Gestión dinámica de claves y transferencia segura de datos basada en una estructura de M-Tree con un marco de seguridad multinivel para la Internet de los vehículos

Kevin Andre Rodriguez Lima
Leonardo Gustavo Gaona Briceño
Philco Puma Josue Samuel

13 de diciembre de 2024

Resumen

En la actualidad, las redes inalámbricas de banda ancha y el 5G han mejorado la calidad y confiabilidad de los servicios de red para vehículos móviles de alta velocidad. Dentro de un entorno de comunicación abierto en el Internet de los vehículos, denominado *IoV* (*Internet of Vehicles*), los detalles personales pueden ser revelados a través de la red Wi-Fi. Considerando la seguridad de la información y la privacidad, esta investigación se enfoca en cómo proteger la transmisión segura de información en tiempo real a través de IoV, evitando además que vehículos ilegales, transeúntes o conductores no autorizados se conecten y planten o alteren datos significativos.

Esta investigación proporciona una infraestructura de seguridad multivariable con un algoritmo de firma digital basado en curvas elípticas (*ECDSA*) y la estructura de M-tree, para asegurar la transmisión de datos en los entornos tanto de IoV como de la nube. Durante la transmisión, este estudio ofrece varios esquemas flexibles y escalables para gestionar los problemas de seguridad, ajustando dinámicamente el marco de trabajo dependiendo de la topología rápidamente cambiante de IoV, acelerando el tiempo de sincronización de la reconstrucción de la clave del sistema y disminuyendo la cantidad de fases necesarias para re-sincronizar la clave del sistema.

Además, mientras que la mayoría de la investigación sobre gestión de claves no se enfoca en la transmisión segura de datos, nosotros integramos la gestión de claves basada en M-tree con la transmisión segura de datos para lograr un IoV seguro. Simultáneamente, la gestión de claves propuesta para la seguridad multivariable es completamente adecuada para un IoV adaptable y expansible.

1. Introducción

A medida que el Internet de Vehículos (IoV, por sus siglas en inglés) se vuelve más popular e inteligente, los vehículos pueden establecer conexiones con dispositivos más abiertos, lo que genera problemas de seguridad. En la actualidad, el IoV está atrayendo gran atención de los investigadores, ya que permite la comunicación mutua entre vehículos, equipos viales e incluso servicios en la nube. Se espera que en el futuro el IoV permita aplicaciones y análisis de grandes datos en la computación en la nube, mientras que las tecnologías V2X (Vehicle-to-Everything) se usarán para mejorar la seguridad en la conducción. Estas incluyen la comunicación de vehículos a infraestructura (V2I), de vehículos a equipos viales (V2R), de vehículo a vehículo (V2V), de vehículos a peatones (V2P), entre otras.

Actualmente, muchos países están invirtiendo en la investigación de vehículos autónomos y sin conductor. El avance de la tecnología 5G impulsará esta tecnología, lo que permitirá una red IoV masiva y conectada. Los vehículos podrán obtener información en tiempo real sobre su estado y el entorno mediante sensores, GPS, radares, cámaras y otros dispositivos de procesamiento de imágenes. Gracias a la computación en la nube, estos datos se analizarán y procesarán para encontrar las mejores rutas y transmitir el estado de las condiciones de tráfico a los centros de control.

En las primeras etapas del IoV, las comunicaciones dependían de transmisiones inalámbricas típicas similares a las redes Wi-Fi, lo que resultaba en una baja fiabilidad y vulnerabilidad a intrusiones. Sin embargo, con el desarrollo de 5G, se espera que IoV evolucione hacia una infraestructura más segura y confiable.

El IoV enfrenta riesgos debido a su entorno de comunicación abierto, lo que puede exponer datos personales en redes Wi-Fi. Este estudio se enfoca en cómo proteger la transmisión segura de información en tiempo real y evitar que vehículos, conductores o peatones no autorizados participen en la red para modificar o robar información crítica. Se propone un sistema basado en la gestión de claves y la verificación de identidad mediante una infraestructura de clave pública (PKI) y una autoridad certificadora (CA) en la plataforma en la nube.

2. Trabajos Relacionados

En los últimos años, se han implementado mecanismos de seguridad livianos, como la autenticación basada en PUF y el protocolo Diffie-Hellman de curvas elípticas, en áreas como sistemas de información médica, redes de sensores y entornos inteligentes. Dado que las redes vehiculares tienen recursos de computación limitados y comunicaciones inestables, las aplicaciones de IoV requieren esquemas criptográficos livianos, especialmente para operaciones de autenticación y gestión de claves.

