XVI CEEL - ISSN 2178-8308
Universidade Federal de Uberlândia
05 a 09 de novembro de 2018

REDE CAN AUTOMOTIVA – PERSPECTIVAS GERAIS E VULNERABILIDADES

Pedro Ivo de Oliveira Tironi*[1], Felipe Machado Romeros[1], Gustavo Lobato Campos[1], Andrey Gustavo de Souza[2], Saulo Marques Torres de Carvalho[3].

[1]IFMG – Instituto Federal de Minas Gerais *Campus* Formiga.
[2]UFLA – Mestrando em Engenharia de Sistemas e Automação.
[3]Altran – ACT Consultoria em Tecnologia LTDA.

***Resumo* - A criação de um sistema de transmissão de dados para controle da arquitetura eletrônica automotiva é inicialmente motivada para simplificar o cabeamento sem comprometer a confiabilidade e a segurança do sistema. Diante disto, o objetivo deste trabalho é apresentar os principais aspectos da rede *Controller Area Network* (CAN) veicular, tais como contexto histórico, protocolos de transmissão e detalhamento deste processo. Assim como levantar avaliar questões de segurança e vulnerabilidade da rede CAN.**

***Palavras-Chave* - Rede CAN. Segurança. Sistemas automotivos.**

CAN BUS AUTOMOTIVE – GENERAL PERSPECTIVES AND VULNERABILITIES

***Abstract* -The creation of a data transmission system to control the automotive electronic architecture is initially motivated to simplify cabling without compromising system reliability and security. Therefore, the objective of this work is to present the main aspects of the network Controller Area Network (CAN), such as historical context, transmission protocols and detailing of this process. As well as raise evaluate security issues and CAN network vulnerability.**

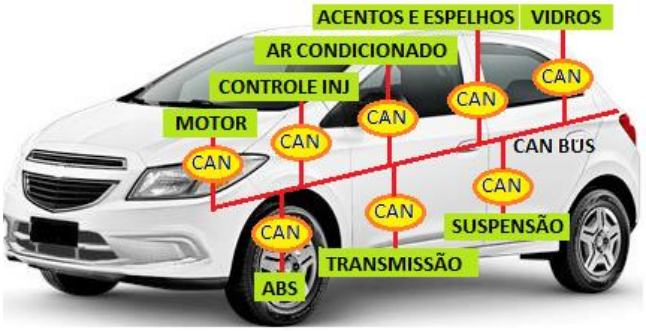
***Keywords* – CAN BUS. Security. Automotive Systems.**

I. INTRODUÇÃO

Com o crescente número de unidades de controle eletrônicas, ou ECUs (do inglês, *electronic central unit*), nos veículos aumentou também a quantidade de cabos e conexões para realizar a comunicação entre tais elementos, provocando frequentes erros, dificuldade na manutenção, assim como aumento do peso do veículo [1]. Assim, faz-se presente a necessidade de criação, ou desenvolvimento de um novo sistema de transmissão de dados para controle dessa nova arquitetura eletrônica automotiva com a presença cada vez mais crescente das ditas ECUs. Ou seja, teve-se como objetivo simplificar o cabeamento sem comprometer a confiabilidade e a segurança do sistema como um todo [2].

Diante de tal cenário, a multinacional alemã Bosch, na década de 80, desenvolveu o protocolo *Controller Area Network* (CAN) com finalidade de oferecer uma maior eficiência na comunicação entre centrais eletrônicas presentes nos automóveis, esquema representado na Figura 1. Isto atendendo a aspectos como segurança, elevada taxa de transmissão, robustez, precisão e baixo custo [3]

Figura 1: Esquema exemplificado da rede CAN em um veículo.



