Revista Eletrônica de Sistemas de Informação
ISSN 1677-3071

v. 17, n. 3

set-dez 2018

DOI: https://doi.org/10.21529/RESI.2018.1703

Sumário

Revista hospedada em: www.periodicosibepes.org.br
Forma de avaliação: *double blind review*

Esta revista é (e sempre foi) eletrônica para ajudar a proteger o meio ambiente, mas, caso deseje imprimir esse artigo, saiba que ele foi editorado com uma fonte mais ecológica, a *Eco Sans*, que gasta menos tinta.

This journal is (and has always been) electronic in order to be more environmentally friendly. Now, it is desktop edited in a single column to be easier to read on the screen. However, if you wish to print this paper, be aware that it uses Eco Sans, a printing font

MAPEAMENTO DA PRODUÇÃO CIENTÍFICA SOBRE A VULNERABILIDADE EM SISTEMAS AUTOMOTIVOS

VULNERABILITY IN AUTOMOTIVE SYSTEMS: A SYSTEMATIC MAPPING STUDY

(artigo submetido em dezembro de 2018)

Airton Zancanaro
Doutor em Engenharia e Gestão do Conhecimento pela Universidade Federal de Santa Catarina (UFSC) e Professor do Instituto Federal Catarinense, *campus* São Bento do Sul
airton.zancanaro@ifc.edu.br

Andréa Letícia de Sousa Tavares
Graduanda em Engenharia de Controle e Automação no Instituto Federal Catarinense, *campus* São Bento do Sul
andrealeticiatavares@gmail.com

ABSTRACT

The improvement of automotive technology and the beginning of the Internet of Things (IoT) bring ease and comfort to the user in maneuverability, braking, durability and safety. However, the involved connectivity also brings cyber attack concerns. This paper aims, through a bibliometric mapping, to identify journals, research groups, researchers and institutions that are developing research on the matter. A total of 63 papers were traced, 40 of which were published in conference proceedings, 21 in scientific journals and 2 as book chapters. The paper organizes information contained in the analyzed work, with the intent to help researchers interested in the matter to further develop their own research.

Key-words: vulnerability; mapping scientific production; system automotive.

RESUMO

O aperfeiçoamento da tecnologia automotiva e o começo da Internet das coisas (IoT) trazem ao usuário facilidade e comodidade na dirigibilidade, na frenagem, na durabilidade e na segurança. No entanto, a "conectividade" demandada está sujeita a ciberataques. O artigo visa a identificar publicações, grupos de pesquisa, pesquisadores e instituições que investem em pesquisas associadas ao tema, por meio de um mapeamento bibliométrico. Foram identificados 63 trabalhos, sendo 40 artigos publicados em conferências, 21 em revistas científicas e 2 capítulos de livros. O artigo procura sistematizar as informações contidas nos trabalhos analisados, com o intuito de auxiliar os pesquisadores interessados no assunto a avançar com suas pesquisas.

Palavras-chave: vulnerabilidade; mapeamento da produção científica; sistemas automotivos.

1 INTRODUÇÃO

No início desta década, atingiu-se a marca de um bilhão de veículos automotores terrestres (carros, motocicletas, ônibus, caminhões e assemelhados) produzidos. Nos últimos vinte anos, a tecnologia embarcada em carros tem sido incrementada principalmente pela diminuição dos custos dos circuitos integrados e, como consequência, a incorporação de um maior número de dispositivos eletrônicos nos veículos (SILVA, 2013).

Por muitas décadas, o avanço tecnológico nos carros esteve voltado ao aumento da velocidade máxima, mas na atualidade o objetivo principal é o conforto, a dirigibilidade, a frenagem, a durabilidade e a segurança. Por conta desta tecnologia embarcada e o surgimento da Internet das Coisas (IoT), Souza, Andrade e Tomioka (2015) afirmam que os veículos modernos estão se tornando cada vez mais conectados/interconectados, com autonomia parcial ou total, mas vulneráveis a ciberataques.

