Segurança em *Vehicular Ad-hoc Networks*

Antonio Carlos S. Furtado Jr.[1], **Tiago R. Kepe**[1]

[1]Departamento de Informática – Universidade Federal do Paraná (UFPR)

Abstract. *This assignment summarizes three papers that propose solutions for distinct security problems in VANEts. It was also done comparative analysis of them.*

Resumo. *Este trabalho resume três trabalhos que propõe soluções para problemas de segurança em VANETs distintos. Também foi feita uma análise comparativa entre eles.*

1. Introdução

Em *Vehicular Ad-hoc Networks* (VANETs), cada veículo é equipado com um dispositivo conhecido como *On-Board Units* (OBUs). Ele permite a comunicação com outros veículos, conhecida como *Vehicle to Vehicle* (V2V), e também a comunicação com as *Roadside Units* (RSUs), comunicação conhecida como *Vehicle to Roadside* (V2R). As RSUs são colocadas em pontos críticos das vias, elas tem o intuito de melhorar o trânsito e torná-lo mais seguro. Elas também podem ser conectadas a um *backbone*, isto permite que outras aplicação de rede e serviços sejam fornecidos aos veículos, como acesso a Internet.

Segurança em comunicação é um assunto que atraiu muitas pesquisas em VANETs. Ainda há um número de problemas a serem resolvidos antes que as VANETS possam ser implementadas. Cada artigo aqui apresentado cobre um problema distinto.

Em [Samara et al. 2010] o foco do artigo está em cuidar com segurança e operações em certificados. Os certificados são usados para distinguir atacantes na rede. No artigo [Wagan et al. 2010] o objetivo é garantir confiança na comunicação entre nodos vizinhos, para que seja formado um grupo no qual há a necessidade de comunicação rápida e segura. Finalmente, em [Liao and Li 2009] o problema do rastreamento de um veículo é estudado. Em VANETs isto é possível através da captura de mensagens em *broadcast* sobre o estado de cada veículo, as quais são necessárias. Para resolver este problema ele apresenta uma solução baseada na troca de pseudônimos na rede.

2. Resumos

2.1. [Samara et al. 2010]

Em uma VANET comum, veículos possuem certificados. Ele permite que cada veículo possa transmitir, mesmo que este seja um atacante. A idéia mais aplicada em artigos relacionados é usar uma Lista de Revogação de Certificados (CRL). A CRL permite que todos os veículos transmitam. Se um veículo recebe uma mensagem, ele irá aceitá-la e verificar se a identificação do transmissor consta na CRL. Se ela constar, a mensagem será ignorada, senão ela será aceita. Este esquema causa uma grande sobrecarga. Ele requer que cada veículo possua um CRL atualizado, o que requer freqüentes retransmissões.

A idéia deste artigo é fornecer dois tipos de certificados na rede. O primeiro é o Certificado Válido (VC), este será atribuído a um veículo "bem-comportado", ou seja, um não-atacante. O segundo é o Certificado Adversário (AC), dado a veículos atacantes. Cada certificado deverá ocupar 100 *bytes* de memória. Os campos do VC são os seguintes:

- **Número serial**;
- **Nome do emissor do certificado**;
- **Início**: Define o início do prazo de validade deste certificado;
- **Fim**: Define o fim do prazo de validade deste certificado;
- **Pseudônimo**;
- **Chave pública**.

Enquanto o AC possui estes campos:

- **Número serial**;
- **Nome do emissor do certificado**;
- **Razão da revogação**;
- **Data de revogação**: Define o início do prazo de validade deste certificado;
- **Data de revisão**: Define o fim do prazo de validade deste certificado;
- **Pseudônimo**.

Cada veículo em uma VANET já possui um certificado de identificação próprio. Ele expira a cada 10 minutos e garante a identidade do transmissor. O uso do VC tem como objetivo garantir a intenção do transmissor. Em uma transmissão, um veículo enviará seu certificado de identificação, juntamente com um VC ou um AC, ambos criptografados. Quando um nodo recebe esta transmissão, ele descriptografa a mensagem e verifica se um VC foi enviado. Se ele for encontrado, a mensagem é aceita. Se um AC for encontrado, a mensagem é ignorada e os nodos vizinhos são alertados sobre a presença do atacante. Este alerta contém os seguintes campos:

- **Identificação do nodo que fez o alerta**;
- **Identificação do atacante**;
- **Marca temporal**;
- **Razão da revogação**: Campo presente no AC;
- **Data de revisão**: Campo presente no AC.