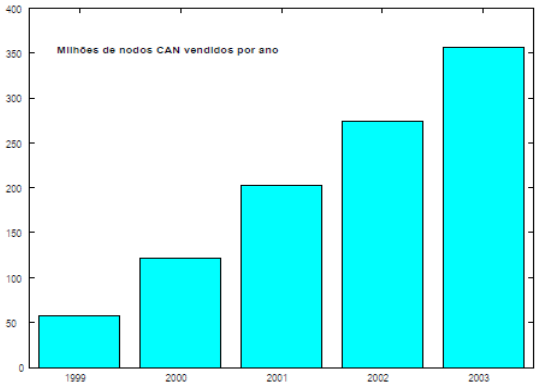
Como consequência do desenvolvimento do protocolo, já em 1987 empresas como Intel e Philips iniciaram a produção de controladores que representa o crescimento de vendas de chips do módulo CAN ao longo do tempo, tal qual demonstrado na Figura 2. Primeiramente, a empresa americana Intel desenvolveu o chip controlador CAN modelo 82526 e pouco tempo mais tarde a empresa Philips Semiconductors lançou no mercado o 82C200 [4], estes possibilitaram, em 1991, o desenvolvimento do primeiro veículo com a presença da rede CAN integrada. Implementado pela montadora Mercedes, o modelo S-W140 tinha por base cinco unidades de controle eletrônico [5].

Com o crescimento do uso da rede CAN, foi necessária uma padronização para promover e ampliar sua utilização. Além das especificações oferecidas pela Bosch, em 1993 a Organização Internacional de Normalização (ISO, do inglês *International Organization for Standardization*) definiu

*pedroivoexatas@gmail.com

inicialmente três padrões o ISO 118989-1, ISO 11898-2, ISO 11898-3 [3]. Ainda conforme o autor, no que se refere ao primeiro padrão, existem normas referentes as camadas de rede e a diferença entre os outros dois é a velocidade definida para aplicações, sendo que o segundo é direcionado a rede CAN de alta velocidade e o terceiro padrão para CAN de baixa velocidade.

Figura 2: Venda de Chips do módulo CAN por ano [6].



Posteriormente a estas normalizações, o protocolo foi amplamente utilizado em variados sistemas eletrônicos embarcados, assim a aceitação da rede CAN se tornou mundial, sendo que "quase todo carro fabricado nas regiões dos tratados comerciais, EMEA (*Europem, MiddleEast, and Africa*), NAFTA (*North American Free Trade Agreement*), LATAM (*Latin America*) e APAC (*Asia-Pacific*) empregam o barramento CAN" [3].

Deste modo, este artigo visa apresentar os principais conceitos vigentes sobre rede CAN automotiva por meio de uma revisão bibliográfica. Um dos objetivos deste trabalho é citar as principais características do protocolo CAN, descrevendo seu modo de operação e sistema de troca de mensagens. Pretende-se também realizar avaliação sobre questões de vulnerabilidade da CAN, fato discutido atualmente por montadoras e usuários [7].

II. CARACTERÍSTICAS E VISÃO GERAL DO PROTOCOLO

O emprego do protocolo CAN é embasado na solução para um tráfego de dados consistente, com bom controle de erros (distinção de erros temporários e falhas permanentes, detecção e sinalização de erros automaticamente) e tempo de latência (tempo suficiente para que todas as unidades eletrônicas recebam uma informação do barramento) bem definido.

Dentre estas características também devem ser citadas: a prioridade de mensagens, no qual um pacote de dados detém maior prioridade para acesso a rede que outro com menor prioridade; a flexibilidade de configuração, visto que podem ser inseridos ECUs com a rede em funcionamento e sem prévia configuração; e capacidade *multicast* que é o conceito no qual todos os módulos recebam a mesma mensagem, no entanto, somente o módulo no qual está destinado o sinal irá processar os dados e atuar conforme a função específica da unidade [1].

Fundamentalmente o protocolo CAN caracteriza-se por ser uma rede de comunicação no qual os nós se dispõem em um barramento e que possibilita o controle em tempo real, de modo que cada controlador tem a oportunidade de acessar o barramento enviando uma mensagem ou requisição, característica denominada como acesso multi mestre [8]. Essas mensagens são enviadas a uma taxa máxima de 1Mbits/s, fator inversamente proporcional ao comprimento físico do barramento [3].

