OBD-III: TENDÊNCIAS E PERSPECTIVAS

Jorge Tomioka[1], Marcelo Pires de Souza[1]

[1]Universidade Federal do ABC – UFABC

jorge.tomioka@ufabc.edu.br, marcelo.s@ufabc.edu.br

RESUMO: Um dos dispositivos mais relevantes no sistema embarcado em seguimento automotivo pode ser atribuído a porta OBD (*On-Board Diagnostic*) que foi desenvolvido por volta de 1980 para controle e monitoramento de emissões de gases veiculares. Atualmente a versão é conhecida como OBD II entre as montadoras e suas variantes são adotadas em vários países. Com uma variedade de leituras de dados sobre o veículo que podem ser coletados com equipamentos e softwares específicos. Já versão que propõe a transmissão de dados é denominado como OBD III, podendo ser dotado com sensores, tais como, GPS (*Global Positioning System*), bússolas, giroscópios e acesso à Internet via WIFI (*Wireless Fidelity*) ou telefonia, abre uma grande possibilidade de recursos que podem ser implementados. Neste trabalho são apresentados os acessos de intrusos em computador a bordo automotivo em redes convencionais como CAN (*Controller Area Network*) acessado localmente ou remotamente. Sobre o uso da porta OBD com acesso à Internet foi pesquisada em bancos de dados de patentes onde se observa número crescente depósitos de patentes a cada ano. Sobre tendências e perspectivas, a versão OBD III poderá ser o próximo dispositivo em conjunto com computador central esta já consolidado na indústria automobilística poderá ser aplicado em sistemas automotivo autônomo. Atualmente, observa-se pesquisa e desenvolvimento na busca de interação: entre veículos V2V (*Vehicle-to-vehicle*), veículo-infraestrutura V2I ou V2X (*Vehicle-to-Infrastructure*), onde envolvem diversos recursos de protocolos de comunicação. O uso deste dispositivo pode gerar diversos tipos aplicativos e serviços, não somente ofertada pela montadora. No entanto, é importante elaborar sistema que garanta a questão da segurança computacional (*Cyber Security*).

ABSTRACT: One of the most important devices in the embedded system in vehicle can attributed to OBD port (On-Board Diagnostic) that developed around 1980 for control and monitoring of vehicle gases emissions. Nowadays the version known as OBDII in vehicle industries and its versions have adopted in many countries. With a variety of data, readings on the vehicle can collected with specific device and software. New version that proposes the transmission of data is referred to as OBD III, which may be equipped with sensors, such as GPS (Global Positioning System), compasses, gyroscopes and Internet access via WIFI (Wireless Fidelity) or phone, it opens a possibility of resources that may be implemented. This article presents the intrusion access to computer automotive board in conventional networks such as CAN (Controller Area Network) accessed locally or remotely. On the tendency of using OBD with Internet access was investigated in the patent databases that we can observe increasing number patent applications every year.

On trends and perspectives, the OBD III version might be the next device in conjunction with central computer is already well established in the automotive industry can used in self-automotive systems. Current, there is R & D in the search of interaction: between vehicles V2V (Vehicle-to-vehicle), vehicle-infrastructure V2I or V2x (Vehicle-to-Infrastructure), on which involve various resources communication protocols. The use of this device can generate a variety of applications and services not only supplied by the manufacturer. However, it is important to develop system that ensures the issue of computer security.

1. INTRODUÇÃO

Existe uma grande preocupação em grandes centros urbanos sobre a questão de emissões de gases poluentes provenientes de veículos que comprometem a saúde da população e o meio ambiente [1]. As frotas veiculares têm uma parcela significativa na questão de emissões de gases e diante disto tem sido foram criadas legislações limitando para serem menos poluentes. E assim se tornou necessário o uso de recursos de dispositivos eletrônicos e de sensores. No estado de Califórnia no EUA em 1988, pioneiramente introduziu CARB (*California Air Resources Board*) com legislações rígidas para emissões de gases veiculares [2]. E consequente ganhou grandes proporções internamente no EUA, se tornou uma lei federal e foi adotado em outros países [3].

Diante desta situação e preocupação com as questões das aplicações das legislações foi desenvolvido um dispositivo para leitura de dados através da OBD a ser instalado em cada veículo para monitoramento de emissões de gases. Caso ocorra algum problema extremo é acionada uma luz indicadora instalada no painel do veículo. Este recurso é conhecido como sinalização de mau funcionamento ou MIL (*Malfunction Indicator Lamp)* conforme ilustrado na Figura *1* com suas variantes. Uma outra versão mais sofisticada de OBD (*On Board Diagnostic*) foi implementada com o mesmo intuito denominado como OBD II (*On Board Diagnostic II*) em 1996 no EUA, também adotada na Europa como EOBD (*European On Board Diagnostic*). Portanto, todos os veículos fabricados nos meados dos anos de 1990 são dotados deste conector para atender as questões de legislação ambiental relativamente rígidas no EUA e em países europeus [4].

Figura 1 – Alguns Sinais Indicadores de Mau Funcionamento

Um dispositivo conectada na porta OBD transmite dados entre e nas unidades eletrônicas conectadas aos sensores específicos que fazem medições de emissão de gases, rotação do motor, velocidade, volume de combustível, temperatura do líquido de arrefecimento, temperatura no motor, situação do freio ABS (*Antilock Braking System*), número do chassi e entre outras implementadas pelas montadoras [5], veja na *Figura 2* um diagrama esquemático convencional de um conector OBD. O conector é dotado com 16 pinos que estão conectados com o computador a bordo do veículo. Os pinos 4, 5 e 16 são padronizados, respectivamente usados para aterramento do potencial elétrico, aterramento de conectores de sinais e fonte elétrica de corrente contínua. E os demais pinos, cada montadora implementa para os protocolos de comunicação. No entanto, existe um problema de vulnerabilidade no protocolo CAN que pode dar acesso ao intruso no sistema de computador de bordo do veículo [6-9].