En 2013, Hu et al. propusieron un esquema que utiliza firmas grupales, pero su tiempo de procesamiento aumenta a medida que se agregan vehículos a la lista de revocación. Otros estudios, como los de Nisha et al. (2018) y Ali et al. (2019), integran blockchain para garantizar la seguridad y privacidad de los vehículos, pero con costos computacionales elevados.

Además, los protocolos basados en firmas y criptografía de identidad, como el propuesto por Xiaodong et al. (2015), mejoran la privacidad pero también aumentan la complejidad operativa. Otros enfoques como los de Joon et al. (2020) y Mu et al. (2021) intentan mejorar la seguridad con técnicas livianas, como el uso de XOR y funciones hash, pero todavía enfrentan limitaciones en términos de eficiencia y escalabilidad.

A pesar de los avances, la mayoría de los métodos existentes para IoV dependen de mecanismos criptográficos complejos, lo que resulta en altos costos de cálculo y comunicación. Por lo tanto, se necesita un sistema de seguridad más liviano, eficiente y escalable para IoV, capaz de proteger las transmisiones de datos frente a una variedad de amenazas.

3. Proceso de Firma Digital ECDSA en IoV

Dado que los dispositivos de IoV tienen recursos de computación limitados, este estudio evalúa diversos algoritmos de firma convencionales y concluye que la firma de curva elíptica (ECDSA) es una opción ideal. ECDSA es eficiente, genera firmas pequeñas y es cada vez más popular. Funciona mediante el uso de una clave privada para firmar un mensaje y una clave pública para verificar la firma, similar a otros algoritmos criptográficos. Sin embargo, ECDSA utiliza claves más pequeñas en comparación con RSA, lo que le permite ofrecer un nivel de seguridad similar pero con menos requisitos de computación y almacenamiento.

A diferencia de RSA, que requiere una mayor longitud de clave y es más lento, ECDSA resuelve el problema del logaritmo discreto en curvas elípticas (ECDLP), lo que lo hace más adecuado para dispositivos con recursos limitados, como los OBUs (On-Board Units) de los vehículos. En este estudio, ECDSA se emplea para asegurar la transmisión de datos entre vehículos (V2V), vehículos y equipos en la carretera (V2R), y vehículos y grupos (V2G).

El protocolo de intercambio de claves ECDH (Elliptic Curve Diffie-Hellman) se utiliza para la gestión dinámica de claves y asegurar la transmisión de datos en el entorno de IoV. ECDH reemplaza las operaciones exponenciales por multiplicaciones y sumas, lo que reduce la carga computacional y la memoria necesaria para los dispositivos en los OBUs. Esto asegura una transmisión rápida y eficiente de información segura.

Además, el estudio considera el uso de un sistema de curvas elípticas con sensores OBU y equipos RSU en el entorno IoV. Se selecciona una curva elíptica definida sobre un campo finito GF(p), donde p es un número primo. Por ejemplo, se utiliza la curva $y^2 = x^3 + x + 1 \mod 307$, que cumple con los requisitos necesarios para garantizar un sistema seguro y escalable.

El proceso de firma ECDSA en este estudio es similar al DSA tradicional, pero utiliza ECC (Elliptic Curve Cryptography) para realizar la firma. El resultado final de la firma se divide en dos partes: r y s. Este enfoque garantiza que la firma sea compacta, eficiente y adecuada para los limitados recursos computacionales de los dispositivos IoV.

4. El Marco de Seguridad Multi-Nivel

El *Internet de los Vehículos* (IoV) requiere integrar vehículos, dispositivos de carretera y servidores en la nube. Debido a esta integración, cada nivel de seguridad se organiza de manera jerárquica, similar a la autorización de empresas. El propósito principal de este estudio es proponer un mecanismo de *gestión de claves* para la seguridad multi-nivel de IoV utilizando un *marco M-árbol (M-tree)*. Este marco asigna diferentes responsabilidades de seguridad a cada nivel, lo que permite gestionar de manera eficiente las claves y la protección de datos.