III. *SOFWARE* E *HARDWARE*

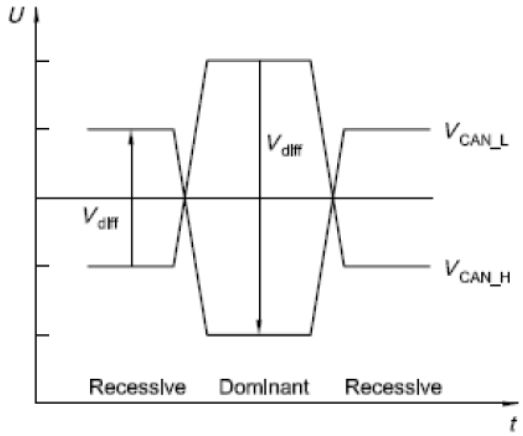
A rede CAN pode ser dividida em dois grupos para análise: *Hardware* e *Software*.

A. Hardware

A camada de enlace de dados é composto por uma linha de dois fios trançados (UTP, do inglês *unshielded twisted pair*) caracterizada por uma topologia em estrela, no qual sucede uma transmissão simétrica de tensões (vide Figura 3). No final de cada terminal existe um resistor de 120Ω conectados em paralelo. Estes são necessários para evitar reflexões de sinal [9], e assim garantir um casamento de impedância no sistema.

Em uma rede CAN, a transmissão física de sinais é fundamentada pela diferença entre as tensões dos dois cabos (CAN *high* e CAN *low*, representado pela Figura 3), fato que reduz os efeitos negativos das tensões induzidas por elementos como motores, o alternador, assim como outros sistemas elétricos (por meio da Lei de Biot-Savart). Por ser baseada na diferença de potencial (ddp), caso um campo magnético elevado afetar os cabos resultará em uma corrente induzida em ambos os fios (Lei de Faraday), porém a tensão induzida em ambos será homóloga, sendo igual e oposta em direção, gerando um cancelamento de efeito no campo e consequentemente condicionando a ddp [9].

Figura 3: Representação das diferenças de tensões entre a *CAN LOW* e a *CAN HIGH* [3].



A transmissão de dados é feita de maneira digital, ou seja, os valores lógicos são 0 e 1, definindo-se 0 para bit dominante e 1 para bit recessivo, fator que não se altera para normas distintas da ISO. Porém, a diferença de potencial entre as linhas CAN *high* (CAN_H) e CAN *low* (CAN_L) é diferente para padrões de baixa e alta velocidade [8]. Para o padrão ISO 11898-2, um bit recessivo apresenta ddp superior a 0,9 Volts

e um bit dominante apresenta ddp menor que 0,5 Volts. A Tabela 1 apresenta os valores de tensão máximos e mínimos para uma rede de alta velocidade [10].

Tabela 1: Valores de tensões para CAN de alta velocidade [10].

Bit	Notação	Unidade	Valor		
			Mínimo	Nominal	Máximo
Recessivo	V_{CAN_H}	V	2	2,5	3
	V_{CAN_L}	V	2	2,5	3
	V_{diff}	mV	-500	0	50
Dominante	V_{CAN_H}	V	2,75	3,5	4,5
	V_{CAN_L}	V	0,5	1,5	2,25
	V_{diff}	V	1,5	2	3

Para o padrão ISO 11898-3, um bit recessivo apresenta ddp superior a 2,2 Volts e um bit dominante apresenta ddp menor que 1,4 Volts. A Tabela 2 apresenta os valores de tensão máximos e mínimos para uma rede de alta velocidade de acordo com as especificações da ISO.

Tabela 2: Valores de tensões para CAN de baixa velocidade [11].

Bit	Notação	Unidade	Valor		
			Mínimo	Nominal	Máximo
Recessivo	V_{CAN_H}	V	4,7	-	-
	V_{CAN_L}	V	-	-	0,3
	V_{DIFF}	V	-5	-	-4,4
Dominante	V_{CAN_H}	V	-	-	1,4
	V_{CAN_L}	V	3,6	-	-
	V_{diff}	V	2,2	-	5

A velocidade de uma rede CAN pode chegar até 1Mbit/s fator inversamente proporcional ao comprimento físico do barramento, como mostra a Tabela 3 [3]. Logo deve ser considerado este parâmetro para a construção de projetos relacionados ao barramento CAN, pois seu desempenho decaí com o comprimento físico.

Tabela 3: Valores taxa de transmissão de bits pelo barramento em relação ao comprimento físico do enlace [3].