Os veículos autônomos ou semi-autônomos possuem unidades de controle eletrônico (ECU) para cada função do carro, como controle de injeção de combustível, oxigênio no motor, controle dos freios ABS, entre outros. Eles se utilizam de uma rede *ad hoc* (VANET) para comunicação entre os carros (V2V) e infraestrutura (U2I). Esta rede, é utilizada para transferência de dados, indicando por exemplo, a condição do tráfego, evitando congestionamento. A VANET é uma conexão aberta entre os veículos e pode ser invadida por meio de dispositivos próximos como *tablets*, notebooks ou *smartphones* (LIU; FANG; SHI, 2007).

Além da VANET, os ataques maliciosos podem ser realizados por outros meios, como conexões com leitores de CD (*Compact Disc*), Bluetooth, USB (*Universal Serial Bus*) e sistemas de monitoramento de pressão (YADAV *et al.*, 2016). Tais conexões permitem que intrusos, por meio do acesso sem fio a longas distâncias, consigam assumir o controle de diversos componentes do veículo, como freios, motores, luzes, buzinas, além de poder adulterar dados.

Quando bem-sucedidos os ataques podem colocar em risco a vida dos condutores e passageiros, já que é possível, por exemplo, realizar frenagens repentinas, alterar as coordenadas de rota do GPS para locais perigosos, ou assumir o controle do carro.

Apesar da emergência do assunto, percebe-se falta de pesquisas científicas atualizadas que realizem um mapeamento sobre as principais publicações, onde estão os grupos de pesquisa, quem são os principais pesquisadores e quais países e instituições estão investindo em pesquisas relacionadas a área de vulnerabilidade em sistemas automotivos.

Trabalhos desta natureza são conhecidos como estudos bibliométricos e têm como propósito fazer uma análise da produção científica de modo a identificar indicadores que possam retratar o desenvolvimento de uma determinada área do conhecimento (BUFREM; PRATES, 2005), oferecendo subsídios para outros interessados, que estão iniciado os estudos.

Na próxima seção são apresentados os procedimentos metodológicos utilizados para a realização da pesquisa. Depois, são apresentados os resultados e, por fim, as considerações finais do trabalho.

2 PROCEDIMENTOS METODOLÓGICOS

O estudo bibliométrico aqui apresentado, parte de uma análise dos trabalhos publicados sobre a vulnerabilidade em sistemas automotivos, sendo realizado em três fases: 1) Busca, seleção e catalogação dos trabalhos; 2) padronização dos trabalhos; e 3) análise e elaboração do documento final. Estas fases compreendem sete etapas, descritas na sequência.

2.1 ETAPA 1: DEFINIÇÃO DOS TERMOS DE BUSCA

Nesta etapa, o propósito é identificar aqueles trabalhos que tratam da vulnerabilidade em sistemas automotivos indexados em base científica. Para a realização das buscas optou-se por utilizar os termos na língua inglesa, para, a partir deles, identificar os principais trabalhos. Para a consulta, utilizou-se a seguinte expressão: ("*cyber threat*" OR *invasion* OR *vulnerability* OR "*cyber attacks*") AND (*car* OR *vehicu**).

2.2 ETAPA 2: BUSCA EM BASE DE DADOS CIENTÍFICA

As buscas foram realizadas na base de dados internacional Scopus, limitando os trabalhos a artigos publicados em revistas científicos, congressos, capítulos de livros e livros, nos idiomas inglês, espanhol e português, nos últimos 10 anos. A Scopus foi escolhida por ser de natureza multidisciplinar, reconhecida internacionalmente pela comunidade científica, por ser amplamente utilizada para estudos bibliométricos (BRAMBILLA; STUMPUF, 2012; REGOLINI; JANNÈS-OBER, 2013) e por ser "referência internacional para a medida da produção científica dos países" (PACKER, 2011, p. 29). Além disso, ela permite exportar os dados para o software de gerenciamento de referências bibliográficas Mendeley, em um formato padronizado.

2.3 ETAPA 3: EXPORTAÇÃO DO RESULTADO DAS CONSULTAS PARA O GERENCIADOR DE REFERÊNCIAS BIBLIOGRÁFICAS

As informações oriundas da consulta à base dados Scopus como título, autores, local de publicação e palavras-chaves foram exportadas para gerenciador de referências bibliográficas Mendeley, formando um conjunto único de artigos.