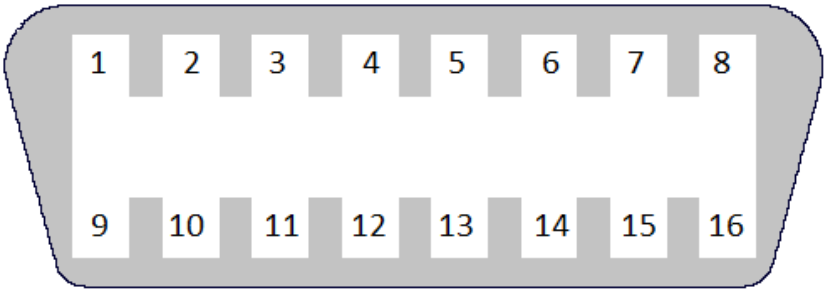

Figura 2 – Conector OBD padrão e seus pinos para conexão de sinais

No Brasil foi adotado *Programa de Controle de Poluição do Ar por Veículos Automotores* (PROCONVE). Tendo como objetivo a redução dos níveis de poluentes emitidos pelos veículos e para desenvolver a tecnologia nacional. O programa é regido pela resolução do Conselho Nacional do Meio Ambiente (CONAMA), Nº 18 de 06/maio/1986. A resolução CONAMA Nº 315 de 29/maio/2002 especifica prazos e limites de emissões de poluentes que devem ser implementadas pelos fabricantes.

Já resolução CONAMA Nº 354 de 13/dezembro/2004 determina a implementação do dispositivo OBD em duas fases denominadas: OBDBr-1 (*On Board Diagnostic Brazil I*) e OBDBr-2 (*On Board Diagnostic Brazil II*). O cronograma dessas fases inicialmente obriga apenas uma parcela de veículos automotores com OBD. E finalmente estas resoluções obrigam as montadoras a instalarem os dispositivos OBD em todos os veículos automotores fabricados a partir do ano de 2011[10].

Além disso, é necessário atender a instrução normativa IBAMA (Instituto Brasileiro do Meio Ambiente e dos Recursos Naturais Renováveis) Nº 126 de 24/outubro/2006 que tem objetivo especificar as normas para implementação das instalações do OBD II no mercado nacional [11].

Portanto, atual sistema embarcado pode se atribuir que se originou de uma legislação ambiental que limitava a emissão de gases poluentes e com o advento da eletrônica, desenvolvimento de sensores e computação se tornou obrigatório atualmente em todos os veículos fabricados. O Brasil por sua vez, atende segue as mesmas legislações praticadas no exterior.

Para atender os quesitos mais rigoroso e com o advento da telefonia celular está em andamento, o OBD III que permite o envio de dados do veículo diretamente para um servidor com todas as informações necessárias sem a necessidade de uma inspeção presencial em postos de atendimento [12]. A versão do dispositivo denominado como OBD III de uma certa forma já existe no mercado com conexão via cabo usando USB (*Universal Serial Bus*) ou outro tipo, bem como já dotado de WIFI que permite acesso a rede Internet ou local.

E desta forma, as informações sobre emissões de cada veículo poderão ser avaliadas em tempo real. O dispositivo é dotado de leitura de dados e é necessário que o veículo da mesma forma de serviço de tráfego de dados esteja vinculado com uma operadora de telefonia para transmissão ou via WIFI, isso pode gerar uma polêmica diante aos consumidores sobre por exemplo: privacidade e segurança de dados. Além disso, é necessário que sejam desenvolvidos mecanismos de atualização crítica dos softwares levando em consideração a rápida disseminação de vírus computacionais atrelado à vida útil de um veículo.

2. VULNERABILIDADES EM SISTEMA EMBARCADO AUTOMOTIVO

Veículos modernos são dotados de redes de comunicação computacional complexa. Isso torna necessário fazer as considerações de segurança como parte do processo. Devido ao longo prazo de desenvolvimento de um veículo, a solução de segurança computacional estática se torna obsoleta e ineficiente com decorrer do tempo. Observa-se ainda que a questão da segurança computacional de sistema embarcado automotivo perde todo sentido quando se trata da vida útil do produto. Para evitar danos, são necessários estratégias e mecanismos de atualização crítica adequada de acordo com a evolução tecnológica dos ataques de intrusos.

Atualmente, um veículo é dotado com mais de 100 ECUs (*Electronic Control Unit*) e conectado fisicamente através de fiações que podem atingir mais de 2.000 (dois mil) metros. E cada ano, observa-se o aumento da implementação de ECUs e atuadores em veículos de diversas modalidades. Também se observa que sutilmente sistemas sensores com comunicação sem fio tem sido acoplado em veículos mais populares. Neste caso, o sensor de pressão nos pneus ou TPMS (*Tire Pressure Monitoring System*) dotado com protocolo de comunicação específica [13].

