PROTOCOLO DE AUTENTICACIÓN MUTUA ENTRE VEHÍCULO Y UNIDAD EN CARRETERA BASADO EN EL ALGORITMO DIFFIE-HELLMAN PARA UNA RED VANET

Julio César Betancourt Saucedo

Universidad Autónoma de Ciudad Juárez, División Multidisciplinaria de Ciudad Universitaria

al107473@alumnos.uacj.mx

Rafael Martínez Peláez

Universidad de la Salle Bajío, Facultad de Ingeniería en Computación y Electrónica

rmartinezp@delasalle.edu.mx

Pablo Velarde Alvarado

Universidad Autónoma de Nayarit, Área de Ciencias Básicas e Ingenierías

pvelarde@uan.edu.mx

Joel Ruíz

Universidad Estatal de Sonora, Departamento de Ingeniería de Software

joel.ruiz@ues.mx

Yesica I. Saavedra Benítez

Instituto Tecnológico de Toluca, División de Estudios de Posgrado e Investigación

ysaavedrab@toluca.tecnm.mx

Resumen

El proceso de autenticación es un componente clave para incrementar la seguridad en una red vehicular. La mayoría de los protocolos de autenticación propuestos en la literatura, se basan en criptografía asimétrica, y específicamente en el uso del algoritmo RSA. Además, se considera el uso de certificados digitales y una infraestructura de clave pública. Por lo tanto, el proceso de autenticación suele ser complejo. Con la intención de proponer una solución segura, sin el uso de certificado digitales y el algoritmo RSA, se presenta un protocolo de autenticación mutua basado en el algoritmo Diffie-Hellman para establecer una

clave de sesión entre vehículo (OBU) y unidad de carretera (RSU). A partir de la clave de sesión, se puede establecer un canal de comunicación seguro para transmitir el identificador de cada participante y los respectivos parámetros de seguridad. Para realizar el proceso de autenticación, las entidades realizan operaciones de bajo costo computacional, como son funciones hash y XOR. Una vez concluido el protocolo de autenticación mutuo, el vehículo y la unidad de carretera podrán intercambiar mensajes de manera segura.

Palabra(s) Clave(s): algoritmo Diffie-Hellman, autenticación mutua, intercambio de claves, registro de vehículos, VANET.

1. Introducción

De acuerdo a información proporcionada por el Instituto Nacional de Estadística y Geografía, el número de accidentes de tránsito terrestre en las zonas urbanas del país fue de 378,240 durante el año 2014. El 1.1% de dichos accidentes fueron fatales, se perdieron 4,708 vidas. En este sentido, la Organización Mundial de la Salud estima que 1.24 millones de personas pierden la vida a causa de accidentes de tránsito cada año [1]. En consecuencia, se han realizado diversos esfuerzos para reducir el número de accidentes de tránsito terrestre, entre las que se encuentran: sanciones legales más severas, operativos de tránsito, y desarrollos tecnológicos.

Uno de los desarrollos tecnológicos que más ha llamado la atención es la red ad-hoc vehicular o *vehicular ad-hoc network* (VANET) [2]. La red VANET tienen su origen en las redes inalámbricas que han ganado bastante popularidad entre los empresarios y usuarios debido a la comodidad de poderse conectar a la red de redes desde cualquier lugar y en cualquier momento. Además, se ha mejorado la tasa de transferencia y la distancia de alcance de las comunicaciones inalámbricas, permitiendo el desarrollo de nuevas aplicaciones y servicios. También, se tiene que tener en cuenta los bajos costos relacionados con la adquisición de dispositivos y por conectividad. En conjunto, las redes inalámbricas son la base de nuevos desarrollos tecnológicos, como son: redes de sensores

inalámbricas, redes ad-hoc, redes móviles ad-hoc, y más recientemente el Internet de las cosas.