2.4 ETAPA 4: ADOÇÃO DE CRITÉRIOS PARA A SELEÇÃO DOS TRABALHOS

No gerenciador de referências bibliográficas foram aplicados os seguintes critérios para a seleção dos trabalhos, retirando os que: a) não possuíam autoria; b) envolviam custos para acessar o texto completo; c) o texto completo não foi localizado; d) estavam fora do contexto do estudo.

Optou-se por selecionar as publicações em inglês, devido a sua relevância na comunicação do conhecimento internacional. Já o espanhol e o português foram considerados devido à natureza geográfica e nacionalidade dos autores. Quanto à delimitação temporal das publicações, devido a atualidade do tema, optou-se em selecionar todos os trabalhos publicados nos últimos 10 anos, permitindo análises anuais completas.

2.5 COMPLEMENTO DE INFORMAÇÕES DOS REGISTROS

As informações referentes à afiliação dos autores e as referências bibliográficas não estão disponíveis nos metadados, gerando a necessidade de buscá-las diretamente no texto do artigo. Também foram complementadas informações referentes às palavras-chave. Para auxiliar neste processo, uma nova base de dados foi criada, utilizando o Microsoft Access. Cada item foi padronizado e os dados complementados manualmente. No caso das referências bibliográficas utilizadas nos artigos, foram descartadas aquelas que não possuíam a data de publicação ou acesso. O processo de padronização demanda tempo e é essencial para o estudo bibliométrico.

2.6 ETAPA 7: ANÁLISE DOS DADOS E ESCRITA DO RELATÓRIO FINAL

Com o conjunto final de trabalhos selecionado e padronizado, foi possível gerar consultas e imagens que melhor apresentam os dados. Os resultados foram descritos em um relatório final.

3 RESULTADOS

Nesta seção são apresentados os resultados obtidos a partir da análise e síntese das informações sobre o conjunto de trabalhos selecionados com base nos procedimentos descritos anteriormente.

3.1 DADOS BIBLIOMÉTRICOS GERAIS DA PESQUISAS

A pesquisa bibliométrica foi realizada em março de 2018, possibilitando a avaliação de trabalhos sobre o tema vulnerabilidade em sistemas automotivos, publicados no período de janeiro de 2008 até março de 2018. A Tabela 1 mostra um resumo dos processos de seleção que culminou no conjunto de 63 trabalhos analisados.

Dentre os 63 trabalhos selecionados, 40 são artigos publicados em conferências, 21 foram publicados em revistas científicas e 2 representam capítulos de livros. Todos foram publicados no idioma inglês. A Tabela 2 apresenta os dados gerais da pesquisa.

Tabela 1 - Processo de seleção dos trabalhos

Passo	Realizado	Número de trabalhos selecionados	
		Retirado	Mantido
1	Resultado da busca inicial na base de dados Scopus	-	823
2	Seleção dos artigos nos idiomas inglês, espanhol e português	47	776
3	Seleção dos trabalhos que são: artigos científicos, artigos publicados em conferências, livros e capítulos de livros	51	725
4	Retirada dos artigos sem autoria definida	46	679
5	Retirada dos artigos publicados antes de janeiro de 2008	153	526
6	Leitura do título, resumo, palavras-chave e retirada dos artigos fora do contexto do estudo	442	84
7	Retirada dos artigos que não disponibili-zam o texto completo de forma gratuita	21	63

Fonte: elaborada pelos autores

Tabela 2. Dados bibliométricos gerais da pesquisa

Dados bibliométricos	Frequência absoluta
Número total de trabalhos selecionados	63
Total de fontes de publicações (veículos em que foram publicados os trabalhos)	55
Total de autores	210
Total de instituições às quais os autores estão afiliados	96
Total de países das instituições dos autores	29
Total de palavras-chaves distintas utilizadas nos trabalhos	192
Total de referências distintas utilizadas para compor os trabalhos	1064

Fonte: elaborada pelos autores

3.2 TENDÊNCIAS TEMPORAIS

Ao analisar os 63 trabalhos identificados, observa-se pelo gráfico da Figura 1, que a houve poucas publicações sobre vulnerabilidade em sistemas automotivos até o ano de 2014.

