Una aproximación sistemática a los problemas de ciberseguridad en las redes VANET

Arizaga-Silva, Juan A
Ingeniería en Sistemas Automotrices
Universidad Politécnica de Puebla
Juan C. Bonilla, Puebla
juan.arizaga@uppuebla.edu.mx

Alonso-Pérez, *Marco A*
Ingeniería en Sistemas Automotrices
Universidad Politécnica de Puebla
marco.alonso@uppuebla.edu.mx

Etcheverry, Gibran
Departamento de Computación, Electrónica y Mecatrónica
Universidad de las Américas Puebla
gibran.etcheverry@udlap.mx

López-Bárcenas, Mónica
Ingeniería en Sistemas Automotrices
Universidad Politécnica de Puebla
monica.lopez@uppuebla.edu.mx

Martín-Ortíz, Manuel
Laboratorio Nacional de Supercomputo
B.Universidad Autónoma de Puebla
manuel.martin@correo.buap.mx

***Abstract*—Intelligent transport systems (ITS), which will allow efficient and controlled management of vehicular traffic and urban mobility in general within the so-called "smart cities", are fundamentally based on the development of new communication technologies.**

The VANET networks (Vehicular Ad-hoc Network) are a type of Ad-Hoc networks or wireless distributed mobile networks that will increase safety for users and vehicles in various automotive environments (urban and road) because of the new services offered to drivers and pedestrians. As a result of the communications augmentation, many types of attacks can occur in this kind of network, where every constituent element will need a different cybersecurity approach.

This article presents the high-value elements within VANET networks and the cybersecurity threats which they could be exposed to.

Keywords— cybersecurity, VANET, threats, asset, automotive security

I. INTRODUCCIÓN

Los sistemas inteligentes de transporte (ITS), que permitirán una gestión eficiente y controlada del tráfico de vehículos y la movilidad urbana en general, dentro de las llamadas ciudades "inteligentes" se basan fundamentalmente en el desarrollo de nuevas tecnologías de comunicación.

Las redes VANET (*Vehicular Ad-hoc Network*) son un tipo especial de redes móviles (MANET) con una estructura de red *Ad-Hoc* o una red móvil inalámbrica distribuida que se ha desarrollado para aumentar la seguridad de los usuarios y vehículos en diversos entornos automotrices, así como también brindar nuevos servicios a los conductores. y peatones.

Hay muchos tipos de ataques que pueden ocurrir en una red VANET (amenazas a la confidencialidad integridad y autenticidad de la información, robo de identidad), cada elemento dentro de la red necesita un enfoque de ciberseguridad diferente según su naturaleza. Este artículo, en su primera parte, muestra los antecedentes inmediatos de las redes VANET, para después, desde el punto de vista de ciberseguridad establecer los elementos de alto valor tanto tangibles como intangibles, los activos (*assets*) que hacen de las redes VANET el blanco de ataques cibernéticos; por último se exponen los diferentes tipos de amenazas a los que pueden estar expuestos cada uno de los diferentes activos en la red.

II. ANTECEDENTES

A) Redes VANET

En los últimos años, los automóviles han dejado de ser considerados un medio de transporte para convertirse en centros de datos móviles con la intención de incrementar la seguridad de los pasajeros y prevenir accidentes [1] ; para esto se han diseñado una gran variedad de aplicaciones móviles lo que ha creado un nuevo mercado, ante la necesidad de transferir la información de los autos o los ocupantes a través de Internet u otro tipo de red. La nueva generación de automóviles será capaz de realizar conexiones con su entorno, a través de lo que se ha dado a conocer como redes vehiculares, estas conexiones son diversas en aplicaciones y de diferente naturaleza: entre vehículos (V2V), con la infraestructura (V2I), con los peatones (V2P), entre otras; todas ellas agrupadas con el nombre de VANET's. (*Vehicular Ad-Hoc Networks*)[2].

Las redes VANET son un tipo de redes *Ad-Hoc* o de redes móviles distribuidas de naturaleza inalámbrica, formadas por dos tipos de nodos: estáticos y móviles. Los nodos estáticos, son elementos fijos emplazados a lo largo de las carreteras llamados RSU (*Road-Side Unit*), cuya función es la de enviar, recibir y retransmitir paquetes para aumentar el rango de cobertura de la red pudiendo también ofrecer acceso a Internet. Los nodos móviles son los vehículos equipados con un dispositivo electrónico llamado OBU (*On Board Unit*) para poder comunicarse con otros vehículos o con las RSU. Estos tipos de nodos tienen la capacidad de enviar, recibir y retransmitir mensajes entre ellos[3].

