Revisão Sistemática da Literatura sobre Autenticação Anônima em Redes Veiculares

Osmarildo Paviani[1], Daniel Domingos Adriano[2]*, Michelle Silva Wangham[2]

[1]Universidade do Oeste de Santa Catarina (UNOESC) – SC – Brasil

[2]Universidade do Vale do Itajaí (UNIVALI) – SC – Brasil

osmarildo.paviani@unoesc.edu.br, daniel.dadriano@gmail.com

wangham@univali.br

Abstract. *Vehicle networks are characterized by data communication networks between vehicles (V2V) or between vehicles and stationary infrastructures located along streets or highways (V2I) and are used to exchange traffic safety information (such as accident reporting) or general purpose data. Due to the fact that these are heterogeneous and dynamic networks, many challenges need to be addressed so that they can be implemented in large-scale. Anonymous authentication and conditional privacy are some of these challenges. This paper aims to present the results of a systematic literature review (SLR) on proposed solutions that were simulated in order to provide anonymous authentication and conditional privacy in V2V communication. Once the solutions were identified, they were then analyzed, classified and compared.*

Resumo. *As redes veiculares são caracterizadas por redes de comunicação de dados entre veículos (V2V) ou entre veículos e a infraestrutura fixa localizada às margens de ruas ou rodovias (V2I) e são utilizadas para troca de informações sobre segurança de trânsito (como comunicação de acidentes) ou dados de propósito geral. As redes veiculares, por se tratarem de redes heterogêneas e dinâmicas, apresentam muitos desafios que precisam ser resolvidos para sua adoção em larga escala. Entre estes desafios citam-se: a autenticação anônima e a privacidade condicional. Este artigo tem por objetivo apresentar os resultados de um revisão sistemática da literatura (*RSL*) sobre soluções que foram propostas e/ou avaliadas através de simulações/implementações para prover autenticação anônima e privacidade condicional na comunicação* V2V. *Após identificadas as soluções, estas foram analisadas, classificadas e comparadas.*

1. Introdução

As redes VANETs (*Vehicular Ad hoc Network*) pertencem a uma classe de redes de comunicação móveis com nós em movimento, ou seja, os veículos [Sahil Garg 2014]. Uma VANET consiste em unidades de bordo (*OBU*) instaladas em veículos e unidades fixas nas bordas das vias (*RSUs*). Esta infraestrutura possibilita estabelecer comunicação veículo a veículo (*V2V*) e veículo para infraestrutura (*V2I*) por meio do protocolo de comunicação de curto alcance (DSRC - *Dedicated Short Range Communications*) [Cheng et al. 2011, Alasmary and Zhuang 2010].

*Bolsista CAPES.

A implementação de redes veiculares é indicada para o auxilio na segurança no trânsito, no controle da poluição, na gestão e eficiência de tráfego e para o entretenimento dos passageiros [Bayat et al. 2015, Gerla et al. 2014]. Na segurança no trânsito, mensagens de alertas podem ser disseminadas quando ocorrer um acidente, fazendo com que os condutores reduzam a velocidade dos veículos, possibilitando a informação sobre outras rotas possíveis a serem utilizadas de forma a evitar a região onde ocorreu o acidente. Neste caso, benefícios incluem a melhora no fluxo dos veículos e ganhos de agilidade no serviço de emergência. Na gestão de tráfego, as redes veiculares proporcionam aos motoristas informações envolvendo situações de congestionamento, controle de bordo e automação de serviços de cobrança nas rodovias. De acordo com [Oulhaci et al. 2016], o principal objetivo das VANETs é compartilhar o tráfego de dados para melhorar a segurança rodoviária e as condições de condução.

Dentre os principais desafios das redes veiculares, destacam-se os relacionados à segurança. A garantia da autenticidade nas comunicações e preservação da privacidade são duas preocupações principais [Shen et al. 2012]. As comunicações nas redes veiculares devem ser autenticadas para impedir que os atacantes injetem conteúdos maliciosos nas mensagens trocadas, bem como para evitar a espionagem [Liu et al. 2016]. Sem a garantia da autenticidade e privacidade, adversários podem ainda rastrear a localização do veículos. Portanto, mecanismos de segurança são necessários para autenticar cada veículo e RSU e assim garantir autenticidade e integridade das mensagens trocadas entre os veículos legítimos [Oulhaci et al. 2016]. Por exemplo, se as mensagens de segurança no trânsito forem modificadas, descartadas ou houver atrasos intencionais, problemas podem ocorrer gerando acidentes.

