta, Side-Channel ed al testo in chiaro. Nonostante queste vulnerabilità, AES possiede ottime performance, specialmente quando utilizzato con chiavi di 128 bit.
Lo sviluppo dell'algoritmo di cifratura AES include funzioni per cifrare e decifrare dati utilizzando diversi modi di operare come ECB (Electronic Codebook), CBC (Cipher Block Chaining) e CFB (Cipher Feedback).
Nel processo di cifratura, il blocco di dati in ingresso viene suddiviso in una matrice, su cui vengono eseguite operazioni di sostituzione, permutazione e combinazione per produrre il blocco di dati cifrati.
Inoltre, l'algoritmo genera una serie di sottochiavi da una chiave di cifratura fornita come input. La chiave segreta viene creata utilizzando il protocollo Diffie-Hellman.

Un altro protocollo di sicurezza sviluppato è ZUC. ZUC è un algoritmo di cifratura a flusso ed è stato scelto come algoritmo di cifratura per le reti di telecomunicazioni di quinta generazione (5G) in Cina. È incluso nello standard di cifratura per il 5G adottato dalla 3rd Generation Partnership Project (3GPP).
L'esecuzione di ZUC coinvolge la generazione di un flusso di bit pseudocasuale dalla chiave segreta e il suo XOR con i dati in ingresso. La chiave segreta viene elaborata attraverso una rete di generatori di flusso che producono una sequenza di bit apparentemente casuale.
L'implementazione dell'algoritmo di crittografia ZUC gestisce il processo di inizializzazione, che comprende l'inizializzazione degli elementi chiave, l'espansione della chiave, l'azzeramento di variabili e registri, e l'esecuzione di un ciclo di inizializzazione per aggiornare gli elementi dell'array LFSR_S. Successivamente, la sua funzione principale è gestire la crittografia dei dati trasferiti sulla rete, utilizzando una chiave di 128 bit.

Per quanto riguarda l'algoritmo di scambio delle chiavi all'interno di 5G-air-simulator, è stato utilizzato Diffie-Hellman (DH), uno dei protocolli più diffusi nel campo della crittografia asimmetrica. Offre un elevato livello di sicurezza e una buona efficienza dal punto di vista computazionale. Il suo obiettivo è consentire a due parti di stabilire una chiave segreta condivisa su una rete non sicura senza mai scambiare direttamente la chiave. La sua sicurezza si basa sulla complessità computazionale del calcolo del logaritmo discreto.

L'implementazione dell'algoritmo di scambio chiave Diffie-Hellman comprende funzioni dedicate alla gestione dell'algoritmo e alla facilitazione della comunicazione tra mittente e destinatario. Queste funzioni consentono l'instaurazione di una comunicazione tra il server e il client, permettendo loro di scambiare dati di tipo intero attraverso l'utilizzo di socket.

Infine, il lavoro di tesi si è focalizzato sull'analisi delle prestazioni dei protocolli attraverso la misurazione dei tempi di esecuzione durante le simulazioni. La latenza di rete può variare per diversi motivi, come il carico di rete, la congestione e i ritardi di instradamento. La crittografia, tuttavia, non è la principale fonte di variabilità nella latenza. Pertanto, se la cifratura e la decifratura sono ottimizzate e veloci, il tempo che il pacchetto trascorre in rete rimane invariato, indipendentemente dalla crittografia. Viceversa, una crittografia inefficiente o complessa può aumentare il ritardo e causare possibili perdite di pacchetti in rete.
Un tempo richiesto per la crittografia di pochi millisecondi per un singolo pacchetto è generalmente considerato abbastanza veloce e può indicare che si sta utilizzando uno sviluppo efficiente dell'algoritmo AES e ZUC. Dai dati raccolti e dai tempi ottenuti durante le misurazioni, emerge che le implementazioni di AES e ZUC, che sfruttano il protocollo Diffie-Hellman, sono state realizzate con efficienza e ottimizzazione. Dunque, esse non compromettono le prestazioni complessive del tool 5G-air-simulator.