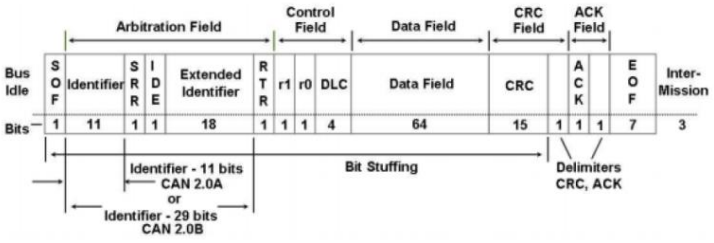
Velocidade de transmissão	Tempo p/ transmitir 1 bit	Comprimento do barramento
1 Mbit/s	1 µs	≤ 40m
500 kbit/s	2 µs	100 m
250 kbit/s	4 µs	200 m
125 kbit/s	8 µs	500 m
10 kbit/s	100 µs	6000 m

B. Software

Duas versões do protocolo CAN são mais utilizadas, a 1.0 e 2.0, ambas desenvolvidas inicialmente pela empresa Bosch, sendo que a versão 2.0 é dividida em duas variantes 2.0A (*Standard*) e 2.0B (*Extended*), a diferença primordial nas duas versões trata-se do número de bits nos identificadores, a versão 1.0 e 2.0A possuem 11 bits e a versão 2.0B pode ter tanto identificadores com 11 e 29 bits [8]. Ainda conforme o autor, fato negativo ocorre quando controladores CAN 1.0 recebem mensagens com o formato estendido gerando erros.

Avaliando a capacidade de circulação de dados um *frame* do tipo *Standard* pode ter até 2048 mensagens distintas, número baixo em virtude do grande número de ECUs existentes em automóveis atualmente, colocando limite no número de dispositivos e informações na rede, já o *frame* do tipo *Extended* permite o uso de 537 milhões de identificadores distintos. Estes *frames* possuem sete campos diferentes no *Frame* de dados, sendo ilustrado na Figura 4 [1].

Figura 4: Datagrama rede CAN [3].



A transferência destes conjuntos no barramento CAN é definida por quatro tipos de *frames*, sendo estes: *frame* de dados transporta os dados entre as ECU's; *frame* remoto, transmite solicitação para que outra ECU transmita um dado com um mesmo identificador; *frame* de erro, mensagem transmitida por qualquer ECU para informar um erro, seja temporário ou contínuo; e por último o *frame* de sobrecarga, gera uma série de atrasos específicos na transmissão de *frames*, quando a(s) ECU(s) entram em sobrecarga de mensagens e não conseguem processar [12].

O *frame* do protocolo CAN pode ser subdividido em sete camadas, sendo elas: campo de início do *frame*; campo de arbitragem; campo de controle; campo de dados; campo CRC; campo ACK; e o campo de fim do *frame* [3].

- Campo de início do *frame* (SOF, do inglês, *Start of Frame*): é um espaço de um bit (dominante) para indicar o início da mensagem, visto que o barramento inativo permanece em estado lógico "1" no qual não dissipa potência [3].

- Campo de arbitragem: é de grande importância para a largura de banda realmente disponível para a transmissão de dados [13]. Este campo consiste de em um identificador de 11 ou 29 bits e um bit de transmissão remoto (RTR do inglês, *remote transmission request).* Neste processo de arbitrariedade que ocorre sempre quando dois nós querem acessar o barramento. É resolvido por uma arbitração bit por bit, em uma situação que ambos tentam acessar o barramento é o utilizado o processo CSMA/CA (do inglês, *Carrier Sense Multiple Access With Collision Avoidance*) tendo preferência para o bit dominante acima do recessivo. Quando uma mensagem envia um bit recessivo e outra um bit dominante, a do bit recessivo perde o processo de arbitrariedade e muda seu estado para recepção [3].

- Campo identificador: é usado para estabelecer a prioridade da mensagem, no qual uma mensagem com

menor valor binário sobrescreve uma mensagem de maior valor.

- Campo RTR (requisição de transmissão remota): indica se a mensagem é um frame de dados ou se é um frame de requisição, caso dominante e recessivo respectivamente. O mesmo fator é usado para o Extended (SRR – substituto de transmissão remota) este sobrescreve o bit RTR, com bit dominante, pois não se envia frame remoto em formato Extended [8].