A autenticação anônima é um dos requisitos fundamentais para prover algumas das principais propriedades de segurança, isto é, a integridade dos dados, autenticidade e o não-repúdio do remetente da mensagem. A autenticação anônima deve garantir o anonimato de um veículo sem que haja nenhuma ligação entre as mensagens trocadas entre os veículos e a sua localização. A preservação da privacidade nas VANET deve ser condicional, ou seja, em caso de ações maliciosas o anonimato deve ser revogado [Zhang et al. 2014, Wang et al. 2016, Guo et al. 2014].

O objetivo deste trabalho é, por meio de uma revisão sistemática da literatura (RSL), analisar quais soluções foram propostas ou avaliadas através de simulações para prover autenticação anônima na comunicação *V2V*. Segundo [Kitchenham and Charters 2007], por meio de uma revisão sistemática da literatura é possível identificar, avaliar e explanar as pesquisas relevantes para uma área ou para um problema de pesquisa.

O restante do trabalho está dividido da seguinte forma. A Seção 2 descreve como a revisão sistemática da literatura foi conduzida, enquanto a Seção 3 descreve os trabalhos selecionados. A análise dos trabalhos relacionados é discutida na Seção 4 e, por fim, na Seção 5, são apresentadas as considerações finais e os trabalhos futuros.

2. Revisão Sistemática da Literatura

A parte mais importante de uma revisão sistemática (RSL) para [Kitchenham and Charters 2007], é o estabelecimento das questões de pesquisa. Para ele, quatro etapas são necessárias para sua elaboração: (a) identificação dos recursos

(questão de pesquisa, palavras-chave e fontes), (*b*) seleção dos estudos, (*c*) extração dos dados e (*d*) análise dos dados. O processo de uma RSL visa encontrar e analisar os possíveis estudos que são capazes de responder às questões de pesquisa formuladas. Para identificar e selecionar estes estudos, foi definido e executado um protocolo de busca. O protocolo de busca definido visa responder a seguinte questão: quais soluções foram propostas ou avaliadas através de simulações para prover autenticação anônima na comunicação *V2V*? Por meio da análise das publicações, buscou-se analisar os trabalhos que apresentem resultados obtidos através de simulações.

Na revisão sistemática, definiu-se que apenas os estudos publicados na língua inglesa seriam considerados de acordo com a *string* de busca: (*"vanets"* OR *"vehicular ad hoc networks"*) AND (*"anonymous"* OR *"anonymity"* OR *"conditional privacy"*) AND (*"authentication"*).

O protocolo de busca foi executado considerando as cinco fontes mais relevantes da área, a saber: ACM Digital Library[1], IEEE Explore[2], Science Direct[3], Scopus[4] e SpringerLink[5]. Para extrair a primeira lista de trabalhos, executou-se a string de busca nas fontes citadas, considerando o título e resumo, e utilizou-se como filtro trabalhos publicados no período entre 2011 e 2016. A Tabela 1 apresenta o total de publicações retornadas de cada uma das cinco bases científicas, o que representou um total de 117 (centro e dezessete) trabalhos.

A Tabela 1 apresenta os resultados da execução de um protocolo de busca. A coluna "Resultado da *string* de busca" mostra a quantidade de artigos retornados em cada base. Na coluna "Trabalhos repetidos/removidos", é apresentada a quantidade de trabalhos que foram excluídos. Para exclusão, fez-se leitura do título e do resumo. A leitura do resumo se deu em virtude de alguns trabalhos possuírem títulos diferentes mas com resumos muito semelhantes, sendo assim possível a exclusão dos trabalhos repetidos (mantendo o mais recente). Já para os trabalhos nos quais o título e o resumo apresentam informações conflitantes, ou seja, o título remete a um assunto e o resumo a outro, ou ainda, os trabalhos que não abordam soluções de autenticação, estes foram removidos da lista.