Para realizar a pesquisa sobre ameaças cibernéticas em sistemas veiculares, primeiramente é importante analisar quais são os pontos de acesso compreendendo a topologia da rede conforme ilustrado *na Figura 3.* Basicamente o sistema apresentado é um exemplo de rede interna veicular. Onde A se refere ao protocolo que atua no chassi aqui como Flex Ray, o B um protocolo CAN para segurança, o C para infoentretenimento com protocolo MOST (*Media Oriented Systems Transport*), o sistema de conforto pelo protocolo CAN em D, a chave sem fio sendo uma sub - rede LIN (*Local Interconnect Network*) em F, o E sendo gateway central e finalmente o G onde se localiza a porta OBD II [14, 15].

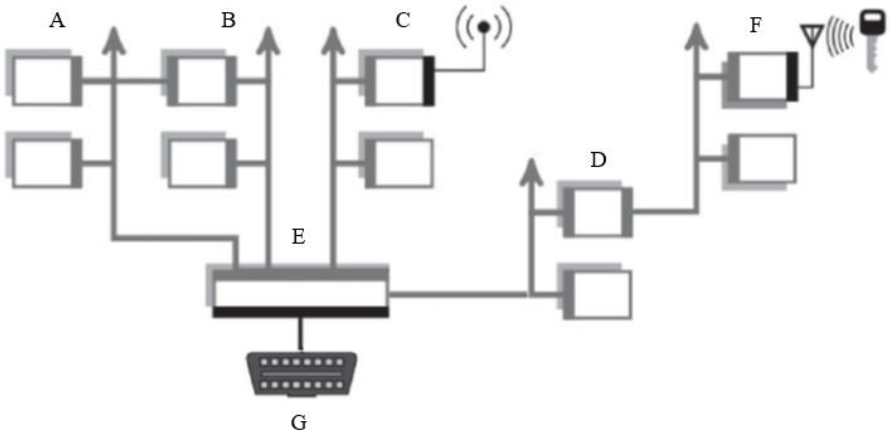

Figura 3 – Diagrama de Rede Típico de Veículo Moderno.

Conforme a topologia aqui apresentada, podem ocorrer ataques que podem físicos ou lógicos de acordo com camada de protocolos que pode ser que seja utilizado em veículos.

Foi demonstrado que o acesso via protocolo CAN é possível acessar o controle e desta forma atacar portas, janelas e sistema de Air Bag [8]. Outra demonstração de ataque é o acesso na ECU onde pode se tomar controle de outras unidades e assim comprometer na condução do veículo ignorando completamente os comandos do condutor acionando freios, controle individual de rodas, buzina, limpador de vidro, desligamento de motor e assim por diante [16].

Pela análise até o momento, existem diversos meios de ataques externos em veículos modernos e é demonstrado que é possível pelos meios físicos instalados tais como: leitor óptico de CD *(Compact Disc)* ou DVD *(Digital Versatile Disc), USB* e leitor de memória em geral. Uma vez inserido código malicioso num desses meios, torna-se possível através de redes sem fio ter o acesso por completo e tomar o controle do veículo [17].

Desta forma, o mecanismo de infecção por vírus, neste caso, mais especificamente por *MalWare* (*Malicious Software*) normalmente em determinados sistemas operacionais passam despercebido, fica apenas anexado e hibernado em algum arquivo específico e ao mesmo tempo procurando algum tipo de equipamento alvo, por exemplo, em algum tipo de formato de áudio, foto ou vídeo que são comuns como uso em entretenimento. Para o usuário é praticamente imperceptível que esteja manipulando arquivo infectado. Assim que algum dispositivo lê o conteúdo de algum meio (CD, DVD ou USB), por exemplo, o *MalWare* em algum momento identifica o alvo. Assim que é identificado o alvo, passa a gerar códigos específicos pré-programados para realizar algum tipo de atividade.

O mais famoso *MalWare* que foi projetado é o *STUXNET* que interferiu no programa nuclear iraniano conforme era previsto, onde controladores de um modelo e fabricante eram alvos foram infectados, desta forma danificou diversos equipamentos de processo de produção de materiais nucleares [18]. No mundo da segurança computacional é muito comum ocorrer ataques cibernéticos para obter informações secretas de empresas e governos. Os dados são transferidos em diferentes servidores com tentativa de ocultar a destinação final. Portanto, ataques remotos em veículos também são possíveis considerando que no atual e futuro mercado saem com acesso a rede Internet. E também,

os provedores de serviços de veículos conectados podem ter controle dominados sem que o real administrador tenha acesso [19].

No caso do *STUXNET* é anexado em arquivo qualquer, no caso a transferência em redes é muito rápido. No entanto, alvos na maioria das vezes estão desconectados da rede com acesso à Internet. Neste caso, o *MalWare* também se infecta em arquivos que são copiados em unidades de armazenamento, desta forma, caso seja utilizado em algum computador desconectado da rede, este é o caminho para chegar até o alvo, na *Figura 4* é mostrado o mecanismo de funcionamento de vírus. A explanação sobre a forma como se opera é descrito da seguinte forma:

1 O vírus é programado e é colocado em algum computador que pode se definir como gênese virótico. E se anexa em algum arquivo copiado em unidade de memória de massa. Ainda tem a funcionalidade para avaliar se é alvo analisando os certificados de propriedade de algum software;
2 Neste passo analise se computador contaminado se faz parte de algum alvo;
3 Caso não seja alvo, não executa nada. Mas se espalha e realiza as atualizações quando está conectado na rede Internet;
4 Na fase do ajuste, o vírus procura brechas ou falhas nos programas, ou "*Zero Day*", ou seja, um dia antes da atualização do software;
5 Já no controle, reconhecendo que é o alvo, o vírus começa a fazer operações tomando controle do computador e de equipamentos conectados;
6 Finalmente com os controles, as operações são as mais diversas possíveis, desde coleta e envio de dados, bem como controlar remotamente. No caso de invasão em veículos, existe a possibilidade de ter dados de configuração previamente realizados na montadora por outras, bem como o controle sendo tomado do condutor.