4.1. Niveles de Seguridad en IoV

- **Nivel 4 (Vehículos):** Cada vehículo (OBU - *On-Board Unit*) se encuentra en el nivel más bajo, donde se encarga de enviar y recibir datos. Los vehículos están conectados en grupos, y cada grupo es considerado como una *unidad de gestión de claves*.
- **Nivel 3 (Unidades de Carretera - RSU):** Las RSU actúan como mediadores que recopilan los datos de los vehículos y los transmiten a la siguiente capa (LCA). Estas unidades se encargan de la *recolección de datos* y la transmisión de información de un vehículo a otro o hacia los servidores de la nube.
- **Nivel 2 (Autoridades Locales de Certificados - LCA):** Estas autoridades gestionan las claves a nivel local, supervisando la autenticación y el intercambio de claves en una zona geográfica específica.
- **Nivel 1 (Autoridad Global de Certificados - GCA y Servidores en la Nube):** En el nivel superior se encuentra el GCA y los servidores de la nube que administran las claves a nivel global y la infraestructura centralizada de IoV.

4.2. Propósito del Estudio

Este estudio propone un *acuerdo de gestión de claves* basado en un sistema multi-nivel para *integrar el criptosistema de curvas elípticas* (ECC) con IoV y plataformas de servicios en la nube. La clave de este enfoque es utilizar el protocolo de intercambio de claves *ECDH* (Elliptic Curve Diffie-Hellman) para garantizar la transmisión segura de datos entre los vehículos (V2V), entre vehículo y unidad de carretera (V2R), y entre vehículos y la nube (V2G).

4.3. Proceso de Gestión de Claves (M - TREE)

El sistema de gestión de claves utiliza un *árbol M* (M-tree) para organizar los dispositivos de IoV según su nivel de seguridad. La propuesta incluye:

- **Gestión de claves a nivel de grupo:** Los vehículos se agrupan y se asigna una *clave de sesión* a cada nodo hoja en el árbol. Esta clave se transmite hacia arriba por las capas del árbol, comenzando en los vehículos (nivel 4) hasta llegar a la *Autoridad Local de Certificados* (LCA) y luego al *GCA*.
- **Resincronización eficiente de claves:** Si un dispositivo (como una RSU) se desconecta o falla, el sistema puede recalcular las claves de manera rápida y eficaz, minimizando el impacto en la seguridad general del sistema.

4.4. Elementos del Sistema

El sistema propuesto se compone de los siguientes elementos:

- **Autoridad de Certificados (CA):** El CA, que tiene grandes recursos de computación y almacenamiento, es responsable de emitir certificados digitales para las RSUs, OBUs y vehículos. Se divide en *GCA* (Autoridad Global de Certificados) y *LCA* (Autoridad Local de Certificados). El GCA supervisa el sistema IoV a nivel global, mientras que el LCA lo hace a nivel local.
- **Unidades de Carretera (RSU):** Las RSU son dispositivos ubicados a lo largo de la carretera, y actúan como mediadores para transmitir la información entre los vehículos (OBUs) y el LCA. Estas unidades también deben ayudar a verificar la identidad real de los OBUs y garantizar la transmisión segura de mensajes cifrados.
- **Unidad a Bordo (OBU):** El OBU es un dispositivo instalado en los vehículos. Debe estar registrado en el GCA con certificados, pares de claves y parámetros del sistema antes de unirse a IoV. El OBU es responsable de las operaciones de seguridad como la firma, el cifrado y el descifrado de datos, y transmite información periódica sobre la posición, hora, tráfico, velocidad, dirección y otros eventos importantes del vehículo.

5. Gestión de Claves en el Internet de Vehículos (IoV)

La gestión de claves en el Internet de Vehículos (IoV) es crucial para garantizar la seguridad en la transmisión de datos. Este estudio propone un esquema basado en árboles M (M-tree) para gestionar claves de forma eficiente y segura en un entorno dinámico como el IoV. A continuación, se describen los elementos principales del sistema y el esquema de gestión de claves.

5.1. Gestión de Claves con M-Tree

El esquema propuesto utiliza criptografía basada en curvas elípticas (ECC) y el acuerdo de claves de Diffie-Hellman (ECDH) para generar claves de sesión de manera eficiente. Los pasos principales son:

1. Cada vehículo genera un par de claves privadas y públicas (V_x, P_x) y utiliza ECDH para calcular una clave de sesión común con vehículos vecinos.
2. Las claves de sesión se transmiten jerárquicamente desde los vehículos hacia las RSUs, luego a las LCAs y finalmente a la GCA, que calcula la clave del sistema completo.
3. Ante cambios en la topología, como la salida de un nodo, solo es necesario recalcular las claves desde el nodo afectado hasta la GCA, reduciendo significativamente los costos computacionales.