A coluna "Trabalhos candidatos" apresenta os trabalhos que, após a leitura do título e do resumo, ainda deixaram dúvidas se seriam incluídos ou excluídos como pré-selecionados. Para sanar essas dúvidas, foi realizada a leitura de todo artigo e, os que de fato respondem a questão de pesquisa foram incluídos na lista de trabalhos selecionados, conforme o valor apresentado na coluna "Trabalhos selecionados".

3. Descrição dos Trabalhos Selecionados

[Park et al. 2011] propõem um protocolo de segurança que utiliza chave de assinatura baseada em localização. Neste protocolo, são considerados a utilização de acordo de chaves autenticadas baseada em IBE *(Identity Based Encryption)* para autenticação mútua entre um veículo e uma RSU e a assinatura hierárquica baseada em HIBE *(Hierarchical*

[1] http://dl.acm.org/
[2] http://ieeexplore.ieee.org/
[3] http://www.sciencedirect.com/
[4] http://link.springer.com/search
[5] http://link.springer.com/

Tabela 1. Resultados da Execução do Protocolo de Busca e Seleção de Trabalhos

	ACM	IEEEXplorer	ScienceDirect	Scopus	Springer	Total
Res. da string	3	42	9	24	39	117
Trab. repetidos/removidos	3	22	8	23	27	83
Trab. candidatos	0	14	1	1	8	24
Trab. selecionados	0	6	0	0	4	10

Identity Based Encryption). Pseudônimos são utilizados no processo de autenticação para preservar a privacidade. As simulações serviram para medir o atraso no processamento de mensagens e o tempo de verificação de assinatura baseado em localização em um lote de mensagens.

[Biswas and Misic 2011] apresentam um esquema de autenticação anônima que fornece anonimato condicional aos veículos. O mecanismo proposto faz uso de assinaturas baseadas em curvas elípticas para assinar as mensagens de segurança. Com a utilização do ECDSA, o esquema proposto não necessita utilizar um certificado de chave pública de terceiros para autenticação de mensagens. O anonimato dos veículos é garantido através da utilização de uma grande gama de chaves pré carregadas na OBU. O esquema proposto para assinatura de mensagens e autenticação anônima para os usuários nas VANETs foi simulado utilizando o NS-2, tendo como parâmetros o protocolo IEEE 802.11p. Foi possível concluir que o esquema proposto não necessita de uma grande largura de banda mesmo em um cenário de tráfego denso.

[Bhavesh et al. 2013] propõem um protocolo de autenticação com vários níveis de anonimato (AMLA) em VANETs. O protocolo AMLA faz uso de um mecanismo de assinatura baseado em identidade (IBE), em conjunto com pseudônimos para proporcionar o anonimato. São atribuídos aos pseudônimos um tempo de vida (*timestamp*) para tornar a revogação do anonimato mais simples, pois a AC *(Autoridade Certificadora)* não necessita verificar todos os pseudônimos emitidos antes da data atual. O protocolo AMLA foi simulado, utilizando o simulador QualNet. Para implementar o protocolo criptográfico IBE, foi utilizada a biblioteca criptográfica PBC (*pairing based cryptography*). Os autores concluem de forma qualitativa que o protocolo AMLA gera assinaturas leves, tendo assim um baixo *overhead* na comunicação V2I e V2V.

[Guo et al. 2014] apresentam o protocolo LPP *(Lightweight Privacy Preserving Protocol)* que provê autenticação mútua entre OBUs e RSUs e faz uso de assinatura de *hash chameleon* baseada em curvas elípticas. No esquema de assinatura proposto pelos autores, a chave pública é atualizada a cada sessão de autenticação (chaves públicas dinâmicas). O protocolo LPP garante o anonimato e a não rastreabilidade devido às seguintes propriedades: *(i)* as informações enviadas pelas OBUs usam diferentes chaves públicas de diferentes sessões, desta forma não é possível rastrear um veículo; *(ii)* as informações relacionadas com os certificados são criptografadas utilizando o par de chaves da sessão, de tal forma que o certificado verdadeiro não possa ser extraído; e *(iii)* o par de chaves é atualizado em todas as sessões. Através das simulações foi possível concluir que o protocolo LPP pode alcançar a autenticação mútua, tanto para comunicações V2V ou V2I, com um menor custo computacional.