B) Tipos de conexión en las Redes VANET

Se han definido diferentes tipos de conexiones o escenarios de comunicación en las redes vehiculares: la comunicación intervehicular o vehículo a vehículo (V2V), en la que los automóviles intercambian mensajes directamente, la comunicación vehículo a infraestructura (V2I), la comunicación vehículo a RSU (V2R) y la comunicación vehículo a Peatón (V2P) [4].

Vehículo a Vehículo (V2V: *Vehicle to Vehicle*): Este tipo de comunicación se refiere a la comunicación directa o basada en multisaltos entre vehículos en una red VANET. Esto significa que los vehículos funcionan como receptor, emisor y ruteador de información a través de la red.

Vehículo a Infraestructura (V2I: *Vehicle to Infrastructure*): El escenario de comunicación V2I hace referencia a la conexión existente entre los vehículos y la infraestructura (semáforos, luminarias, avisos, casetas de peaje) a lo largo de la carretera.

Vehículo a Peatón (V2P: *Vehicle to Pedestrian*): V2P hace referencia a la comunicación entre los nodos de una red VANET y los peatones que circulan en un ambiente urbano.

Directo en el Vehículo (DIV: *Direct in Vehicle*): la comunicación DIV es poco referenciada por la literatura y se da cuando dos o más unidades de aplicación (AU) en el mismo vehículo intercambian información entre ellas; un ejemplo de esto es un dispositivo dentro del automóvil compartiendo acceso a Internet a otros dispositivos.

Vehículo a la red eléctrica (V2G:*Vehicle to Grid*) es un sistema en el que los vehículos eléctricos se comunican con la red eléctrica para devolver electricidad a la red o acelerar la velocidad de carga del vehículo. Será un elemento en algunos modelos de autos que se conectan a la red y se utiliza como un modulador de red eléctrica para ajustar dinámicamente la demanda de energía.

Vehículo a Hogar (V2H: *Vehicle to Home*): escenario propuesto por la ITU (*International Telecommunication Union*) para la convergencia de Redes de Nueva Generación con redes VANET. Hace referencia a la comunicación entre un nodo de una red vehicular con un nodo de una red fija en el hogar a través de una infraestructura de red de próxima generación (*Next Generation Network*) NGN [5].

Todos los tipos anteriores son agrupados según la literatura en el tipo genérico (V2X) *Vehicle to everything*.

III. Ciberseguridad en Redes VANET

Las redes VANETs son redes auto-organizadas diseñadas para la comunicación entre vehículos. En una VANET, cada vehículo se define como un nodo de la red Mediante la OBU los vehículos son capaces de comunicarse de forma inalámbrica entre sí, así como con las unidades de la carretera RSU. Los automóviles cuentan además con una unidad de aplicación llamada AU (*Application Unit*), las AU hacen referencia a los dispositivos que muestran información al usuario. Generalmente se les da esta denominación a dispositivos como computadores portátiles, smartphones o pantallas

Se espera que las redes VANET soporten una amplia gama de aplicaciones prometedoras tales como servicios basados en la ubicación. Sin embargo, la naturaleza de la difusión del medio inalámbrico permitiría a un agente adverso espiar las comunicaciones que contengan los identificadores de nodo, y estimar las ubicaciones de los nodos de comunicación con suficiente precisión para rastrear los nodos [5-7].

La implementación de la seguridad en las redes VANET tiene desafíos únicos. El caso es más complicado debido a los diferentes requisitos de las distintas aplicaciones. La seguridad para la difusión segura de la información se requiere un enfoque diferente al requerido para aplicaciones de gestión del tráfico debido a que existen diferentes tipos de ataques que pueden ocurrir dentro de una red VANET.

La clasificación de los tipos de ataques dentro de la literatura especializada depende en gran medida del grupo de investigación por lo que en este artículo se mostrará una aproximación a los problemas de ciberseguridad basada en los activos (assets) presentes dentro de una red VANET

Ejemplos de la diversidad de clasificaciones se presentan a continuación: Los investigadores Du y Zhu proponen en su trabajo [8] un modelo de árbol de ataque donde asignan a cada nodo del árbol una probabilidad de sufrir un ataque por parte de un agente externo. La probabilidad en cada nodo depende de tres atributos: costo de ataque, dificultad técnica y dificultad de descubrimiento.