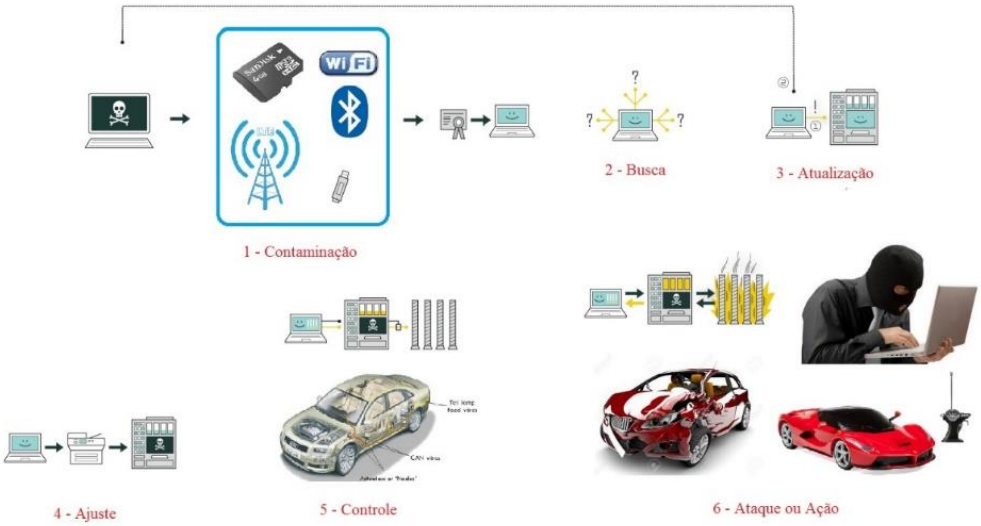

Figura 4 – Fluxo de contaminação de vírus computacional [18].

É necessário que sejam levantados os tipos de ataques que podem ocorrer em veículos altamente automatizados. Para este propósito são apresentadas as definições sobre tipos de ataques [20, 21]:

- *Interno versus externo*: Ataque interno é um membro autenticado de uma rede que pode comunicar com outros membros. Já o ataque externo é considerado pelos membros externos como um intruso, consequentemente, é limitado na diversidade de ataques. Mesmo assim, pode bisbilhotar na comunicação;
- *Malicioso versus racional*: Um ataque malicioso não procura benefícios diretos, tem como objetivo prejudicar os membros ou funcionalidades da rede. Já um ataque racional visa tirar vantagens, portanto, é mais previsível em termos de meios de ataque e os alvos.
- *Ativo versus passivo*: Um ataque ativo pode gerar pacotes ou sinais para obter o seu desempenho. Já o ataque passivo tem como objetivo bisbilhotar o canal de comunicação interna do veículo;
- *Local versus estendido*: Um ataque local pode ser limitado no seu âmbito, controlando várias entidades focadas (internamente no veículo ou bases). Já o ataque estendido controla várias entidades que estão espalhadas por toda rede, abrangendo o seu escopo.
- *Intencional versus não intencional*: Um ataque intencional gera ações propositais. Já o não intencional é um incidente cibernético que poderiam ser gerados por defeitos de sensores ou equipamentos.

Considera-se como ataques todos os tipos citados. Exceto o não intencional, este depende da qualidade dos sensores e de equipamentos.

3. ATAQUES NO PROTOCOLO CAN

O grande desafio é relação ao protocolo CAN ser amplamente utilizado em redes internas automotiva, onde diversas pesquisas demonstram que existem vulnerabilidades que podem ser acesso de invasão [22-24].

Sobre a porta OBD, muitas montadoras implementam usando diversos protocolos de comunicação. E o mais utilizado é o CAN e suas variantes devido ao seu baixo custo e alta taxa de confiabilidade para transmissão de dados, isso não significa que seja considerado como o mais seguro em termos computacionais [7, 9, 22].

Sobre o funcionamento do protocolo CAN, na *Figura 5* é ilustrada um diagrama conceitual sobre as descrições do estado normal de mensagens e sob ataque. Como pode se observar cada mensagem gerada pelas ECUs tem seus intervalos regulares. E sob ataque é feito a tentativa de injeção de mensagens para executar um comando numa ECU. Diante da situação, a ECU envia mensagens ciclicamente e assim aumentando o tráfego na rede.