[Chuang and Lee 2014] propõem o TEAM *(TRUST-EXTENDED AUTHENTICA-*

TION MECHANISM) para proteger os usuários válidos em VANETs de ataques maliciosos. A quantidade de cálculo criptográfico do TEAM foi substancialmente menor do que nos sistemas existentes, pois o TEAM só utiliza operações *XOR* e uma função *hash* (SHA-1 e SHA-512). Além disso, o TEAM baseia-se no conceito de relações de confiança transitiva para melhorar o desempenho no processo de autenticação. As simulações foram feitas com o objetivo de medir o tempo computacional e o custo de armazenamento durante o processo de autenticação em cada operação. O TEAM se mostrou eficiente quando comparado com o RSA. Com relação ao custo de armazenamento, o TEAM se mostrou eficiente mesmo quando houve um aumento significativo no números de veículos. Este trabalho é uma continuação de uma versão preliminar publicada por [Chuang and Lee 2011].

Os autores [Shao et al. 2015a] propõem um protocolo de autenticação anônima de limiar para VANETs, usando o esquema de assinatura de grupo descentralizado. O modelo de grupo descentralizado possibilita distribuir a geração dos certificados entre diversas Autoridades Certificadoras (AC). Neste modelo, as AC's são as RSU's implantadas ao longo das vias que são responsáveis por fornecer os certificados para as OBU's. Os autores concluem que o protocolo proposto possui eficacia nas VANETs, mas, que esta eficacia não é constante, para tanto os autores estão planejando um novo protocolo em que o custo computacional e verificação em lotes seja constante.

Os autores [Shao et al. 2015b] apresentam uma proposta muito semelhante ao trabalho apresentado pelos autores [Shao et al. 2015a]. Os dois aspectos que diferenciam os trabalhos são: (*i*) a geração de certificado de grupo associado ao uso de criptografia baseada em identidade para gerar a chave privada e, (*ii*) o método para criptografar as informações na OBU. Neste trabalho é utilizado a criptografia ELGamal em vez da criptografia linear. Desta forma, os autores concluem que há uma redução nos custos computacionais para gerar e transmitir as assinaturas.

Os autores [Wang et al. 2016] apresentam o LESPP, um esquema que utiliza uma pseudo-identidade autogerada para garantir tanto a preservação da privacidade como a rastreabilidade condicional. Ele requer apenas criptografia simétrica e geração de código de autenticação de mensagem (*MAC*) para assinatura de mensagem. As simulações, utilizando o simulador de rede ONE, demonstram que o LESPP é praticável e tem um bom desempenho proeminente na assinatura e verificação das mensagens, com baixa perda de mensagens e latência da rede. O LESPP emprega principalmente operações simétricas para assinatura e verificação de mensagens, o que reduz a sobrecarga de computação e comunicação. A assinatura baseada em identidade usada pelo KMC *(key management center)* para assinar mensagens não precisa transmitir o certificado acompanhado dela, o que reduz ainda mais a sobrecarga de comunicação e evita o gerenciamento de certificados.

[Malhi and Batra 2016] apresentam uma estrutura de autenticação segura com preservação da privacidade utilizando pseudônimos para a comunicação anônima. A proposta faz uso de assinaturas baseada em ID para comunicação V2V e V2I e duas autoridades confiáveis: *i)* a autoridade regional de transporte (RTA); e *ii)* o centro de geração de chaves (KGC). A primeira autoridade é utilizada para registrar a identificação do veículo e a segunda para a geração das chaves para as OBU's e RSU's. Em seguida, as RSU's monitoram os veículos que estão ao seu alcance e atribui pseudônimos a eles. As RSU's