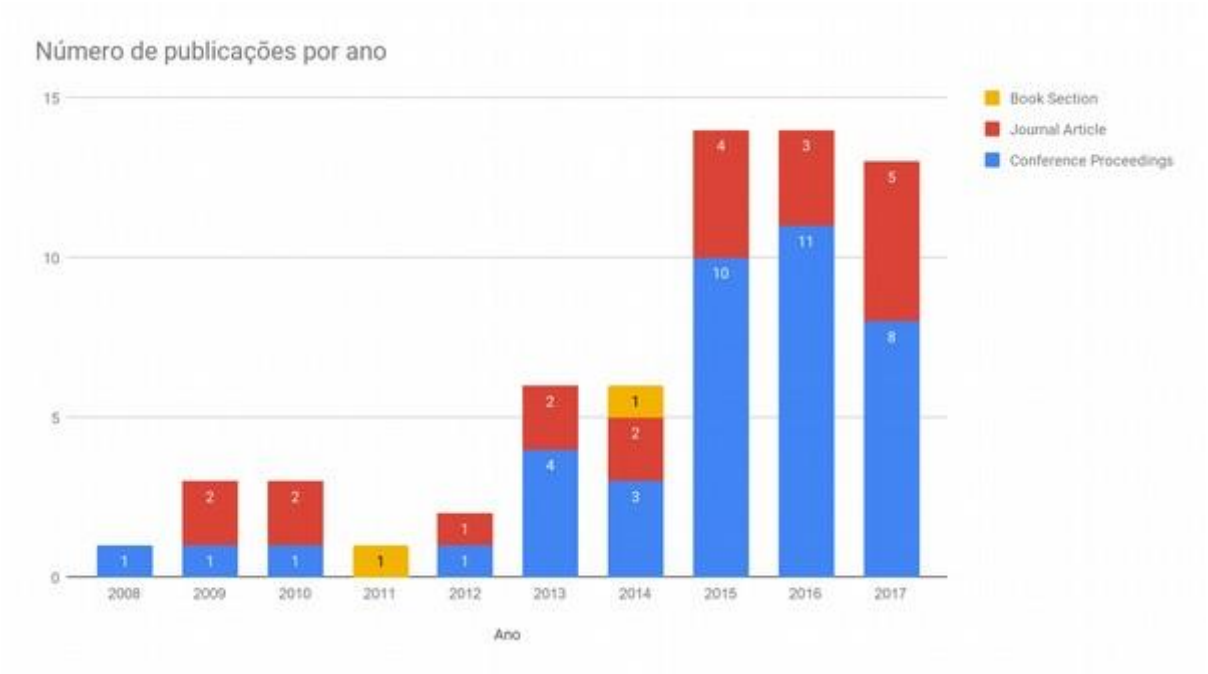

Figura 1. Número de publicações por ano

Fonte: elaborada pelos autores

O interesse maior pela temática surgiu a partir de 2015, com publicações principalmente em congressos, como o *International Conference on Connected Vehicles and Expo* (ICCVE).

3.3 PRINCIPAIS FONTES DE PUBLICAÇÕES

Dos 63 trabalhos selecionados, 21 foram publicados em periódicos científicos. Apenas dois desses periódicos tiveram mais de uma publicação sobre o tema no período analisado: o *Journal of Theoretical and Applied Information Technology* (JATIT) e o *IEEE Transactions on Vehicular Technology*. Ambos publicaram dois artigos sobre vulnerabilidade em sistemas automotivos. O primeiro deles é de acesso aberto, as publicações são mensais e está sediado no Paquistão. O segundo, também com publicações mensais, tem sede na *Tohoku University*, Japão.

No que diz respeito aos artigos publicados em conferência, destaca-se: *International Conference on Connected Vehicles and Expo* (ICCVE) com três artigos e, com dois artigos publicados cada, a *82nd Vehicular Technology Conference, a International Conference on Electro Information Technology* (EIT) e a *International Conference on Cyber Security of Smart Cities, Industrial Control System and Communication*.

3.4 PRINCIPAIS AUTORES E INSTITUIÇÕES

Pela análise da autoria dos trabalhos, foram identificados, na Tabela 3, os principais autores e, nas Tabelas 4 e 5, as instituições com maior números de autores e seus respectivos países.