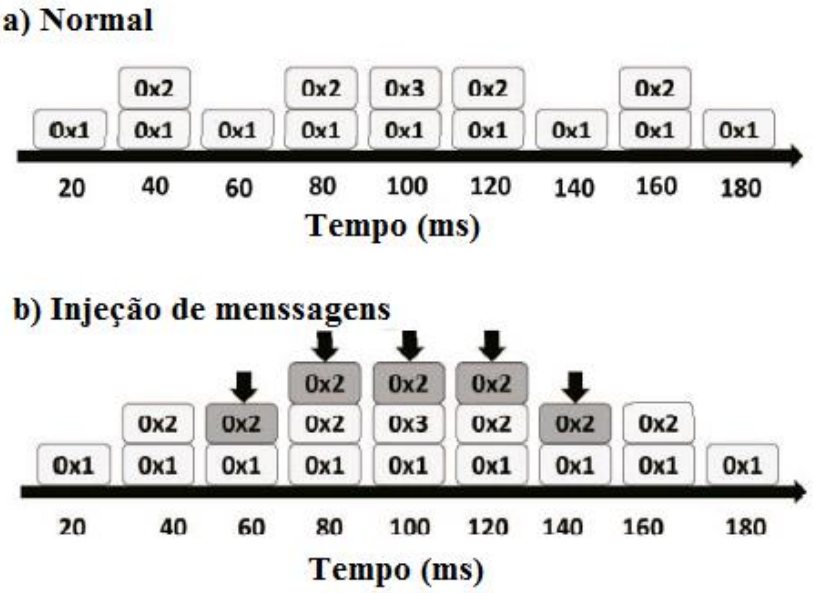

Figura 5 – Diagrama conceitual sobre transmissão de mensagens no protocolo CAN. a) Estado Normal, b) Injeção de mensagens de ataque [23].

Existem duas formas de ataque com injeção no protocolo CAN, uma injeta mensagens de diagnóstico e a outra é a injeção de mensagem padrão enviada para intimar ECU. Os ataques podem ser realizados injetando mensagens normal, injeção de mensagens aleatórias ou pré-ordenadas de forma múltipla e, injeção massiva de mensagens como DoS (*Denial of Service*) [9, 23].

O controle no volante está conectado ao protocolo CAN para acesso especificamente em centrais multimídias [25]. Portanto, conforme pesquisas realizadas sobre meios de acessos de intrusos podem estar relacionadas com dispositivos bem mais comuns, tais como: leitor de unidade óptica (CD/DVD), USB e outras formas de acesso de dados. Neste caso, os arquivos podem estar contaminados com vírus programados para atacar sistemas veiculares. Neste caso, trata-se apenas de contaminação por meio físico e a situação pode ser mais complexa quando recurso como uso do dispositivo Bluetooh abrir o acesso indevido [15].

Os ataques podem ser oriundos internamente com o uso da porta OBD e externamente pelo acesso remoto (Bluetooth, WIFI ou 3G/4G). Isso pode gerar desconforto ao condutor e ao veículo que podem resultar em sinistros. Para todos os ataques existem soluções para eliminar ou minimizar as ameaças usando técnicas adequadas para cada caso. Podendo ser pela correção de software ou melhoria ou troca de sensores.

Implementada nos veículos desde 1996 juntamente com o padrão, a porta OBD II é a interface de acesso ao automóvel mais relevante, normalmente utilizada nas manutenções por profissionais especializados para efetuar diagnósticos, ajustes de desempenho, coleta de informações e programações no sistema, ela viabiliza o acesso direto ao barramento CAN do automóvel, tornando vulnerável todo o sistema automotivo, passíveis a acessos (leitura de dados) e interferências (inserção de códigos maliciosos), capazes de avariar os códigos de programações presentes nas ECUs [17].

Historicamente estas ferramentas de acesso ao barramento CAN, através da porta OBD II, eram restritas, desenvolvidas e fabricadas pelas montadoras e/ou empresas sistemistas envolvidas no desenvolvimento dos novos carros e encontradas apenas em redes de concessionárias autorizadas. Na atualidade, com o aumento significativo da frota mundial de veículos e consequentemente o aumento de oficinas reparadoras de automóveis, este tipo de ferramentas de diagnósticos se popularizou e podem ser facilmente adquiridas para diversas finalidades e adulterar para outras finalidades.

4. PESQUISA EM BANCO DE PATENTES SOBRE OBD

Uma das estratégias para analisar as tendências tecnológicas em setor automotivo, além de estudos pelo *roadmap* (mapa que apresenta tendências ou caminhos de negócios) é o uso de banco de dados de patentes [26, 27]. Utilizando técnica de busca adequada, ou seja, não apenas usando as palavras-chaves e sim pela Classificação Internacional de Patentes – CIP ou *International Patent Classification* - IPC, é possível levantar inúmeras informações de patentes e sobre as suas descrições, reivindicações e aplicações para o setor automotivo.

Neste caso foram consultadas bases de dados da *World Intellectual Property Organization* – WIPO, Derwent *Innovations Index* e *United* States *Patents and Trademark Office* – USPTO (EUA) para realizar a pesquisa sobre patentes que envolve o uso do OBD. Sobre as bases de dados citados, o volume de patentes de diferentes áreas depositadas, a WIPO tem cerca de 7 milhões, Derwent com 14,3 milhões e USPTO com 15 milhões patentes registradas.

De acordo com os dados coletados, especificamente sobre o uso de dispositivo a ser conectado na porta OBD com acesso à Internet, forma:

- Derwent Innovations Index com 26 patentes;
- World Intellectual Property Organization – WIPO com 3.010 patentes;
- United States Patents and Trademark Office – USPTO com 497 patentes.

Observa-se no banco de dados de patentes da Derwent e WIPO respectivamente agregam bancos de dados de 40 e 120 países. No caso do USPTO agrega apenas as patentes protegida nos EUA desde 1790. Portanto, o banco de dados da USPTO é um acervo muito importante para monitorar as tendências tecnológicas de alguns segmentos industriais, pode se correlacionar com os adventos tecnológicos no passado. Na *Figura 6* é ilustrado histórico sobre depósito de OBD com acesso à Internet com diversos tipos de funcionalidade e ano de 2014 atingiu pico com 535 patentes. No ano de 2016, somente no primeiro quadrimestre observa-se 224 depósitos de patentes. Cabe salientar que a patente tem sua vigência de 20 anos no momento que se deposita e não existe a possibilidade de alongar o período de concessão como é erroneamente divulgado em meios de comunicação [28].