5.2. Modos de Transmisión Segura

Para adaptarse a distintos escenarios, se proponen dos modos de transmisión segura:

- **Modo de Clave de Grupo:** Utilizado cuando los vehículos pertenecen al mismo RSU o LCA. Este método acelera la comunicación segura al emplear claves comunes.
- **Modo ECDSA:** Aplicado cuando los vehículos pertenecen a diferentes LCAs. Aquí se utilizan firmas digitales basadas en ECDSA para autenticar la identidad y proteger los datos transmitidos.

5.3. Transmisión Segura entre IoV y la Nube

El esquema también aborda la transmisión de datos desde el IoV hacia la nube utilizando una infraestructura PKI. Las etapas incluyen:

1. Solicitud de certificados por parte de los vehículos y las RSUs a la GCA.
2. Uso de firmas digitales ECDSA para autenticar la identidad y garantizar la integridad de los datos durante la transmisión.
3. Validación de la autenticidad de los datos en la nube mediante HMAC y algoritmos hash.

5.4. Arquitectura de Transmisión Segura en la Nube

Para operaciones como MapReduce en la nube, se emplea Kerberos para autenticar participantes y garantizar la seguridad. Se utilizan claves de sesión distribuidas por un centro de claves (GCA) para proteger las operaciones.

6. Análisis de Seguridad y Rendimiento

6.1. Verificación de Firma

La verificación de firma se asegura utilizando el algoritmo ECDSA, garantizando que la firma es correcta y que la identidad del emisor es validada.

6.2. Verificación de Identidad

El sistema garantiza que solo los participantes legítimos puedan obtener la clave de sesión mediante el uso de contraseñas secretas, evitando suplantaciones.

6.3. Confidencialidad en Comunicación V2V y V2G

- En la comunicación entre vehículos (V2V), solo los vehículos que comparten una clave de sesión común pueden cifrar y descifrar los datos, asegurando la confidencialidad. - En la comunicación entre vehículos y grupos (V2G), solo los vehículos con la misma clave de grupo pueden participar, previniendo accesos no autorizados y garantizando la confidencialidad de los mensajes.

6.4. Escalabilidad del Sistema

El uso de un M-árbol dinámico permite gestionar las claves de grupo de manera eficiente, manteniendo una complejidad de tiempo $O(\log_M N)$, lo que asegura una buena escalabilidad incluso con un gran número de vehículos.

6.5. Eficiencia en la Gestión de Claves

Comparado con otros esquemas como B-tree y None-tree, el esquema M-árbol presenta mejores resultados en términos de costos de comunicación y operaciones al manejar la resincronización de claves.

6.6. Tiempo de Resincronización

El esquema basado en M-árbol es más eficiente que los esquemas GDH y DH, requiriendo menos tiempo para recalcular las claves del sistema cuando un vehículo se une o deja la red IoV.

7. Conclusiones

Gracias al desarrollo de la tecnología 5G, la conducción autónoma sin conductor está cada vez más cerca. Dado que el IoV opera en un entorno de comunicación abierto, la información personal está expuesta a la red inalámbrica, lo que convierte la seguridad de la información en un tema crucial.

El acuerdo propuesto para la gestión de claves de seguridad multinivel en IoV se basa en la estructura de un M-árbol, capaz de ajustarse dinámicamente a la topología cambiante de IoV. Este mecanismo acelera el tiempo de sincronización de la reconstrucción de la clave del sistema y reduce el número de fases necesarias para resincronizar la clave del sistema. Además, la gestión de claves multinivel es adecuada para entornos IoV flexibles y expansibles, reduciendo los costos operativos y de comunicación.

En comparación con un B-árbol, el M-árbol propuesto es más eficiente en la gestión de claves. Además, al emplear operaciones de adición y multiplicación en lugar de operaciones exponenciales complejas, se reduce la carga computacional de los dispositivos OBU y RSU, siendo más adecuado para IoV con recursos limitados de cálculo. Finalmente, el uso de una longitud de clave más corta en ECDSA proporciona un nivel de seguridad comparable al de Diffe-Hellman o RSA, asegurando la transmisión de datos entre los dispositivos de IoV y las plataformas de servicios en la nube.