Tabela 3. Atores com maior número de publicações e suas instituições

Autor	Total de trabalhos publicados	Afiliação do autor
Juan Deng	2	*Clemson University*
Richard R. Brooks	2	
Dietmar P. F. Möller	2	*Clausthal University of Technology (TUC)*
Ashwin Rao	2	*Carnegie Mellon University*
Roland E. Haas	2	*International Institute of Information Technology Bangalore*

Fonte: elaborada pelos autores

Jua Deng e Richard R. Brooks estão afiliados ao departamento de Engenharia Elétrica e Engenharia de Computação da Universidade de Clemson, EUA, atuando principalmente em pesquisas sobre cibersegurança e medidas para superar ataques de rede em grande escala. Já Dietmar P. F. Möller é professor do Instituto de Estocástica Aplicada e Pesquisa Operacional da *Clausthal University of Technology*, tendo como foco pesquisas voltadas à computação ubíqua, Internet das coisas, redes sociais, entre outros. Ashwin Rao, professor do Departamento de Ciências da Computação da *Carnegie Mellon University*, é pesquisador de temas voltados a V2V seguras e redes veiculares. Por fim, Roland E. Haas é afiliado ao *International Institute of Information Technology Bangalore*, na Índia, tendo como foco as pesquisas como gestão do conhecimento e gerenciamento de TI no setor automotivo.

Com base nas instituições em que os autores estão afiliados, foi possível gerar um mapa (Figura 2) mostrando os locais em que mais ocorrem pesquisas sobre a vulnerabilidade em sistemas automotivos.

Tabela 4. Instituições mais produtivas

Instituição	Total de autores afiliados	Cidade	País
Carnegie Mellon University	8	Pittsburgh	Estados Unidos
Clemson University	6	Clenson	Estados Unidos
University of California San Diego	6	San Diego	Estados Unidos
VIT University	6	Vellore	Índia
Deakin University	5	Geelong	Austrália
Penn State University	5	State College	Estados Unidos
University of Washington	5	Seattle	Estados Unidos
The Ohio State University	5	Columbus	Estados Unidos
Shanghai Jiao Tong University	5	Xangai	China
University of Luxembourg	5	Esch-sur-Alzette	Luxemburgo
International Institute of Information Technology Bangalore	4	Bengaluru	Índia
Khalifa University	4	Abu Dhabi	Emirados Árabes Unidos
University of Massachusetts	4	Dartmouth	Estados Unidos
University of Michigan	4	Ann Arbor	Estados Unidos