Las redes ad-hoc son redes que se comunican a través de un medio inalámbrico y sin la necesidad de una infraestructura; es decir, las redes ad-hoc se pueden establecer en cualquier lugar [3]. En el siguiente paso de evolución, se encuentran las redes móviles ad-hoc. A diferencia de su predecesor, las redes móviles ad-hoc son capaces de adaptarse a los cambios de topología a través de protocolos de enrutamiento proactivos y reactivos. En vista de su versatilidad y rendimiento, se produjo la adaptación a redes vehiculares.

Las redes vehiculares requieren de una unidad a bordo u *on board unit* (OBU) y un componente de infraestructura de carretera o *road side unit* (RSU) [4]. A través de la OBU, el vehículo se puede comunicar con otros vehículos (comunicación OBU-OBU) a lo largo de una carretera o con la RSU (comunicación OBU-RSU). En conjunto, se busca mejorar la experiencia de manejo de las personas, haciendo más seguro el camino y con mejores rutas.

Sin embargo, las redes vehiculares son propensas a ser atacadas [5] debido al medio de comunicación, movilidad y falta de procesamiento en la OBU. En consecuencia, un atacante puede generar e inyectar paquetes con información falsa a la red, generando problemas de vialidad. Para incrementar la seguridad en una red vehicular, se han propuesto mecanismos de autenticación que limiten el intercambio de paquetes entre usuarios legítimos, en alguno de los escenarios existentes: OBU-OBU y OBU-RSU.

En [6], se propone un esquema de autenticación basada en infraestructura, donde se usa un sistema de autenticación mutua entre RSU y OBU. Tiene como principal característica preservar la identidad del vehículo. El proceso de autenticación se lleva a cabo mediante el intercambio de claves públicas, certificados digitales e información cifrada. La desventaja de este esquema es el alto costo de almacenamiento y procesamiento computacional.

En [7], se propone un esquema basado en criptografía simétrica, gracias a este procedimiento, se reduce el procesamiento computacional; sin embargo, el receptor no puede comprobar si dicha entidad es quien dice ser.

En [8], se utiliza un sistema de grupo de claves aleatorias para autenticar a los vehículos con la *RSU*, pero este esquema no cuenta con una autoridad confiable o *trusted authority* (TA), siendo más probable que las unidades mientan sobre su verdadera identidad.

En el presente trabajo se propone un protocolo de autenticación entre OBU-RSU utilizando el protocolo de intercambio de clave presentado por Diffie-Hellman en 1976 [9] y operaciones de bajo costo computacional, como son funciones hash [10] y XOR.

El artículo se encuentra estructurado de la siguiente manera. En la sección 2, se describen los conceptos básicos de una red vehicular. En la sección 3, se describen los supuestos y la nomenclatura. En la sección 4, se introduce el proceso de registro de la OBU. En la sección 5, se presenta la propuesta del protocolo de autenticación. En la sección 6, se realiza el análisis de seguridad del protocolo propuesto. Finalmente, se presentan las conclusiones del artículo en la sección 7.

2. Redes Vehiculares: Conceptos Básicos

En la actualidad, los vehículos se han convertido en "computadoras motorizadas" o "redes motorizadas", donde la comunicación vehículo a infraestructura cada vez es más importante. Por lo tanto, los vehículos deben ser equipados con herramientas que sean capaces de establecer una red VANET estable y segura.

Componentes de una red vehicular

Los principales componentes de una red vehicular son: OBU, RSU y TA [4]. A continuación, se describe cada componente con sus principales características:

- OBU [4]: unidad de comunicación que tiene la funcionalidad de procesar y gestionar la información recibida para su transmisión. Una OBU debe ser capaz de enviar y recibir información otros OBUs y/o RSUs, manteniendo de esta manera un viaje seguro de los conductores. Las unidades se encuentran equipadas con una EDR (registrador de datos de eventos,

graba información sobre percances o accidentes), GPS (sistema de posicionamiento global), interfaz de comunicación inalámbrica de bajo alcance, y cuenta con un ancho de banda de 75 MHz en una banda de 5.850 - 5.925 GHz [6]. La se alimenta con la energía proporcionada por la batería del vehículo. Las OBUs se encuentran limitadas en el poder de procesamiento y poder de transmisión. Es importante mencionar que, la OBU tiene que registrar toda su información y clave privada en una Autoridad Confiable [11].