- Campo IDE (Identificador de extensão): indica se o formato da mensagem é *Standard* (caso for dominante) ou no formato *Extended* (caso for recessivo).

- Campo de controle: é dividido por bits reservados e DLC (do inglês, data *length code*). No caso de bits reservados no formato *Standard* é apenas um o r0 e no caso *Extended* existem dois bits reservados para modificações futuras (r0 e r1), são enviados em formato dominante. O DLC (4 bits) indica quantos bits terá a mensagem a ser enviada a seguir [8].

- Campo de dados: é preenchido com os dados que serão enviados, podendo ter de 0 a 64 bits. Nele é contida toda informação que será exposta no barramento, como por exemplo, informações referentes a condição de sensores e atuadores [3].

- Campo CRC (do inglês, *cyclic redundancy check*): é reservado para um controle de erros no envio das mensagens. No qual efetua um teste de redundância cíclica (15 bits) utilizando um polinômio identificador e mais um bit recessivo limitador no final da sequência. É gerado um erro do CRC quando o cálculo do receptor não for o mesmo que foi emitido, neste caso a mensagem é descartada e é enviado um *frame* de erro ao barramento.

- Campo ACK: são transmitidos dois bits (ACK *slot* e ACK *delimiter*), no qual o transmissor envia ambos em estado recessivo e caso ocorra algum erro durante a o processo de transmissão da mensagem a ECU que identificar indica ao barramento colocando um estado dominante no bit [8].

- Campo de fim do *frame*: é composto por 7 bits recessivos enviados no barramento, sinalizando assim o fim da mensagem.

Além do *frame* de dados existe também o *frame* de erro, remoto, e de sobrecarga. O *frame* remoto é semelhante ao *frame* de dados, porém não possui o campo de dados. Tem como função solicitar o envio de alguma mensagem de outra ECU Assim, as ECUs transmissoras podem atuar sob demanda, ou seja, não precisam ficar enviando seus dados a todo o momento. Para isso a central receptora envia um identificador igual ao da mensagem desejada.

O *frame* de erro é usado para indicar quando uma central está com defeito, ou quando uma unidade identificar um erro em uma mensagem, assim ela irá abortar a transmissão e enviar uma sinalização. Esta mensagem consiste em seis bits dominantes e oito bits recessivos.

O *frame* de sobrecarga é gerado para as centrais conseguirem escutar uma mensagem enviada no barramento que foi enviada em uma velocidade maior do que a de processamento [3].

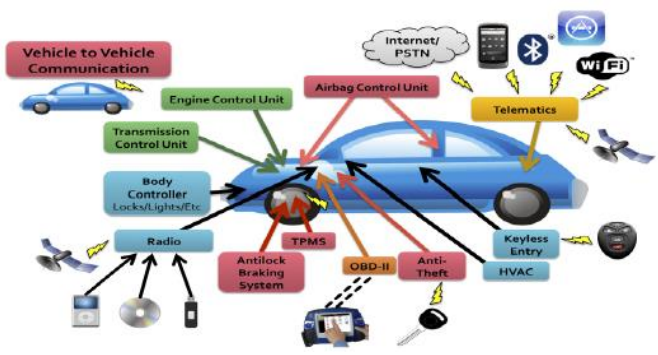
Dentro da mensagem além de cada processo descrito acima também existe o Bit *Stuff* que consiste em inserir um bit a cada cinco bits de mesmo valor. Ou seja, a cada cinco bits recessivos é inserido um bit dominante, fato inversamente análogo ocorre com bits dominantes. Quando a mensagem chega na central receptora e esta é encarregada de retirá-los. Este é basicamente composto por três campos: *flag* de sobrecarga, composto de seis bits dominantes, sobreposição das *flags* de sobrecarga, pode chegar a seis bits dominantes, e delimitador de sobrecarga que consiste de oito bits recessivos [13].