Fonte: elaborada pelos autores

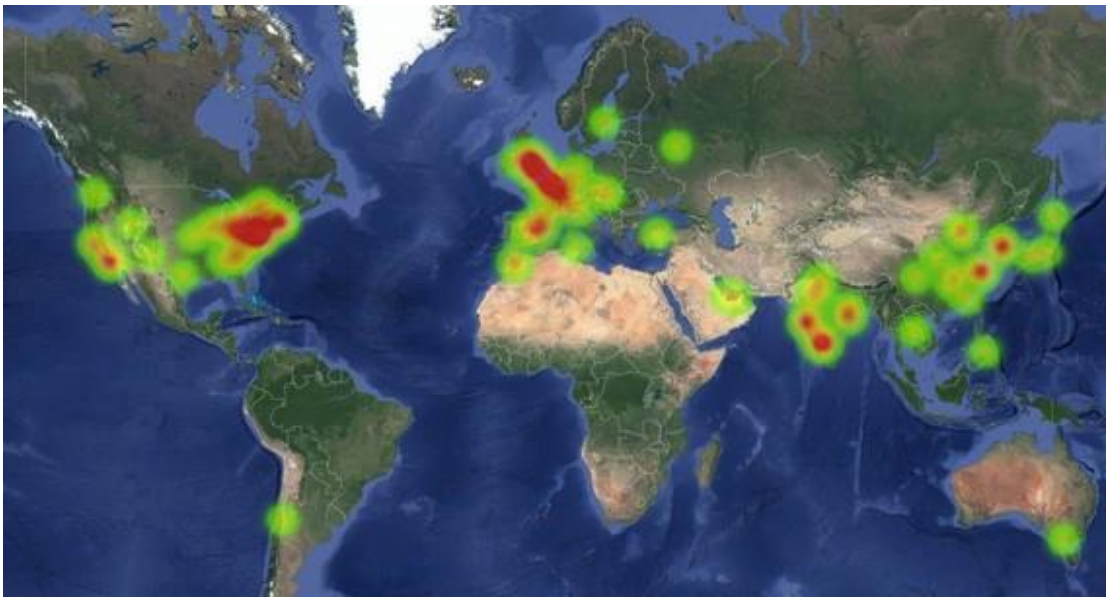

Figura 2. Mapa mundi mostrando a localização das pesquisas sobre vulnerabilidade em sistemas automotivos

Fonte: Elaborada pelos autores

Os pontos em vermelho representam a maior concentração de pesquisadores atuando sobre o tema. Nota-se que Estados Unidos, Índia e China são regiões de maior concentração de pesquisadores sobre o tema. A Tabela 5 apresenta o número de pesquisadores por país.

Tabela 5. Países com maior número de instituições

País	Número de instituições	Número de autores
Estados Unidos	27	79
India	12	24
China	10	14
UK	7	9
França	5	7
Espanha	4	10
Canadá	3	4
Japão	3	3
Coréia do Sul	2	6
Alemanha	2	2
Itália	2	3
Marrocos	2	5

Fonte: elaborada pelos autores

Na América do Sul, o único país que possui pesquisas sobre o tema é o Chile, com três autores afiliados à *Universidad de Chile*.

3.5 PRINCIPAIS PALAVRAS-CHAVE

Os 63 trabalhos considerados neste estudo utilizaram 192 diferentes palavras-chave. Os termos mais utilizados foram "*Vehicular ad hoc network* (VANET)", presente em 18 publicações, e "*Security*", em 16. A nuvem de *tags* ilustrada na Figura 3 apresenta as palavras-chave mais utilizadas.

Figura 3. Nuvem de palavras-chave

Fonte: elaborada pelos autores

3.6 PRINCIPAL REFERENCIAL TEÓRICO CITADO

Com base nos 63 trabalhos analisados, identificou-se que 1064 diferentes referências bibliográficas foram utilizadas pelos autores para compor as suas publicações. A Tabela 6 apresenta as principais referências.

A publicação *Comprehensive Experimental Analyses of Automotive Attack Surfaces* (CHECKOWAY *et al.*, 2011) envolve uma revisão de literatura sobre o comprometimento dos automóveis modernos, por meio de ataques remotos internos e externos. Os autores constatam que os ataques podem acontecer por meio de ferramentas mecânicas ou por meio de comunicação sem fio e discutem os desafios que estas vulnerabilidades trarão para o futuro dos veículos.

Experimental Security Analysis of a Modern Automobile (KOSCHER *et al.*, 2010) descreve a vulnerabilidade e a fragilidade dos automóveis modernos no que diz respeito a ataques cibernéticos. Apresenta, por meio de experimentos empíricos, as implicações dos ataques que comprometem as unidades de controle eletrônico (ECU), como o bloqueio do motor, freios, painel de instrumentos, entre outros. Constatam que estes ataques, quando bem-sucedidos, são ameaças significativas à segurança física dos condutores e passageiros dos veículos.

Tabela 6 – Referencial teórico

Autores	Ano de public.	Título	Núm. de citações
Stephen Checkoway, Damon McCoy, Brian Kantor, Danny Anderson, Hovav Shacham e Stefan Savage	2011	*Comprehensive Experimental Analyses of Automotive Attack Surfaces.*	23
Karl Koscher, Alexei Czeskis, Franziska Roesner, Shwetak Patel e Tadayoshi Kohno	2010	*Experimental Security Analysis of a Modern Automobile*	21
Xiaonan Liu, Zhiyi Fang, Lijun Shi	2007	*Securing Vehicular Ad Hoc Networks*	11
Ishtiaq Rouf, Rob Miller, Hossen Mustafa, Travis Taylor e Sangho Oh	2010	*Security and privacy vulnerabilities of in-car wireless networks: A tire pressure monitoring system case study*	11
Maxim Raya Panos Papadimitratos e Jean-pierre Hubaux	2006	*Securing vehicular communications*	8
Tobias Hoppe, Stefan Kiltz e Jana Dittmann	2008	*Security threats to automotive can networks — practical examples and selected short-term countermeasures*	8
Maxim Raya e Jean-Pierre Hubaux	2005	*The security of vehicular ad hoc networks*	7
Charlie Miller	2013	*Adventures in Automotive Networks and Control Units*	7