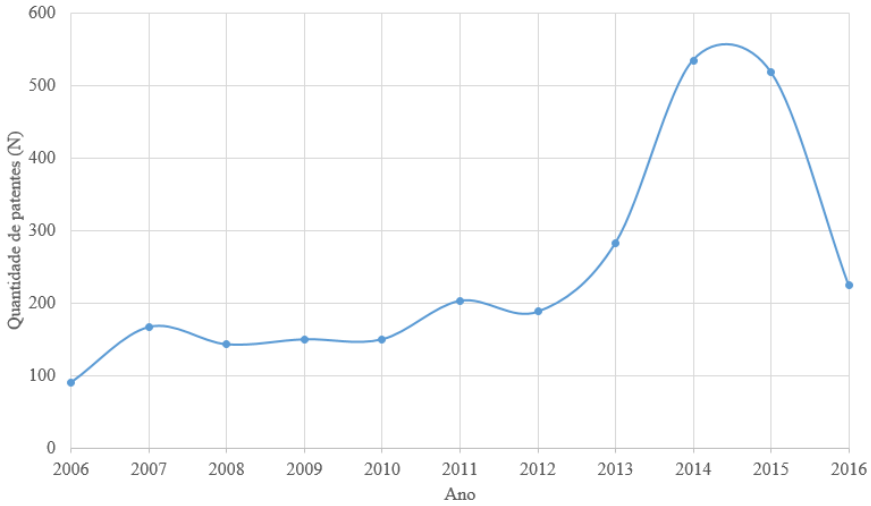

Figura 6 – Depósitos de patentes relacionado a OBD com acesso à Internet.

Na *Figura 7* é apresentado um resumo sobre patentes e suas classes depositadas desde o ano de 2006 com classe G06F que se trata de dados digitalizados com 855 depósitos. Isto demonstra que existem uma grande demanda de componentes embarcados voltadas para o setor automotivo.

Cabe observar, as classes B60R e B60W apesar de estarem em subclasses diferentes, somando as duas com 434 patentes. Quando se trata somente de dispositivos ou componentes que são mais complexos no que tange as questões sobre seus desenvolvimentos, perante às outras reivindicações, a quantidade de patentes é bem expressiva.

Sobre composição molecular, nesta pesquisa observa-se a classificação C08G que estão relacionadas com as questões de emissão de gases veiculares, podendo ser sensores e controladores que monitoram o funcionamento do motor e catalizador. As demais classes da seção de física: G01C, G01M e G06C, estão concentrados em medidas de grandezas de distância, tempo, inclinação e tratamento de sinais digitais. Sobre a seção de eletricidade onde se observa H04L e H04W, as reivindicações na classe de telecomunicação centrada em transmissão e redes de comunicação.

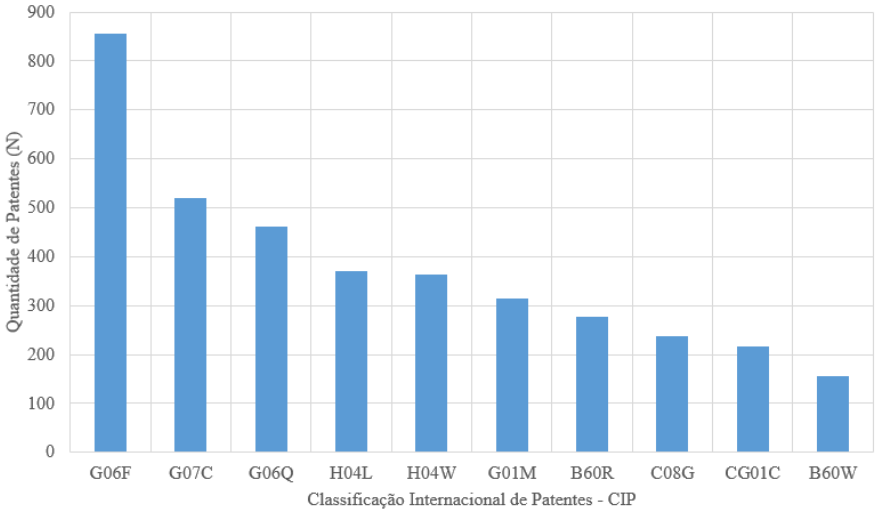

Figura 7 – Quantidade de patentes, segundo Classificação Internacional de Patentes – CIP.

Na *Tabela 1* é ilustrada as patentes depositadas de acordo com a CIP e nesta busca no WIPO predomina medidas, controle, cálculo e computação.

Código	Seção	Classe	Sub-Classe
B60R	Técnicas industriais diversas; transporte.	Veículos em geral	Dispositivos e compoentes de veículos.
B60W	Técnicas industriais diversas; transporte.	Veículos em geral	Sistemas de controle de veículos.
C08G	Química; metalurgia	Composição química	Composto macromolecular
G01C	Física	Metrologia; medidas	Medida de distância; topografia; navegação
G01M	Física	Metrologia; medidas	Medidas da dinâmica das máquinas
G06F	Física	Computação; cálculo	Tratamento de dados digitalizados
G06Q	Física	Computação; cálculo	Processamento de dados
G07C	Física	Dispositivos de controle	Dispositivo para controle de tempo
H04L	Eletricidade	Telecomunicação	Transmissão de sinal digital
H04W	Eletricidade	Telecomunicação	Redes de comunicação

Tabela 1 – Incidência de OBDs no IPC.