- RSU [4]: son unidades estáticas que se encuentran en las inmediaciones de la carretera, no están en movimiento. La RSU provee apoyo en la autenticación de mensajes con las OBUs, logrando así el menor uso de procesador y de memoria en los vehículos. Este tipo de unidades no tienen restricciones en cuanto a poder de procesamiento, energía y poder de transmisión. Estas unidades se encuentran estratégicamente localizadas a una cierta distancia de la carretera y de unas a otras, similar a un punto de acceso en una red convencional, para proveer información y comunicación a las OBUs y otras RSUs. Algunas de estas unidades se encuentran conectadas a una red troncal centralizada [11].
- TA [11]: este componente puede ser una autoridad de certificación (CA), división de vehículos motorizados (MVD), etc. Este tipo de componentes gestionan y verifican las credenciales. Estos centros no deben ser comprometidos y deben permanecer lo más confiables posible [11].

Aplicaciones de las redes vehiculares

A continuación, se describe dos aplicaciones de las redes vehiculares en pro de la comodidad y seguridad del conductor. El escenario de estudio es la comunicación entre OBU-RSU.

Aplicaciones en la seguridad [12], [11]: se pueden dividir principalmente en tres campos;

- asistencia (geolocalización, manejo asistido con otros vehículos, cambio de carril seguro, etc.),

- información (aviso de obras públicas en el camino, despliegue de señales de tránsito), y
- advertencia (obstáculos o estado físico de la carretera, avisos sobre accidentes, etc.).

Esto se logra gracias a la información que recaban las RSUs y transmiten a vehículos (OBUs) al pasar cerca de ellas; esta comunicación debe ser directa y con el mínimo retraso posible, ya que, la información es muy importante para mantener al conductor bien informado.

Aplicaciones orientadas a la comodidad del usuario [13]: una RSU puede informar de promociones, realizar transacciones de pagos, y transmitir información comercial, sobre los establecimientos cercanos a la ruta del conductor. También, se pueden utilizar para descargar música o realizar compras en línea [14].

3. Preliminares

Debido a la complejidad de una red VANET, se ha tenido que realizar los siguientes supuestos:

- La *OBU* que desea ingresar a la red debe estar previamente registrado en la *TA*, de lo contrario la *RSU* rechazaría su petición de conexión al verificar que no está registrado en el sistema.
- La *RSU* no tiene limitaciones de energía, capacidad de procesamiento y almacenamiento.
- La *TA* es una entidad de confianza, tanto para la *RSU* como para la *OBU*.
- La comunicación entre la *TA* y la *RSU* es segura.
- La *TA* es un organismo que tiene la facultad de generar el identificador para cada *OBU*.
- La *TA* es la encargada de generar los valores g, p, W_{OBU}, Z_{OBU}.
- La *TA* almacena la información en un servidor seguro – se cifra la información o se cifra el disco duro.
- La *RSU* conoce los valores g, p.
- Las entidades participantes utilizan SHA-2 para calcular la función *hash*.

La tabla 1 presente la nomenclatura utilizada a lo largo del documento.

Tabla 1 Nomenclatura.

Nomenclatura	**Definición**
TA	Autoridad Confiable
RSU	Unidad en Carretera
OBU	Unidad a Bordo
ID	Identificador de la *OBU*
K_{RSU}	Clave secreta de la *RSU*
K_{OBU}	Clave secreta de la *OBU*
ΔT	Tiempo de validez de la clave de sesión
$H(\ )$	Función hash
ID	Identificador de la *OBU*
$h_i = H(\ )$	Resultado de una función hash que pertenece a la entidad *i*
G	Generador
P	Número primo
$\otimes$	Or-exclusivo
W_{OBU}	Número aleatorio para cada *OBU*
Z_{OBU}	Número aleatorio para cada *OBU*
R	Clave de sesión entre *OBU* y *RSU*
$A = E_R(\mathrm{m})$	Cifrado simétrico de un mensaje con la clave de sesión *R*
$D_R(A) = m$	Descifrado simétrico de un mensaje cifrado con la clave de sesión *R*

4. Registro de la OBU

Para que la *OBU* pueda recibir información de una *RSU*, se debe realizar el registro de la unidad. El proceso se divide en dos etapas. La primera etapa es crear el *ID* del vehículo y el segundo proceso es generar y almacenar los parámetros de seguridad en la *OBU* y en la *TA*. A continuación, se describen los dos procesos.