IV. SEGURANÇA E VULNERABILIDADE

Os automóveis que conhecemos hoje são o resultado de vários anos de desenvolvimento na área automobilística. Atualmente os veículos vêm sendo equipados com dispositivos eletrônicos telemáticos avançados e também com sistemas de controle completo, todos conectados pela rede interna CAN [14]. Conforme esse autor a rede CAN, pela sua característica de *broadcast*, torna acessível qualquer ECU por um único ponto de acesso e no caso de entrada à rede por um invasor todas as informações presentes no barramento veicular estarão disponíveis.

Para agravar mais ainda este problema, a superfície de ataque para automóveis modernos está crescendo rapidamente, quanto maior a sofisticação, maior são os recursos de comunicação incorporados nos veículos, implicando em mais pontos de acesso [15] (vide Figura 5). Subsistemas atualizáveis pelo usuário, como leitores de áudio são rotineiramente ligados à rede CAN veicular, assim como uma variedade de dispositivos de curto alcance sem fios (*Bluetooth*, sensores de pressão dos pneus sem fio (TPMS), Wi-Fi, etc.) [15]. Exemplos de sistemas telemáticos, são os recursos de resposta automática a acidente, de diagnóstico remoto e recuperação de veículos roubados, através de uma ligação sem fio de longo alcance, oferecidos pela General Motors (GM) *On Star* [15].

Figura 5: Superfícies de controle e comunicação de um veículo moderno com rede CAN [16].



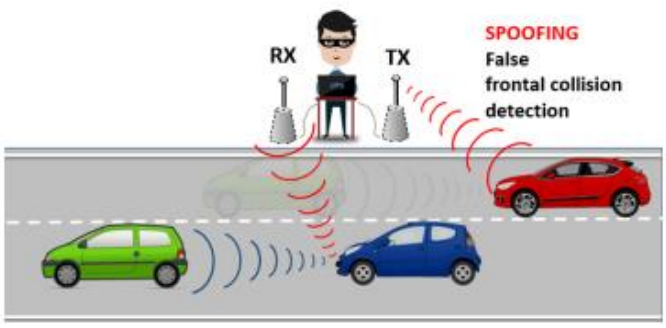
Os automóveis modernos são controlados por uma combinação heterogênea de componentes digitais que

supervisionam uma ampla gama de funcionalidades, incluindo o sistema de transmissão, injeção de combustível, freios, iluminação, entretenimento, entre outros. Na verdade, muito poucas operações não são mediadas pelo controle de computador, como o freio de mão [16]. Estima-se que um veículo de luxo moderno inclui de 70 a 100 ECUs no seu interior, todos conectados processando cerca de 100 milhões de linhas de código de *software*, segundo o professor de informática da Universidade Técnica de Munique e um especialista líder de *software* em carros Manfred Broy [17].

Análise de segurança cibernética atualmente vem sendo muito discutida e sempre foi uma questão de indiferença para os OEMs *(Original Equipment Manufacturer*). No entanto, devido à crescente ocorrência de invasões da rede CAN automotiva, a segurança desses sistemas se tornou fundamental [18]. Visto que a complexidade dos automóveis tente aumentar [17], leva o questionamento sobre o aumento das chances de falhas no código de *software*, no qual pode implicar que invasores com conhecimento nesse ramo usufruam e ataquem de forma maliciosa os veículos [15].

A vulnerabilidade da rede CAN está ligada aos seus pontos de acesso, que sistematizam no conjunto de métodos no qual se tem a comunicação com o barramento CAN, esses pontos podem ser por meios físicos diretos (portas OBD-II, RS-232, USB, etc.), acesso sem fio em curto alcance (*bluetooth*, Wi-Fi, TPMS, etc.), e também por acesso sem fio alongo alcance (Sistema de Posicionamento Global (GPS), Rádio por satélite, etc.)[16], conforme pode ser ilustrado pela Figura 6. Dentro de cada uma destas categorias, caracterizam uma superfície de ataque que expõe a segurança do barramento. Para cada meio de acesso, existe em profundidade um nível de exposição real e explorável que permitem o controle do automóvel sem a necessidade de acesso físico direto [16]. Na conferência Black Hat de segurança, realizada nos Estados Unidos em 2015, os pesquisadores Charlie Miller e Chris Valasek explicaram como invadiram o sistema de um Jeep Cherokee, demonstrando em detalhes que é possível invadir a rede CAN utilizando conexão Wi-Fi [19]. O portal G1 (2016), relatou outro caso de invasão, sendo o do automóvel da Tesla Model S, no qual por uma brecha na eletrônica deu abertura para que invasores chineses obtivessem o controle de seu sedã, em que pôde ser controlado em movimento e à distância, para isso foi invadida a rede CAN do automóvel pelo navegador conectando a uma rede Wi-Fi [20].