Cabe salientar que 2/3 de informações científicas e tecnológicas estão documentados em patentes e os demais em periódicos especializados, livros técnicos ou em meios de divulgação geral como jornais de grande circulação, mídias digitais, congressos, seminários e simpósios. Portanto, é importante que seja realizada buscas em banco de

dados de patentes para analisar as tendências e perspectivas tecnológicas de qualquer setor, exceto informações que são mantidas como sigilos que por sua vez não tem o mesmo amparo legal de uma propriedade intelectual [29, 30].

De acordo com o desenvolvimento tecnológico da área de microeletrônica, técnicas computacionais e de associação entre montadoras e grandes empresas de softwares, fica evidente que os veículos nos próximos anos serão muito mais parecidos com computadores dotados de um sistema complexo de redes e sensores. Aliado ainda com o conceito de veículos autônomos, um meio para este tipo de propósito é a engenharia atuando de forma interdisciplinar para busca de soluções tecnológicas no setor automotivo [31, 32].

O grande desafio no setor da indústria automobilística pode ser atribuído à acirrada concorrência entre as montadoras e seus parceiros. Diante da concorrência para se permanecer no mercado, bem como a expansão, grupo pequeno de montadoras tentam desenvolver sistemas computacionais específicos. Isto eleva o custo de desenvolvimento do veículo e ainda corre risco de entrar em obsolescência tecnológica devido a recusa do mercado. Para isto, tenta-se consolidar a AUTOSAR, um consórcio envolvendo as principais montadoras com objetivo de padronizar as questões computacionais, componentes e sensores [33-36].

5. CONCLUSÃO

A porta OBD III pode ser o próximo recurso para uso para diversas finalidades com acesso à Internet. Este recurso pode gerar muitas demandas para área computacional para desenvolver aplicativos que podem interagir, como por exemplo, com smartphones.

O grande desafio ainda está na questão de vulnerabilidade computacional que se observa no protocolo CAN amplamente utilizado na grande maioria dos veículos. Os estudos demonstram que é altamente recomendável implementar recursos complementares para aumentar o nível de segurança computacional.

Na porta OBD, das 16 vias padronizadas e dentre elas 3 são reservadas (pinos 4, 5 e 16) são implementados protocolos CANs. Portanto, se o dispositivo conectado na porta OBD pode abrir meios para ataque através das técnicas de injeção de mensagens ou DoS. Podendo ser localmente ou remotamente através da conexão via Internet.

Os pedidos de patentes utilizando a porta OBD para acesso à Internet com diversas funcionalidades apresenta o interesse pelos grandes fabricantes de equipamentos eletrônicos, isto demonstra que pode existir nos próximos anos uma infinidade de recursos implementados em veículos.

Os recursos que o OBD pode proporcionar é uma grande surpresa futuramente para os consumidores nos próximos anos. Os veículos podem interagir entre si ou com infraestrutura ao longo da via informando condutor e centro de monitoramento de trânsito. Além disso, o desempenho do veículo pode ser monitorado em tempo real evitando assim, a inspeção em postos de atendimento para análise de emissão de poluentes.

No entanto, ainda no setor da indústria automobilística não existe uma tentativa com maior esforço para desenvolver tecnologia de forma de cooperação como AUTOSAR para otimizar recursos em pesquisa e desenvolvimento. Esta forma de atuação independente entre montadoras, além do aumento do custo, tem gerado incompatibilidade e atraso na área computacional. E as falhas computacionais em veículos podem gerar problemas para os usuários e em casos extremos pode acidentes pela falha de segurança computacional. Talvez, o setor automobilístico esteja transitando de forma silenciosa a entrada de novos *players*, quebrando a sequência do atual modelo de indústria automobilística com as entradas de grandes empresas de softwares como Google, Microsoft e Apple. Com visível advento de veículos elétricos, o cenário promete ser bastante diferente como tem sido visto nos últimos 100 anos. E o OBD que foi inicialmente implementado para diagnóstico de veículos com motores a combustão, poderá ser utilizado para outras finalidades com o uso de motores elétricos. Aliado ao advento da microeletrônica, sensores e computação, poderá ocorrer uma grande revolução na indústria automobilística, bem como a preocupação com a "*Cyber Security*" ou Segurança Cibernética.

REFERÊNCIAS

[1] M. J. Molina and L. T. Molina, "Megacities and atmospheric pollution," *Journal of the Air & Waste Management Association*, vol. 54, pp. 644-680, 2004.

[2] D. Gerard and L. B. Lave, "Implementing technology-forcing policies: The 1970 Clean Air Act Amendments and the introduction of advanced automotive emissions controls in the United States," *Technological Forecasting and Social Change*, vol. 72, pp. 761-778, 2005.

[3] J. C. Cramer, "Population growth and air quality in California," *Demography*, vol. 35, pp. 45-56, 1998.

[4] A. Cheng, G. Zhou, and M. Xie, "The vehicle diagnostic information system based on OBD standard."

[5] R. Bosch, *Manual de tecnologia automotiva*: Edgard Blucher, 2005.

[6] J. A. Bruton, "Securing CAN Bus Communication: An Analysis of Cryptographic Approaches," 2014.

[7] P. Carsten, T. R. Andel, M. Yampolskiy, J. T. McDonald, and S. Russ, "A system to recognize intruders in controller area network (CAN)," in *Proceedings of the 3rd International Symposium for ICS & SCADA Cyber Security Research*, 2015, pp. 111-114.