Kaur et al [9] presentan cinco diferentes categorías de ataques, aunque no muestran evidencia de por qué realiza esta división, antes bien cita trabajos anteriores [6,7,10]. Por otro lado, Tyagi y Dembla proponen solo dos clasificaciones de ataque, internos y externos, sin imponer un criterio explícito de dicha división[3].

Al igual que con otros sistemas, los desafíos de seguridad de los vehículos autónomos y las redes vehiculares se pueden clasificar en términos generales en ataques a la confidencialidad, integridad, privacidad y disponibilidad como lo mencionan Gerla y Reiher [11]; los otros sistemas a los que se refieren estos autores corresponden a sistemas ciberfísicos que soportan infraestructura crítica y sistemas de información gubernamental y empresarial donde es necesario asegurar los activos (valores tangibles e intangibles) de las organizaciones.

Esta diversidad de clasificaciones si bien ayuda a catalogar los distintos trabajos realizados desde diferentes ópticas no responde a las necesidades de la industria automotriz la cual ha desarrollado su propio marco de referencia[20].

Los activos son los objetivos potenciales de un atacante que son críticos para el correcto funcionamiento del sistema y los intereses de los grupos interesados , es decir, los elementos que deben protegerse. En otras palabras, la identificación de los activos debe estar alineada con los objetivos comerciales y los marcos regulatorios obligatorios.

Desde el punto de vista de ciberseguridad, los siguientes elementos son considerados activos dentro de las redes VANET [12]:

1) Usuario de la red VANET: Al ser una red concebida para incrementar la seguridad física de los automovilistas, éstos constituyen, junto con su información privada, el activo más importante de la red.

2) Intercambio de información: Al igual que otras redes, los usuarios de las redes Vehiculares también exigen seguridad en términos de integridad de datos, confidencialidad y disponibilidad (CIA por sus siglas en inglés: *confidentiality, integrity and availability*).

3) Vehículos: Dentro de las redes VANET los automóviles representan un activo importante por las tareas que realizan al interior de la red. Un vehículo en la actualidad más que un medio de transporte se ha convertido en un centro de datos móvil. Al interior del vehículo se encuentran los sensores que colectan la información que después será transmitida a través de la red utilizando la OBU hacia los nodos adyacentes al vehículo.

El automóvil puede también, como se ha mencionado anteriormente, transmitir, recibir y rutear paquetes de información hacia los demás elementos de la red.

4) Unidades en carretera (RSU) Este elemento sirve como puente entre el entorno de infraestructura y el entorno ad-hoc. En estos nodos se instalarán los sensores necesarios, las unidades de procesamiento y el sistema de comunicación para recibir información de otros nodos. Debido a su naturaleza estática es un activo con una alta probabilidad de ser atacado. Si la RSU se ve comprometida, los datos almacenados en el interior se ven comprometidos y no se puede garantizar la comunicación segura con la infraestructura.

5) Protocolos de comunicación de red: Las comunicaciones en una red VANET son por su naturaleza principalmente inalámbricas, el estándar de facto para comunicaciones vehiculares son las Comunicaciones Dedicadas de Corto Alcance (DSRC).

El DSRC se basa en la tecnología IEEE 802.11 y ha sido titulado bajo el nombre de IEEE 802.11p. Estas comunicaciones pueden incluir información de tráfico, información de accidentes, condiciones de la carretera, mensajes de seguridad entre vehículos,cobro de peaje, manejo a través del pago, etc. Otros dos estándares, el ASTM E2213-03 y el IEEE 1609.x conforman el estándar conocido como Acceso inalámbrico en entornos vehiculares (WAVE)[2].

Por otro lado las comunicaciones intravehiculares para conexión de los sensores y las ECU's del auto con la OBU se realizan a través del Bus CAN y Ethernet Automotriz.

6) Entidad central: La entidad central es otro nodo estático en la arquitectura VANET que incluye los servidores de aplicaciones que proporcionan diversas aplicaciones, como aplicaciones para evitar colisiones, actualizaciones del clima y el tráfico, etc.

La entidad central se encuentra en el dominio de la infraestructura y desempeña un papel vital durante la comunicación V2I donde los mensajes son recibidos primero por el servidor de aplicaciones. Autentica el mensaje recibido y lo reenvía a otros vehículos a través de una ubicación geográfica amplia[12].