Figura 6: Ilustração de uma invasão por conexão sem fio [21].



Já existe um *software* (CarShark) que possibilita invasão do sistema de computador em carros, permitindo controle por meio de acesso direto, usando uma porta OBD-II [22]. Pesquisadores liderados por professores da Universidade de Washington e a USCD (Universityof California San Diego) conseguiram invadir a rede CAN por meio desse software para mostrar a vulnerabilidade desse sistema e também as infinitas possibilidades de sua utilização maléfica [22] tal como a inserção de códigos cíclicos de alta prioridade, fazendo que a CAN-BUS se sobrecarregue com mensagens falsas e deixe de realizar operações fundamentais do veículo, tal como a frenagem.

Logo, a questão sobre a vulnerabilidade veicular levanta pesquisas com o intuito de tornar os veículos modernos cada vez mais seguros. Neste contexto citam-se as seguintes iniciativas:

- Projeto EVITA (do inglês, *E-Safety Vehicle Intrusion Protected Applications*), que atuou de 2008 a 2011 foi co-financiado pela EU (União Europeia) com o intuito de projetar, verificar e prototipar uma arquitetura para automóveis e redes veiculares provendo segurança acerca dos componentes instalados nestas [23].

- Projeto PRESERVE, foi desenvolvido entre os anos 2011 e 2015, e teve por objetivo contribuir para questões referentes a segurança e privacidade veicular seja por comunicação veículo-veículo, V2V, ou por veículo-infraestrutura, V2I. Para isto foi abordado em seu desenvolvimento questões sobre escalabilidade, desempenho e capacidade de implementação destes sistemas de segurança, V2X [24].

V. CONCLUSÕES

O artigo demonstra como a rede CAN soluciona o problema enfrentado pelas montadoras no desenvolvimento dos veículos ao longo do tempo. A crescente demanda por mais tecnologia implementada nos veículos é barrada pela quantidade de cabeamento e conexões aplicados ao chicote automotivo. Desta forma, a rede CAN veicular é desenvolvida como solução viável para esse problema.

Com grande robustez, velocidade e tempo de latência garantido, a rede CAN ganha mercado e atualmente é aplicada em diversas áreas. No entanto em relação a questões de segurança, o protocolo CAN vem sendo questionado por fatos decorridos de invasões em seus sistemas por hackers, comprometendo a segurança dos usuários, visto que, atualmente, todos os veículos fabricados vêm sendo equipados com dispositivos telemáticos avançados. Como sugestão futura de pesquisa, propõe-se o estudo das falhas de segurança do protocolo CAN, com a finalidade de encontrar formas de minimizar as chances de invasões não autorizadas no barramento CAN.

AGRADECIMENTOS

A todos os integrantes do Grupo de Pesquisa CNPq, GSE (Grupo de Soluções em Engenharia), pela interação e colaboração no desenvolvimento do presente trabalho, assim como ao IFMG - *Campus* Formiga.

REFERÊNCIAS

[1] BARBOSA, L. R. G. Rede CAN. 2003. 14 f. Escola de Engenharia da UFMG (Universidade Federal de Minas Gerais), Belo Horizonte.

[2] SOUZA, Andrey Gustavo de; CAMPOS, Gustavo Lobato. Rede can veicular: levantamento bibliográfico e apresentação de conceitos iniciais. For Science: Revista Científica do IFMG,Formiga, v. 5, n. 1, e00234, jan./jun. 2017.

[3] CARVALHO, S. M. T. de. Avaliação do método *worst case response time* para o cálculo do tempo de resposta em mensagens CAN. 2017. 87 f. Trabalho de conclusão de curso - Instituto Federal de Minas Gerais, 2017.

[4] CAN-CIA.ORG. History of CAN technology. Disponível em: https://goo.gl/sWLf2m. Acesso em: 8 Jan. 2018.