Fonte: elaborada pelos autores

Em *Securing Vehicular Ad Hoc Networks* (LIU; FANG; SHI, 2007), os autores abordam a rede que realiza a comunicação entre os carros e entre os carros e a estrada (VANET - *Rede Ad hoc Veicular*). Consideram que a segurança do sistema de transferência de informações é crucial para que os requisitos de autenticação, verificação da consistência dos dados, disponibilidade, identificação de causas de acidentes, privacidade e comunicação em tempo real sejam atendidos.

No artigo *Security and Privacy Vulnerabilities of In-Car Wireless: A Tire Pressure Monitoring System Case Study*, Rouf *et al.* (2010) avaliam a segurança do sistema que verifica a pressão dos pneus dos veículos. Por ser uma transmissão que ocorre por meio de uma rede sem fio, ela pode ser facilmente interceptada e mensagens podem ser enviadas remotamente para os sensores. Desta forma, os autores sugerem a implementação de práticas de segurança, como a implementação de criptografia.

Securing Vehicular Communications (RAYA; PAPADIMITRATOS; HUBAUX, 2006) apresenta uma análise sobre a vulnerabilidade veicular e as possíveis soluções. Além disso, sugere uma estrutura de como as comunicações veiculares (VC) podem ser protegidas e uma discussão sobre o protocolo IEEE 802.11 de ambientação da VC.

Na publicação *Security Threats to Automotive Can Networks — Practical Examples and Selected Short-Term Countermeasures* (HOPPE; KILTZ; DITTMANN, 2011), os autores relatam quatro experimentos (vidro elétrico, luzes de alerta, controle do *air bag* e central de comando) realizados nos sistemas de controle dos veículos com o propósito de identificar vulnerabilidades e as possíveis implicações destas vulnerabilidades para a segurança dos passageiros e condutores.

No trabalho intitulado *The Security of Vehicular Ad Hoc Networks*, Raya e Hubaux (2005) fazem uma análise sobre a segurança das VANETs (Rede *Ad-hoc*) utilizadas em projetos de sistemas de transportes inteligentes (ITS) e propõem medidas para tornar essas redes seguras no futuro.

Por último, no relatório técnico *Adventures in Automotive Networks and Control Units* (VALASEK; MILLER, 2014), os autores retratam as maneiras como um invasor pode interferir no comportamento de um automóvel após ataques realizados nas unidades de controle eletrônico (ECU) por meio da execução remota de códigos. Os testes foram realizados em dois carros e informações técnicas são apresentadas para entender como os ataques podem ser realizados e como se precaver.

4 CONSIDERAÇÕES FINAIS

Nesta pesquisa, buscou-se evidenciar estudos sobre os riscos dos ciberataques nos sistemas computacionais em veículos modernos. As buscas realizadas inicialmente trouxeram um grande número de publicações fora do contexto do estudo, tratando principalmente da proteção dos motoristas e passageiros contra acidentes. Isso demonstra ainda uma maior preocupação com a aparência, dirigibilidade, frenagem, durabilidade e segurança e pouca preocupação com a vulnerabilidade aos ataques cibernéticos e às consequências disso para os veículos e as pessoas que estão dentro dele.

Os resultados apresentados contribuem para uma visão ampla sobre a produção acadêmica a respeito da vulnerabilidade dos sistemas automotivos. Para tal, identificou-se os principais autores, em que locais ocorrem as pesquisas e quais são os grupos de pesquisa relevantes sobre o tema.