podem detectar veículos maliciosos e informar as outras entidades sobre este comportamento. A comunicação entre as RSU's ocorre por meio da Internet e a comunicação entre os veículos por meio da comunicação sem fio usando o protocolo IEEE 802.11p. O filtro de *Bloom* é utilizado para verificar os endereços MAC e pseudônimos das mensagens recebidas. Se as mesmas já estão armazenadas no banco de dados é informado ao veículo que ele já está autenticado junto a RSU. A proposta foi implementada utilizando a biblioteca criptográfica MIRACL. As simulações foram feitas utilizando o simulador de rede Ns-2.34 e os resultados são apresentados em relação a comparação do uso do filtro de Bloom e sem o uso do filtro. Os parâmetros utilizados para comparação foram: taxa de entrega de pacotes, latência da rede e atrasos computacionais. O esquema proposto foi comparado com outros esquemas de assinaturas, sendo elas: (ECDSA, BLS, GSIS, ECPP, DCS, PASS e LPA). Desta forma os autores concluem que a utilização do filtro de Bloom melhora o processo de verificação de assinaturas impedindo a sobrecarga na rede quando há um tráfego intenso.

Os autores [Oulhaci et al. 2016] apresentam um sistema de certificação segura e distribuída para autenticação de mensagens de segurança nas redes veiculares, resistente à falsificação de certificação de chave pública. Para aumentar a disponibilidade do serviço de autenticação, a proposta é projetada através de um sistema descentralizado, supervisionado por uma autoridade raiz e gerido por um conjunto de Autoridades de Certificação Regionais (ACR), que são responsáveis pela autenticação dos veículos. Cada ACR supervisiona um grupo de RSU's e colabora com eles ao entregar os certificados para os veículos que utilizam mecanismos como multi-assinaturas e o esquema de assinatura limiar baseado na curva elíptica. As simulações foram feitas utilizando o ambiente Matlab, com o propósito de analisar a taxa de sucesso de certificação, que representa a porcentagem de pedidos de certificação atendidos e a verificação de mensagens, que são o número total de mensagens verificadas com sucesso pelos veículos.

4. Análise dos Trabalhos

Na Tabela 2, são apresentadas as principais informações sobre as técnicas utilizadas para prover autenticação anônima nas redes veiculares, obtidas através da análise dos trabalhos relacionados. A tabela está organizada em oito colunas:

1. Referência: identificado pela citação dos autores;
2. Simulador: qual simulador [6] de rede foi utilizado para efetuar as simulações nos cenários propostos;
3. Camada MAC: refere-se ao canal de comunicação e o endereçamento utilizado neste canal para estabelecer comunicação entre os dispositivos pertencentes à rede veicular;
4. Forma de autenticação: autenticação entre veículos (V2V), autenticação feita pela RSU (V2I) ou híbrida (RSU e veículos);
5. Controle criptográfico: simétrica, assimétrica ou híbrido;
6. Algoritmo criptográfico: os algoritmos utilizados para cifrar as mensagem durante o processo de autenticação;
7. Protocolo criptográfico: o(s) protocolo(s) utilizados e simulados pelos autores;

[6] Quando for indicado um *, significa que este não foi informado pelos autores.

8. Biblioteca criptográfica: a utilização ou não de uma biblioteca criptográfica durante o processo de simulação.

Nos trabalhos apresentados pelos autores [Shao et al. 2015a] e [Shao et al. 2015b], não é apresentado qual simulador foi utilizado, apenas é descrito que os resultados dos testes foram obtidos através de simulação.

Os autores [Park et al. 2011], [Biswas and Misic 2011], [Guo et al. 2014], [Chuang and Lee 2014] e [Malhi and Batra 2016] optaram por empregar o uso do protocolo 802.11p específico para comunicação em redes veiculares. O trabalho apresentado por [Wang et al. 2016], utiliza o protocolo DSRC (*Dedicated Short Range Communications*), que tem como base o padrão 802.11a, ajustado para operações com baixo *overhead*. Os demais trabalhos não apresentam em qual camada MAC a comunicação ocorre.

Nas colunas "Forma de autenticação" e "Controle criptográfico", o uso do termo *híbrido* se dá quando são empregados ambos os métodos V2V e V2I como forma de autenticação, ou uso de chaves assimétricas ou simétricas como controle criptográfico. Apenas os autores [Chuang and Lee 2014] utilizam como método de autenticação a comunicação V2V. Somente o trabalho dos autores [Shao et al. 2015b], utiliza como controle criptográfico o método híbrido, os demais fazem uso de chaves simétricas ou assimétricas.