Generación del identificador

El usuario debe realizar el proceso de registro para poder ingresar a la red VANET. En dicho proceso, se generará el *ID* de la *OBU* y quedará registrada en la *TA*. La figura 1 muestra los componentes del *ID*. El proceso se describe a continuación:

- Paso 1: El propietario del vehículo debe asistir a las oficinas de la *TA* y presentar en físico la información del vehículo y su licencia de conducir.

- Paso 2: El personal de la *TA* corrobora el VIN (*Vehicle Identification Number*) y las placas del vehículo.
- Paso 3: El personal de la *TA* corrobora la legitimidad de la licencia de conducir.
- Paso 4: El personal de la *TA* genera el *ID* del vehículo combinando información del VIN, placas y licencia de conducir.

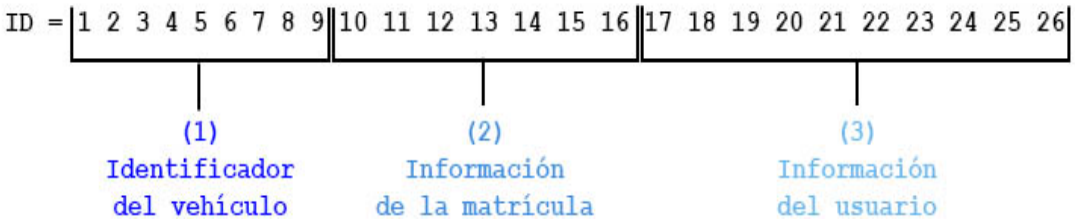

Figura 1 Componentes del ID del OBU.

A continuación, se detallan los tres componentes que dan origen al *ID* del vehículo. Cabe mencionar que, el proceso propuesto permitirá generar identificadores únicos, evitando la duplicidad en el sistema:

- Identificador del vehículo. Los primeros nueve dígitos del ID son tomados del VIN. El VIN se considera como la huella dactilar del vehículo. Los primeros tres dígitos informan sobre la identificación del fabricante (región en que fue ensamblado y el tipo de vehículo). Los siguientes cinco dígitos despliegan la descripción física del vehículo: peso o potencia del vehículo, tipo de vehículo (camioneta, van, coche, etc.), modelo en específico del coche, número de puertas, información del motor. Por último, se presenta un identificador que el fabricante autorizó.
- Información de la matrícula. Los siguientes siete dígitos del ID representan íntegramente la matrícula (placas) del vehículo. Las placas de vehículos que circulan en el interior de la república mexicana constan de siete dígitos, mientras que, las placas para vehículos que circulan en el Distrito Federal y áreas metropolitanas constan de seis dígitos. Las placas del vehículo permiten identificar si el vehículo se encuentra en orden para circular.

- Información del usuario. Los últimos diez dígitos del ID son los números de serie de la licencia de conducir del propietario del vehículo. Por medio de la licencia de conducir se puede relacionar al propietario con el vehículo.