7) Terceros en la red: Los terceros en la red representan a los distintos tipos de autoridades (policía y tránsito), los cuales se encuentran en la parte de la red VANET que representa la Infraestructura. También se incluye a los fabricantes de los automóviles, los cuales a través de canales dedicados de comunicación pueden tener acceso a la red intravehicular, al OBU o la Unidad de aplicación.

Es necesario asegurarse que los terceros sean confiables a través de algún elemento de seguridad, cuando esto sucede, son conocidos como TTP (*trusted third parties*)

IV. Amenazas de seguridad.

Esta sección presenta diversas amenazas potenciales para los activos de las redes VANET

A) Riesgos sobre los usuarios

A nivel de Usuario de la red las principales amenazas están relacionadas con la confidencialidad de la información personal del usuario así como su localización geográfica y otra información sensible.

Por ejemplo, se prevé que los servicios ofrecidos en VANET incluyan conexión a Internet y aplicaciones peer to peer para compartir archivos entre usuarios de la red. Un agente adversario podría generar aplicaciones maliciosas que sustraigan mayor información de los usuarios o que incluso pueda existir robo de identidad.

Otra amenaza hacia los usuarios de las redes VANET, como cualquier otra red es aquella basada en ingeniería social (*Physhing* o *spoofing*).

B) Amenazas a nivel de información

Siempre existen amenazas a la información donde el principal interés del atacante es comprometer su confidencialidad, integridad y autenticidad (CIA). Las amenazas a la información pueden explotarse siguiendo diferentes aspectos de seguridad

Al interior del vehículo, se ha comprobado que existen diversos ataques a las comunicaciones internas del vehículo, específicamente en el Bus de comunicaciones CAN [19], lo que podría dar lugar al envío de información errónea por parte de un usuario a los demás nodos de red, sobre todo en comunicaciones V2V y V2I, sobre diferentes aspectos relacionados a la velocidad y posición de un nodo móvil de la red[14].

C) Amenazas a la confidencialidad, integridad y disponibilidad de la información.

Un nodo de red puede actuar de manera maliciosa de diferentes formas, cada de una de ellas puede clasificarse como un intento de manipulación de la información.

Por ejemplo, cada nodo dentro de la red puede servir de puente como ruteador de la información entre dos nodos, cuando por algún motivo no conocido un nodo decide no retransmitir los paquetes de datos ante una solicitud es entonces cuando la disponibilidad de la información se ve alterada y la seguridad de los usuarios, automovilistas y peatones se ve en riesgo.

Por otro lado la confidencialidad de los paquetes de datos puede verse vulnerada al existir algún canal inalámbrico inseguro con un cifrado que resulte ineficiente[15].

De igual forma la integridad de la información se ve comprometida cuando un atacante externo puede alterar, modificar e incluso borrar paquetes de datos transmitidos entre varios elementos de la red.

Existen diversos vectores de potenciales amenazas a la información [10,12]:

- Escuchas de datos confidenciales.
- Ataque de interferencia (*Jamming*).
- Ataques de suplantación
- Ataques de hombre en el medio *Man in the middle*(MITM).
- Ataques de suplantación de identidad (*Spoofing*).

D) Amenazas a la infraestructura (RSU y Entidad central)

La infraestructura, siendo la entidad estática en VANET, es una de las ubicaciones favoritas para que un atacante lance diferentes ataques de red del tipo Denegación de Servicio (DoS) y del tipo Hombre en el medio (MITM), para generar alteración de mensajes en el canal y ataques de suplantación [17].

La forma de los ataques pueden ser del tipo[12,14,19]:

- Envío de mensajes comprometidos.
- Caída de mensajes.
- Fuga de datos en el canal cableado del *back-end.*
- Inundación de red con mensajes.
- Alteraciones de mensajes en ruta a otros vehículos a través de RSU y entidad central
- Ataques relacionados con la calidad (QoS) del mensaje

Como puede observarse en algunos dominios los tipos de ataques se superponen. Esto se debe a la naturaleza heterogénea de las redes VANET las cuales cubren diferentes tipos de protocolos, topologías y medios de transmisión

V. Conclusiones

En las últimas dos década, se han emprendido muchos proyectos VANET al rededor del mundo y se han desarrollado varios estándares VANET para mejorar las comunicaciones entre vehículos (V2V) y vehículo a otros (V2X). La existencia de redes VANET abre el camino para una amplia gama de aplicaciones y ha abierto la puerta a diversos riesgos de ciberseguridad.