A coluna "Protocolo criptográfico" apresenta quais protocolos foram utilizados para garantir o anonimato nas redes veiculares. [Chuang and Lee 2014] não apresentam qual foi utilizado em seu trabalho, enquanto [Park et al. 2011] fazem uso da combinação de dois protocolos, o Emparelhamento Bilinear, e IBE (*Identity Based Encryption*). [Guo et al. 2014] e [Chuang and Lee 2014] fazem uso do Emparelhamento Bilinear, e [Bhavesh et al. 2013], [Wang et al. 2016] e [Malhi and Batra 2016] o protocolo IBE. Os autores, [Biswas and Misic 2011], [Shao et al. 2015a] e [Shao et al. 2015b] utilizam assinaturas de grupo. [Oulhaci et al. 2016] é o único a utilizar o esquema de criptografia Limiar que permite criar um conjunto de processos para gerar uma assinatura criptográfica sem revelar a chave privada.

A coluna "Biblioteca criptográfica" tem como objetivo identificar quais bibliotecas criptográficas foram implementadas durante o processo de simulação. Apenas o trabalho de [Bhavesh et al. 2013], implementou a baseada em emparelhamento (*PBC*). A biblioteca *Cripto++*, foi empregada por [Chuang and Lee 2014], enquanto [Shao et al. 2015b] utilizou a *Pairingbased*. [Malhi and Batra 2016] fazem uso da biblioteca *Miracl*. Os demais trabalhos não indicaram ou não fizeram uso de bibliotecas em seus procedimentos de simulações.

Tabela 2. Comparação dos trabalhos relacionados

Referência	Simulador	Camada MAC	Forma de autenticação	Controle criptográfico	Algoritmo criptográfico	Protocolo criptográfico	Biblioteca criptográfica
Park et al. 2011	NS-2	802.11p	Híbrida	Assimétrica	*	Emparelhamento bilinear, IBE	*
Biswas and Misic 2011	NS-2	802.11p	Híbrida	Simétrica	ECDSA	Assinatura de grupo	*
Bhavesh et al. 2013	QualNet	*	Híbrida	Assimétrica	AMLA	IBE	PBC
Guo et al. 2014	NS-2	802.11p	Híbrida	Assimétrica	RSA	Emparelhamento bilinear	*
Chuang and Lee 2014	NS-2	802.11p	V2V	Simétrica	*	*	Cripto++
Shao et al. 2015a	*	*	Híbrida	Híbrido	AES, ECDH	Assinatura de grupo	Pairingbased
Shao et al. 2015b	*	*	Híbrido	Assimétrica	El Gamal	Assinatura de grupo	*
Wang et al. 2016	ONE	DSRC	Híbrida	Simétrica	AES	IBE	*
Malhi and Batra 2016	NS-2	802.11p	Híbrida	Assimétrica	IBE	IBE	Miracl
Oulhaci et al. 2016	Matlab	*	Híbrida	Assimétrica	ECDSA	Criptografia Limiar	*

5. Conclusão

O objetivo deste trabalho foi identificar quais soluções estão sendo empregadas para prover autenticação anônima na comunicação V2V. Até o momento dois procedimentos metodológicos foram realizados: pesquisa bibliográfica e análise dos trabalhos relacionados. A pesquisa bibliográfica abordou conceitos, características, requisitos, mecanismos de segurança em redes veiculares, simuladores, protocolos criptográficos e camada MAC. A análise dos principais trabalhos, descreveu os mecanismos e técnicas para prover autenticação anônima utilizados nos trabalhos. Esta pesquisa foi essencial para compreensão do problema de pesquisa, em especial para identificar quais são as formas de autenticação, híbrido, V2V ou V2I. Dos 10 (dez) trabalhos selecionados um deles utiliza apenas a forma de autenticação V2V.

Como trabalhos futuros, pretende-se implementar uma aplicação alvo para avaliar, por meio de simulações, os impactos causados na aplicação e na rede veicular utilizada pelo uso dos mecanismos de autenticação analisados.

Referências

Alasmary, W. and Zhuang, W. (2010). The mobility impact in ieee 802.11p infrastructureless vehicular networks. In *Vehicular Technology Conference Fall (VTC 2010-Fall), 2010 IEEE 72nd*, pages 1–5.