Generación de parámetros de seguridad

Una vez concluido el proceso de registro, se tiene un *ID* por cada *OBU*; por lo tanto, se debe calcular parámetros de seguridad que permitan a las *RSU*, verificar la identidad de las *OBU*s. La *TA* realiza el siguiente procedimiento:

- Paso 1: CALCULA $h_{OBU} = H(ID)$.
- Paso 2: GENERA Z_{OBU} y $W_{OBU.}$
- Paso 3: CALCULA $h_{TA\text{-}OBU1} = H(Z_{OBU})$ y $h_{TA\text{-}OBU2} = H(W_{OBU})$.
- Paso 4: CALCULA $h_{TA\text{-}OBU3} = H(h_{TA\text{-}OBU1} \otimes h_{TA\text{-}OBU2} \otimes ID)$.
- Paso 5: CALCULA $C = h_{TA\text{-}OBU3} \otimes ID.$
- Paso 6: COMPARTE h_{OBU} con todas las *RSU.*
- Paso 7: ALMACENA g, p, h_{OBU}, $h_{TA\text{-}OBU1}$, $h_{TA\text{-}OBU2}$, $h_{TA\text{-}OBU3}$ en la *OBU.*
- Paso 8: ALMACENA *ID*, g, p, h_{OBU}, $h_{TA\text{-}OBU1}$, $h_{TA\text{-}OBU2}$, C en la *TA.*

5. Propuesta de Protocolo de Autenticación

El protocolo de autenticación se basa en el algoritmo Diffie-Hellman [9]. El protocolo consta de las dos primicias básicas de seguridad: autenticación mutua y establecer una clave de sesión.

Establecimiento de la clave de sesión

La *OBU* realiza los siguientes pasos:

- Paso l: GENERA $K_{OBU} > p$ en donde K_{OBU} se obtiene del reloj de la *OBU.*
- Paso 2: CALCULA $x = g^{KOBU} \bmod p.$
- Paso 3: ENVÍA $x \parallel h_{OBU}$ a *RSU* a través de un canal de comunicación abierto.

Una vez recibido la solicitud de autenticación ($x \parallel h_{OBU}$), la *RSU* verifica en la base de datos que se encuentre el h_{OBU}. En caso de no encontrarse se termina la comunicación; en caso contrario, se realizan los siguientes pasos:

- Paso 4: GENERA $K_{RSU} > p$ en donde K_{RSU} se obtiene del reloj de la *RSU.*
- Paso 5: CALCULA $y = g^{KRSU} \ mod \ p.$
- Paso 6: ENVÍA *y* a *RSU* a través de un canal de comunicación abierto.
- Una vez que ambas partes conocen los valores (*x*, *y*), se procede a calcular la clave de sesión.
- Paso 7: *OBU* CALCULA $R = y^{KOBU} \ mod \ p.$
- Paso 8: *RSU* CALCULA $R = x^{KRSU} \ mod \ p.$

Una vez calculada la clave de sesión *R*, ambas partes pueden intercambiar información de manera segura a través de un canal de comunicación abierto. En este momento, la *OBU* y la *RSU* tienen la misma clave de sesión, pero aún no se ha realizado el proceso de autenticación mutua. Se ha verificado que la *OBU* se encuentra registrada en el sistema.

Autenticación mutua

Después de haber sido establecido este canal de comunicación seguro, se procede a realizar un *challenge-response* para verificar la identidad de cada uno. Inicialmente, la *OBU* utiliza la información almacenada por la *TA* de la siguiente manera:

- Paso 1: Calcula $D = h_{TA\text{-}OBU1} \otimes h_{TA\text{-}OBU2} \otimes h_{TA\text{-}OBU3}.$
- Paso 2: Genera un número aleatorio *V.*
- Paso 3: Calcula $E = h_{TA\text{-}OBU3} \otimes V.$
- Paso 4: Calcula $A = E_R (D \parallel E \parallel h_{OBU})$.
- Paso 5: ENVÍA *A* a *RSU.*

Una vez que *RSU* recibe el mensaje (*A*), la *RSU* procede a descifrar el mensaje y reenviarlo a la *TA*. Cuando la *TA* recibe el mensaje de la *RSU*, la *TA* procede a verificar la identidad de la *OBU*. El procedimiento es el siguiente:

- Paso 6: BUSCA en la base de datos h_{OBU} y obtiene los valores de *ID*, $h_{TA\text{-}OBU1}$, $h_{TA\text{-}OBU2}$, y *C*.
- Paso 7: CALCULA $h_{TA\text{-}OBU3} = C \otimes ID$