No que se refere as limitações da pesquisa, foram localizadas uma grande quantidade de artigos que estavam fora do contexto do estudo. Ampliar ou rever as palavras-chave para a busca nas bases de dados pode auxiliar na seleção de trabalhos com maior relevância. Outro limitador foi a busca em uma única base de dados. Sugere-se, para trabalhos futuros, a

realização de buscas em outras bases de dados e repositórios, com o propósito de melhor representar e ampliar as discussões sobre o tema.

REFERÊNCIAS

BRAMBILLA, S. D. S., & STUMPUF, I. R. C. Produção científica da UFRGS representada na Web of Science (2000-2009). *Perspectivas em Ciência da Informação*, v. 17, n. 3, p. 34-50, 2012.

BUFREM, Leilah; PRATES, Yara. O saber científico registrado e as práticas de mensuração da informação. *Ciência da Informação*, v. 34, n. 2, p. 9-25, 2005.

CHECKOWAY, Stephen; MCCOY, Damon; KANTOR, Brian; ANDERSON, Danny; SHACHAM, Hovav; SAVAGE, Stefan. Comprehensive experimental analyses of automotive attack surfaces. In: 20th Usenix Conference on Security, 20., San Francisco, EUA. *Proceedings...* p. 1-16, 2011.

HOPPE, Tobias; KILTZ, Stefan; DITTMANN, Jana. Security threats to automotive CAN networks: practical examples and selected short-term countermeasures. *Reliability Engineering & System Safety*, v. 96, n. 1, p. 11-25, 2011.

KOSCHER, Karl; CZESKIS, Alexei; ROESNER, Franziska; PATEL, Shwetak; KOHNO, Tadayoshi. Experimental security analysis of a modern automobile. In: Symposium on Security and Privacy, 1., 2010, Berkeley/Oakland, Ca, EUA. *Proceedings...* IEEE, p. 1-16, 2010.

LIU, Xiaonan; FANG, Zhiyi; SHI, Lijun. Securing vehicular ad hoc networks. In: International Conference on Pervasive Computing and Applications, 2., Birmingham, UK. *Proceedings...* IEEE, p. 1-6, 2007.

PACKER, A. L. *Os periódicos brasileiros e a comunicação da pesquisa nacional*. Revista da USP, n. 89, p. 26-61, 2011.

RAYA, Maxim; HUBAUX, Jean-Pierre. The security of vehicular ad hoc networks. In: 3rd ACM Workshop on Security of Ad Hoc and Sensor Networks, 3., Alexandria, EUA. *Proceedings...* p. 11-21, 2005.

RAYA, Maxim; PAPADIMITRATOS, Panos; HUBAUX, Jean-pierre. Securing vehicular communications. In IEEE Wireless Communications. 2006.

REGOLINI, A., & JANNÈS-OBER, E. A bibliometric study of informing science. *Informing Science: the International Journal of an Emerging Transdiscipline*, n. 16, p. 117-130, 2013.

ROUF, Ishtiaq; MILLER, Rob; MUSTAFA, Hossen; TAYLOR, Travis; OH, Sangho. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study. In: Usenix Security Symposium, 19., Washington, EUA *Proceedings...*. p. 1-16, 2010.

SILVA, Rafael Luiz da. *Caracterização do sinal do fenômeno de detonação utilizando filtros adaptativos e estimador de potência.* 2013. Dissertação

(Mestrado em Microeletrônica) - Escola Politécnica, Universidade de São Paulo, São Paulo, 2013.

SOUZA, Marcelo Pires de; ANDRADE, Ricardo de; TOMIOKA, Jorge. Vulnerabilidade em sistemas automotivos. In: *Anais do XXIII Simpósio Internacional de Engenharia Automotiva - SIMEA 2014* [Blucher Engineering Proceedings]. São Paulo: Blucher, p. 360-372, 2015.

VALASEK, Chris; MILLER, Charlie. Adventures in automotive networks and control units, *Def Con*, n. 21, p .260-264, 2014.

YADAV, Aastha*;* BOSE, Gaurav; BHANGE, Radhika; KAPOOR, Karan; IYENGAR, N.; CAYTILES, Ronnie D. Security, vulnerability and protection of vehicular on-board diagnostics. *International Journal of Security and its Applications*, v. 10, n. 4, p. 405-422, 2016.