[8] T. Hoppe, S. Kiltz, and J. Dittmann, "Security threats to automotive CAN networks–practical examples and selected short-term countermeasures," in *Computer Safety, Reliability, and Security*, ed: Springer, 2008, pp. 235-248.

[9] J. Staggs, "How to Hack Your Mini Cooper: Reverse Engineering CAN Messages on Passenger Automobiles," *Institute for Information Security*, 2013.

[10] M. Alves, A. Arnhem, P. Baltusis, E. Burgos, and C. Orasmo, "Preliminary Investigation of OBDBr-2 Catalyst Monitor Performance with Aftermarket Catalysts," *SIMEA Paper*, vol. 27, 2009.

[11] F. E. Mendes, "Avaliação de programas de controle de poluição atmosférica por veículos leves no Brasil," UNIVERSIDADE FEDERAL DO RIO DE JANEIRO, 2004.

[12] K. Kamiya, N. Kawabata, Y. Matsuura, and K. Furusawa, "Vehicle diagnosis system having transponder for OBD III," US6225898 B1, 2001.

[13] G. Guette and C. Bryce, "Using tpms to secure vehicular ad-hoc networks (vanets)," in *Information Security Theory and Practices. Smart Devices, Convergence and Next Generation Networks*, ed: Springer, 2008, pp. 106-116.
[14] A. Lang, J. Dittmann, S. Kiltz, and T. Hoppe, "Future perspectives: The car and its ip-address–a potential safety and security risk assessment," in *Computer Safety, Reliability, and Security*, ed: Springer, 2007, pp. 40-53.
[15] J. Petit and S. E. Shladover, "Potential cyberattacks on automated vehicles," *Intelligent Transportation Systems, IEEE Transactions on*, vol. 16, pp. 546-556, 2015.
[16] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, *et al.*, "Experimental security analysis of a modern automobile," in *Security and Privacy (SP), 2010 IEEE Symposium on*, 2010, pp. 447-462.
[17] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, *et al.*, "Comprehensive Experimental Analyses of Automotive Attack Surfaces," in *USENIX Security Symposium*, 2011.
[18] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *Security & Privacy, IEEE*, vol. 9, pp. 49-51, 2011.
[19] I. M. Almomani, N. Y. Alkhalil, E. M. Ahmad, and R. M. Jodeh, "Ubiquitous GPS vehicle tracking and management system," in *Applied Electrical Engineering and Computing Technologies (AEECT), 2011 IEEE Jordan Conference on*, 2011, pp. 1-6.
[20] A. Panchenko and L. Pimenidis, "Towards practical attacker classification for risk analysis in anonymous communication," in *Communications and Multimedia Security*, 2006, pp. 240-251.
[21] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho, and X. Shen, "Security in vehicular ad hoc networks," *Communications Magazine, IEEE*, vol. 46, pp. 88-95, 2008.
[22] H. Mansor, K. Markantonakis, and K. Mayes, "CAN Bus Risk Analysis Revisit," in *Information Security Theory and Practice. Securing the Internet of Things*, ed: Springer, 2014, pp. 170-179.
[23] H. M. Song, H. R. Kim, and H. K. Kim, "Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network," in *2016 International Conference on Information Networking (ICOIN)*, 2016, pp. 63-68.
[24] S. Woo, H. J. Jo, I. S. Kim, and D. H. Lee, "A Practical Security Architecture for In-Vehicle CAN-FD."
[25] J. M. Quigley, R. P. Bertalan, J. E. Bargewell, L. E. Plummer, and T. Scherzinger, "Steering wheel electronic interface," in *US 6253131 B1*, ed: USPTO, 2001.
[26] Y. G. Kim, J. H. Suh, and S. C. Park, "Visualization of patent analysis for emerging technology," *Expert Systems with Applications*, vol. 34, pp. 1804-1812, 2008.
[27] J. O. Lanjouw, A. Pakes, and J. Putnam, "How to count patents and value intellectual property: The uses of patent renewal and application data," *The Journal of Industrial Economics*, vol. 46, pp. 405-432, 1998.
[28] J. Lerner, "150 years of patent protection," National bureau of economic research2000.
[29] A. C. Marmor, W. S. Lawson, and J. F. Terapane, "The Technology assessment and forecast program of the United States Patent and Trademark Office," *World Patent Information*, vol. 1, pp. 15-23, 1979.
[30] L. C. d. O. Dupin and I. A. Spritzer, "A UTILIZAÇÃO DE DOCUMENTOS DE PATENTE COMO FONTE DE INFORMAÇÃO TECNOLÓGICA," ed: COBENGE, 2004.
[31] A. Sangiovanni-Vincentelli, "Automotive electronics: Trends and challenges," in *SAE CONFERENCE PROCEEDINGS P*, 2000, pp. 295-308.
[32] G. Leen and D. Heffernan, "Expanding automotive electronic systems," *Computer*, vol. 35, pp. 88-93, 2002.
[33] H. Fennel, S. Bunzel, H. Heinecke, J. Bielefeld, S. Fürst, K.-P. Schnelle, *et al.*, "Achievements and exploitation of the AUTOSAR development partnership," *Convergence*, vol. 2006, p. 10, 2006.

[34] B. S. d. S. d. Silva, "Desenvolvimento de software embarcado automotivo aderente ao padrão AUTOSAR," 2015.
[35] G. Sandmann and R. Thompson, "Development of AUTOSAR software components within model-based design," *Development*, vol. 1, p. 0383, 2008.
[36] A. C. d. Assis, "Implementação e avaliação do protocolo FTT-CAN sobre o sistema AUTOSAR," 2011.