- Paso 8: CALCULA $h_{TA\text{-}OBU3}^{*} = h_{TA\text{-}OBU1} \otimes h_{TA\text{-}OBU2} \otimes D$
- Paso 9: COMPARA $h_{TA\text{-}OBU3}$?= $h_{TA\text{-}OBU3}^{*}$
- Paso 10: CALCULA $V = h_{TA\text{-}OBU3} \otimes E$
- Paso 11: CALCULA $V + 1$
- Paso 12: CALCULA $F = V + 1 \otimes \Delta T$
- Paso 13: CALCULA $G = h_{TA\text{-}OBU3} \otimes$ verificación de identidad de *RSU*
- Paso 14: ENVÍA $F \parallel G \parallel$ Respuesta = valida o invalida a *RSU*.

Una vez que la *RSU* recibe el mensaje ($F \parallel G \parallel$ Respuesta = valida o invalida), la *RSU* verifica la respuesta sobre la identidad de la *OBU*. En caso que la respuesta sea negativa, la *RSU* procede a eliminar la clave de sesión *R* y cancela la comunicación. En caso contrario, se procede a compartir la clave de sesión *R* con *RSU* vecinas. Posteriormente, la *RSU* procede a cifrar y enviar el mensaje con la clave de sesión *R*. Cuando la *OBU* recibe el mensaje de la *RSU*, la *OBU* procede a realizar los siguientes pasos:

- Paso 14: CALCULA $F = D_R(A)$
- Paso 15: CALCULA $V + 1$
- Paso 15: CALCULA $\Delta T = V + 1 \otimes F$
- Paso 16: CALCULA identidad de *RSU* = $h_{TA\text{-}OBU3} \otimes G$.
- Paso 17: VERIFICA identidad de RSU es positiva, se continúa utilizando la *R*, en caso contrario, la *OBU* cancela la comunicación y elimina la *R*.

Nota: El tiempo de validez de la clave de sesión para comunicarse con otras RSU se encuentra determinado por ΔT. Una vez haya expirado el tiempo de validez, la OBU deberá ser autenticada por otra RSU.

6. Análisis de Seguridad

En este apartado, se realiza el análisis de seguridad del protocolo de autenticación propuesto. A continuación, se presenta los objetivos alcanzados con el protocolo propuesto:

- El protocolo cumple con el proceso de autenticación mutua. En el paso 9, la *TA* se encarga de verificar la identidad de la *OBU* mediante la comprobación del conocimiento del valor $h_{TA\text{-}OBU3}$. Se recuerda que dicho valor es generado por la *TA* en el proceso de registro. Por otra parte, la *OBU* verifica la identidad de la *RSU* mediante el mensaje enviado por la *TA* en los pasos 16 y 17.
- El protocolo cumple con establecer una clave de sesión. Al finalizar la primera parte del protocolo ambas entidades pueden calcular la clave de sesión *R*. El proceso se basa en el algoritmo DH.
- El protocolo cumple con mantener un canal de comunicación seguro. A través de la clave de sesión *R* ambas entidades pueden cifrar la información y mantener la confidencialidad.
- El protocolo cumple con mantener el identificador dinámico en el proceso de autenticación. Debido a que la *OBU* genera un número aleatorio *V*, cada vez que va a ser autenticado, el identificador es dinámico se puede mantener oculta su identidad con las *RSU*.
- El protocolo cumple con definir el tiempo de vida de la clave de sesión. Una vez que el tiempo ΔT ha expirado, se solicitará a la *OBU* se vuelva a autenticar por la *RSU* en turno. De esta manera, se mantiene fresca la clave de sesión *R*.