En este trabajo se ha presentado una revisión de los elementos de alto valor dentro de las redes VANET; también se revisaron algunas de las principales amenazas de ciberseguridad en las que los investigadores han centrado su atención en los últimos años. Así como los diversos tipos de ataques que pueden surgir derivados de estas amenazas.

Referencias

[1] Jindal, V. and Bedi, P. “Vehicular ad-hoc networks: Introduction , standards , routing protocols and challenges” (2016).

[2] Arizaga-Silva J. Alonso-Perez M. Álvarez-González R., “Redes VANET Vehicular Ad-Hoc Networks, la conectividad de los autos. Primera parte.” 2018 Revista Visión Politécnica. Universidad Politécnica de Puebla.

[3] Tyagi and D. Dembla, “Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network,” Wireless Personal Communications, vol. 102, no. 1, pp. 41–60, May 2018.

[4] Al-Sakib Khan Pathan “Mobile ad hoc network and vehicular ad-hoc network security,” Security of self-organizing networks, CR Press. 2019

[5] Al-Sultan, S., Al-Doori, M. M., Al-Bayatti, A. H. & Zedan, H. A comprehensive survey on vehicular ad hoc network. J. Netw. Comput. Appl. 37, 380–392 (2014).

[6] Hoa La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey", International Journal on AdHoc Networking Systems, vol. 4, no. 2, pp. 1-20, 2014.

[7] J. Isaac, S. Zeadally and J. Cámara, "Security attacks and solutions for vehicular ad-hoc networks", IET Communications, vol. 4, no. 7, p. 894, 2010.

[8] Du and H. Zhu, “Security Assessment in Vehicular Networks,” SpringerBriefs in Computer Science, 2013.

[9] R. Kaur, T. P. Singh, and V. Khajuria, “Security Issues in Vehicular Ad-Hoc Network(VANET),” 2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI), May 2018.

[10] "VANET, its Characteristics, Attacks and Routing Techniques: A Survey", International Journal of Science and Research (IJSR), vol. 5,no. 5, pp. 1595-1599, 2016.

[11] M. Gerla and P. Reiher, “Securing the Future Autonomous Vehicle: A Cyber-Physical Systems Approach,” Securing Cyber-Physical Systems, pp. 197–220, Sep. 2015.

[12] Ahmad, F., Adnane, A. and N. L. Franqueira, V. (2016) “A Systematic Approach for Cyber Security in Vehicular Networks”. Journal of Computer and Communications, 4, 38-62.

[13] Nadeem Majeed, M. e. a. Vehicular ad-hoc networks history and future development arenas. ITEE J. (2013).

[14] A. A. Celes and N. E. Elizabeth, "Verification Based Authentication Scheme for Bogus Attacks in VANETs for Secure Communication," 2018 International Conference on Communication and Signal Processing (ICCSP), Chennai, 2018, pp. 0388-0392. doi: 10.1109/ICCSP.2018.8524540

[15] K. M. A. Alheeti, A. Gruebler and K. D. McDonald-Maier, "An intrusion detection system against malicious attacks on the communication network of driverless cars," 2015 12th Annual IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, NV, 2015, pp. 916-921. doi: 10.1109/CCNC.2015.7158098

[16] R. Shringar Raw, M. Kumar and N. Singh, "Security Challenges, Issues and Their Solutions For Vanet", International Journal of Network Security & Its Applications, vol. 5, no. 5, pp. 95-105, 2013.

[17] H. Doumenc, “Estudio comparativo de protocolos de encaminamiento en redes vanet,” tech. rep., Universidad Politecnica de Madrid, 2008.

[18] C. Campolo, A. Molinaro, & R. Scopigno (Eds.), Vehicular ad hoc Networks: standards, solutions, and research (Springter Int., 2015).

[19] Currie, Roderick. T. Hacking the CAN Bus: Basic Manipulation of a Modern Automobile Through CAN Bus Reverse Engineering, SANS Institute paper, Mayo 2017.

[20] Schmittner, C., Ma, Z., Reyes, C., Dillinger, O., Puschner, P.: Using SAE J3061for automotive security requirement engineering. In: Skavhaug, A., Guiochet, J.,Schoitsch, E., Bitsch, F. (eds.) SAFECOMP 2016. LNCS, vol. 9923, pp. 157–170.Springer, Cham (2016).https://doi.org/10.1007/978-3-319-45480-113.