[5] CAN NEWSLETTER. (2015). Mercedes W140: First car with CAN. Disponível em: https://goo.gl/fWCfwt. Acesso em: 9 jan. 2018.

[6] JOHANSSON, K.H.; TORNGREN, M.; NIELSEN, L. Vehicle Applications of CAN. Disponível em:< https://goo.gl/c7i4pY >. Acesso em: 17 Jul. 2018.

[7] GAZETA DO POVO. (2018). Montadoras de carros começam a se preocupar com possíveis invasões hackers. Disponível em: https: https://goo.gl/tupRih. Acesso em 25 Jul. 2018.

[8] MARQUES, M. A. CAN Automotivo: Sistema de monitoramento. 2004. 150 f. Dissertação programa de pós-graduação (Mestrado em Engenharia Elétrica) — Universidade Federal de Itajubá. 2004.

[9] VECTOR.COM. (2017). VECTOR E-LEARNING. Disponível em: https://goo.gl/5F2sbh. Acesso em 9 jan. 2018.

[10] ISO.INTERNATIONALORGANIZATION FOR STANDARDIZATION. ISO11898-1, Roadvehicles – Controller area Network (CAN)–Part 1: Data link layer and physical signaling, 2003a.

[11] ISO.INTERNATIONALORGANIZATION FOR STANDARDIZATION. ISO11898-2, Roadvehicles – Controller area Network (CAN) – Part 2: High-speed medium access unit, 2003b.

[12] FRESCALE. CAN Bosch Controller Area Network (CAN) Version 2.0 Protocol. 1998. Disponível em: http://www.nxp.com/assets/documents/data/en/reference manuals/BCANPSV2. Acesso em: 18 Jan. 2018.

[13] KVASER. (2017). CAN Protocol Tour by Kvaser. Disponível em: https://www.kvaser.com/can-protocol-tutorial/. Acesso em 11 Jan. 2018.

[14] SAMPATHI, R.Gone in 60 Seconds – FBI underlines Cyber Security Threat for Cars!!! LinkedIn. 2016. Disponível em: https://goo.gl/v2eHwm. Acesso em: 18 Jan. 2018.

[15] KOSCHER, K. et al. Experimental Segurity Analysis of a Modern Automobile. IEEE Symposium on Sucurity and Privacy. Estados Unidos da América, 2010.

[16] CHECKOWAY, S. et al. Comprehensive Experimental Analyses of Automotive Attack Surfaces. Estados Unidos da América, 2011.

[17] CHARETTE, R.N. This Car Runs on Code. IEEE Spectrum, 2009. Disponível em: https://goo.gl/Zw7xZ1. Acesso em: 25 Abr. 2018.

[18] YOSHIDA, J. CAN Bus Can be Encrypted, Says Trillium. EETimes. 2015. Disponível em: https://goo.gl/fHeEPx. Acesso em: 18 Jan. 2018.

[19] DROZHZHIN, A. Black Hat USA 2015: The full story of how that Jeep was hacked. Kaspersky. 2015. Disponível em: https://goo.gl/uPGZDD. Acesso em: 18 Jan. 2018.

[20] G1. Hackers chineses conseguem controlar carro da Tesla à distância. 2016. Disponível em: https://goo.gl/SXhkE6. Acesso em: 18 Jan. 2018.

[21] YEN, E.R. Security in Automotive Radar and Vehicular Networks. Disponível em: http://www.caee.utexas.edu/prof/bhat/ABSTRACTS/SecurityOverview_mmWave_V2X.pdf>. Acesso em: 17 Jul. 2018

[22] CARROS E MOTORES. Carros sem segurança – Software CarShark permite hackear, controlar e inutilizar qualquer carro. 2010. Disponível em: https://goo.gl/Jq346h. Acesso em: 18 Jan. 2018.

[23] PROJETO EVITA. EVITA: E-safety vehicle intrusion protected applications. Disponível em: http://evita-project.org/index.html. Acessado em Dez/2016.

[24] PROJETO PRESERVE. PRESERVE: Preparing secure v2x communication systems. Disponível em: https://www.preserve-project.eu. Acessado em Dez/2016.