A continuación, se explica la seguridad del protocolo en contra de ataques conocidos:

- Suplantación de identidad. En caso que un atacante o usuario mal intencionado decida realizar el ataque de suplantación de identidad deberá conocer la información almacenada en la *OBU* (g, p, h_{OBU}, $h_{TA\text{-}OBU1}$, $h_{TA\text{-}OBU2}$, $h_{TA\text{-}OBU3}$). Si bien es cierto que, el valor de g y p son conocidos por todos los miembros de la red VANET, los valores que se utilizan para autenticar la identidad de la *OBU* son $h_{TA\text{-}OBU1}$, $h_{TA\text{-}OBU2}$, $h_{TA\text{-}OBU3}$ y se asume que esa información se encuentra almacenada de manera segura. A pesar que un atacante pueda obtener el valor de h_{OBU} debido a que es enviado en texto

claro sobre un canal abierto, el atacante no podrá engañar a la *TA* porque no conoce los otros valores para demostrar que es la víctima.

- Robo de identidad. En caso que un atacante o usuario mal intencionado desee realizar el ataque de robo de identidad, se verá limitado al no poder conseguir la información almacenada en la *OBU* ($h_{TA\text{-}OBU1}$, $h_{TA\text{-}OBU2}$, $h_{TA\text{-}OBU3}$). Se recuerda que dicha información se encuentra oculta mediante el uso de operaciones or-exclusiva y funciones *hash*.
- Reenvío de información. En caso que un atacante o usuario mal intencionado decida utilizar mensajes enviados por la víctima en ocasiones pasadas, se encontrará limitado por el tiempo de validez de la clave de sesión *R*.
- Hombre en medio. En caso que un atacante o usuario mal intencionado decida escuchar el canal de comunicación, solo podrá conocer el valor de h_{OBU} al iniciar el proceso para establecer un canal de comunicación seguro.

7. Conclusiones y Trabajo Futuro

Se ha presentado un protocolo de autenticación mutua entre OBU-RSU basado en el algoritmo Diffie-Hellman y operaciones de bajo costo. En la propuesto, se establece un canal de comunicación a través del algoritmo Diffie-Hellman. Ese proceso es posible porque la OBU ha sido registrada previamente ante la autoridad correspondiente y entre los parámetros de seguridad recibidos, se encuentran *g* y *mod p*. Con la clave de sesión conocida por OBU y RSU, se puede cifrar información sensible por medio de un canal de comunicación abierto. La información sensible que intercambian OBU y RSU son los parámetros de seguridad entregados a la OBU en el proceso de registro. El proceso de verificación de la identidad de la OBU es delegada a la TA. La TA es la encargada de validar que, la OBU sea legítima en el sistema. Para llevar a cabo el proceso de verificación mutua, TA y OBU calculan operaciones XOR y funciones hash.

El análisis de seguridad ha demostrado que la propuesta es segura ante ataques conocidos y cumple con requisitos de seguridad, tales como: realizar autenticación mutua y generar una clave de sesión

Como trabajo futuro, se realizará un análisis de rendimiento y de tiempo de ejecución para conocer el beneficio de la propuesta en esa dirección.

8. Bibliografía y Referencias

[1] INEGI, Estadísticas a propósito del día mundial en recuerdo de las víctimas de los accidentes de tráfico. Instituto Nacional de Estadística y Geografía, Aguascalientes. 2015.

[2] O. Orozco, D. Chavarro, O. Calderón, “Impacto de la velocidad y modelo de movilidad en una comunicación de datos de una red vehicular”. Entre Ciencia e Ingeniería. Vol. 8. No. 15. 2014. Pp. 62-70.

[3] O. J. Calderón, V. M. Quintero, “Un nuevo aspecto de la movilidad: redes ad hoc – conceptos”. Revista Colombiana de Tecnologías de Avanzada. Vol. 1. No. 3. 2014. Pp. 59-64.

[4] P. Fernandes, U. Nunes, Vehicle Communications: a short survey. IADIS Telecommunications, Networks and Systems. 2007. Pp. 134-138.

[5] M. Raya, J. Hubaux, The security of vehicular ad hoc networks. Third ACM Workshop on Security of Ad Hoc and Sensor Networks, Alexandria, VA, USA. 2005.

[6] V. S. Brijesh Chaurasia, “Infrastructure based Authentication in VANETs”. International Journal of Multimedia and Ubiquitous Engineering. Vol. 6. No. 2. April 2011. Pp. 8-9.