Bayat, M., Barmshoory, M., Rahimi, M., and Aref, M. R. (2015). A secure authentication scheme for vanets with batch verification. *Wireless Networks*, 21(5):1733–1743.

Bhavesh, N. B., Maity, S., and Hansdah, R. C. (2013). A protocol for authentication with multiple levels of anonymity (amla) in vanets. In *Advanced Information Networking and Applications Workshops (WAINA), 2013 27th International Conference on*, pages 462–469.

Biswas, S. and Misic, J. (2011). Location-based anonymous authentication for vehicular communications. In *2011 IEEE 22nd International Symposium on Personal, Indoor and Mobile Radio Communications*, pages 1213–1217.

Cheng, H. T., Shan, H., and Zhuang, W. (2011). Infotainment and road safety service support in vehicular networking: From a communication perspective. *Mechanical Systems and Signal Processing*, 25(6):2020 – 2038. Interdisciplinary Aspects of Vehicle Dynamics.

Chuang, M.-C. and Lee, J.-F. (2011). TEAM: Trust-extended authentication mechanism for vehicular ad hoc networks. In *International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pages 1758–1761.

Chuang, M.-C. and Lee, J.-F. (2014). Team: Trust-extended authentication mechanism for vehicular ad hoc networks. *Systems Journal, IEEE*, 8(3):749–758.

Gerla, M., Lee, E.-K., Pau, G., and Lee, U. (2014). Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds. In *Internet of Things (WF-IoT), 2014 IEEE World Forum on*, pages 241–246. IEEE.

Guo, S., Zeng, D., and Xiang, Y. (2014). Chameleon hashing for secure and privacy-preserving vehicular communications. *IEEE Transactions on Parallel and Distributed Systems*, 25(11):2794–2803.

Kitchenham, B. and Charters, S. (2007). Guidelines for performing systematic literature reviews in software engineering. Technical Report EBSE 2007-001, Keele University and Durham University Joint Report.

Liu, X., Shan, Z., Zhang, L., Ye, W., and Yan, R. (2016). An efficient message access quality model in vehicular communication networks. *Signal Processing*, 120:682 – 690.

Malhi, A. and Batra, S. (2016). Privacy-preserving authentication framework using bloom filter for secure vehicular communications. *International Journal of Information Security*, 15(4):433–453.

Oulhaci, T., Omar, M., Harzine, F., and Harfi, I. (2016). Secure and distributed certification system architecture for safety message authentication in vanet. *Telecommunication Systems*, pages 1–16.

Park, Y., Sur, C., and Rhee, K.-H. (2011). A privacy-preserving location assurance protocol for location-aware services in vanets. *Wireless Personal Communications*, 61(4):779–791.

Sahil Garg, G. S. A. (2014). An attack tree based comprehensive framework for the risk and security assessment of vanet using the concepts of game theory and fuzzy logic. *Journal of Emerging Technologies in Web Intelligence*, 6(2):247–252.

Shao, J., Lin, X., Lu, R., and Zuo, C. (2015a). A threshold anonymous authentication protocol for vanets. *IEEE Transactions on Vehicular Technology*, 65(3):1711–1720.

Shao, J., Lu, R., Lin, X., and Zuo, C. (2015b). New threshold anonymous authentication for vanets. In *2015 IEEE/CIC International Conference on Communications in China (ICCC)*, pages 1–6.

Shen, A.-N., Guo, S., Zeng, D., and Guizani, M. (2012). A lightweight privacy-preserving protocol using chameleon hashing for secure vehicular communications. In *Wireless Communications and Networking Conference (WCNC), 2012 IEEE*, pages 2543–2548.

Wang, M., Liu, D., Zhu, L., Xu, Y., and Wang, F. (2016). Lespp: lightweight and efficient strong privacy preserving authentication scheme for secure vanet communication. *Computing*, 98(7):685–708.

Zhang, L., Song, J., and Pan, J. (2014). Towards privacy-preserving and secure opportunistic routings in vanets. In *2014 Eleventh Annual IEEE International Conference on Sensing, Communication, and Networking (SECON)*, pages 627–635.