[7] A. Perrig, R. Canetti, J.D. Tygar, D. Song, “The TESLA Broadcast Authentication Protocol”. RSA CryptoBytes. Vol. 5. No. 2. 2005. Pp. 2-13.

[8] Y. Xi, K. Sha, W. Shi, L. Schwiebert, T. Zhang, “Enforcing Privacy Using Symmetric Random Key-Set in Vehicular Networks”. Eighth International Symposium on Autonomous Decentralized Systems. 2007. Pp. 344 – 351.

[9] W. Diffie, M. Hellman, “New direction in cryptography”. IEEE Transactions on Information Theory. Vol. 22. Nº 6. 1976. Pp. 644-654.

[10] R. Housley, A 224-bit one-way hash function: SHA-224. Internet Engineering Task Force. 2004.

[11] J. Fuentes, L. Gonzalez-Manzano, A. Gonzalez-Tablas, J. Blasco, “Security models in Vehicular ad-hoc networks: a survey”. IETE Technical Review. Vol. 31. No. 1. 2014. Pp. 47-64.

[12] S. Sesay, Z. Yang, J. He, “A Survey on Mobile Ad Hoc Wireless Network”. Information Technology Journal. Vol. 3. No. 2. 2004. Pp. 168-175.

[13] R. Ramanathan, J. Redi, “A brief overview of ad hoc networks: challenges and directions”. IEEE Communications Magazine. Vol. 40. No. 5. 2002. Pp. 20-22.

[14] X. Liu, Z. Fang, L. Shi, “Securing vehicular ad hoc networks”. Second International Conference on Pervasive Computing and Applications. 2007. Pp. 424-429.

9. Autores

Julio César Betancourt Saucedo es egresado de la ingeniería en sistemas computacionales de la Universidad Autónoma de Ciudad Juárez. Sus áreas de interés son seguridad en redes vehiculares y redes.

Rafael Martínez Peláez es doctor por la Universidad Politécnica de Cataluña e ingeniero en sistemas computacionales por la Universidad del Valle de México en 2003 y 2010, respectivamente. Actualmente, es profesor investigador de tiempo completo en la Universidad de la Salle Bajío y miembro del Sistema Nacional de Investigadores (SNI) con el nombramiento de candidato. Sus áreas de interés son autenticación, seguridad en servicios electrónicos, y privacidad en redes sociales.

Pablo Velarde Alvarado es doctor y maestro en ciencias por el Centro de Investigación y de Estudios Avanzado del IPN e ingeniero en electrónica por la Universidad Autónoma de Guadalajara en 2009, 2001 y 1993, respectivamente. Actualmente, es profesor investigador de tiempo completo en la Universidad Autónoma de Nayarit y miembro del cuerpo académico de nuevas tecnologías aplicadas a la educación. Es miembro del Sistema Nacional de Investigadores (SNI) con el nombramiento de nivel I.

Joel Ruiz Ibarra es doctor y maestro en ciencias por el Centro de Investigación Científica y de Educación Superior de Ensenada e ingeniero en electrónica por el

Instituto Tecnológico de Sonora, en 2011, 2006 y 2004, respectivamente. Actualmente, es profesor investigador de tiempo completo en la Universidad Estatal de Sonora y miembro del Sistema Nacional de Investigadores (SNI.) con el nombramiento de candidato. Sus áreas de interés son protocolos de comunicaciones y redes inalámbricas de sensores.

Yesica Imelda Saavedra Benítez es doctora por la Universidad de Versalles e ingeniera en computación por el Instituto Tecnológico de Toluca en 2013 y 1997, respectivamente. Actualmente, es profesora de tiempo completo en el Instituto Tecnológico de Toluca y directora del laboratorio de investigación. Es miembro del Sistema Nacional de Investigadores (SNI) con el nombramiento de candidato. Sus áreas de interés son redes inalámbricas ad-hoc, redes de sensores y seguridad en redes inalámbricas.