Cada alerta é colocado em uma lista, chamada Lista de Atacantes (AL). Esta lista contém no máximo 10 entradas, ela mantém apenas os atacantes mais recentemente identificados. O uso desta lista é idêntico ao uso da CRL. A diferença é que se um transmissor não for identificado nesta lista, sua mensagem não será aceita automaticamente. Antes será executado o processo de identificação de certificado AC ou VC, o qual foi mencionado anteriormente no texto.

A AL possui duas vantagens claras em relação a CRL. Primeiramente ela é uma lista interna, então ela não precisa ser retransmitida periodicamente. Em segundo lugar, ela não é tão grande, pois só são mantidas informações em relação a nodos vizinhos, e não de toda a rede. Isto torna a busca e armazenamento mais fáceis. O uso desses certificados e da AL eliminarão a necessidade da CRL.

A partir da da idéia de certificados proposta, este artigo propõe um protocolo para a revogação de certificados, chamado de Protocolo do Adversário Válido (VAP). Este protocolo consiste na execução dos seguintes passos:

1. **Suspeita**: A maneira que um veículo levanta suspeitas acerca de outro está fora do escopo deste trabalho. Porém foi considerado o caso em que todos os vizinhos de um nodo possuem VCs e enviam mensagens com a mesma informação, exceto um deles, o qual envia informação contraditória. Se esta informação persistir, uma acusação é feita a RSU;
2. **Acusação**: Se o número de acusações que uma RSU será comparado com um limite. Este limite é definido com base no número de veículos na rodovia. Se este limite for ultrapassado, a RSU envia a acusação para uma Unidade Certificadora (CA);
3. A CA considerará este veículo como um atacante;
4. CA manda uma ordem para a RSU, para que ela apague o certificado daquele veículo. E envia um novo AC para ser usado por aquele veículo;
5. RSU executa as ordens enviadas no passo anterior pelo CA. Além disso ele envia por *broadcast* uma mensagem de alerta, para que todos os veículos adicionem o atacante na AL;

Após ter feito a revogação, este nodo revogado terá apenas um certificado AC para transmitir. Isso dirá a outros veículos que este nodo não é confiável. Em trabalhos futuros é esperado que este protocolo possa ser simulado.

2.2. [Wagan et al. 2010]

Inicialmente estudos propuseram mecanismos de segurança baseados em chaves assimétricas. Esses mecanismos são conhecidos pelo custo computacional caro. Sabendo disso, esquemas posteriores que usavam chaves simétricas foram propostos. Eles reduziam o custo computacional, mas comprometiam a segurança. Este artigo propõe o uso de módulos de criptografia simétricos e assimétricos integrados ao *hardware*, e também o desenvolvimento de confiança entre nodos vizinhos.

Este esquema híbrido é composto de três componentes: hardware, entidade de grupo e comunicação de grupo. Os componentes trabalham colaborativamente.

O hardware consiste de um chip TDM (*Trusted Platform Module*). Sua principal função é garantir que os outros módulos estejam funcionando corretamente. Ele consiste de vários motores criptográficos:

- **Módulo assimétrico(ECC)**;
- **Módulo simétrico**;
- **Gerador de números aleatórios**;
- **Módulo Hash**: Usa SHA1;

O TPM recebe dados de um despachador de mensagens. Ela converte a mensagem para um valor Hash, usando seu módulo Hash. Então usando o ECC é gerada uma assinatura digital. Chaves simétricas também são usadas no envio e recebimento. No ponto de recebimento este processo é revertido. Se um nodo é escolhido como líder de um grupo, uma chave é gerada, usando o módulo simétrico e o gerador de números aleatórios. Esta chave então é distribuída via OBU.

O segundo componente mencionado neste trabalho é o grupo, que é simplesmente um conjunto de nodos. Em VANETs grupos podem ser formados de várias maneiras. Um método bastante usado é dividir geograficamente uma rodovia em segmentos, também

conhecidos como células. Outras técnicas de agrupamento também são possíveis. A formação de um grupo está fora do escopo deste trabalho. Apenas reconhecemos que um grupo é um conjunto de nodos próximos. Nós nos preocupamos aqui com o comportamento dos componentes de um grupo. Um grupo consiste de um líder (GL), membros (GMs) e uma certa área geográfica de tamanho fixo. A seleção de um líder pode ser feita de diferentes maneiras, baseadas na posição posição geográfica. Foi considerado que cada membro do grupo possui o componente de *hardware*.

Na comunicação de grupo, o GL gera uma chave simétrica usando o módulo simétrico do TDM e distribui através de uma conexão assimétrica. Cada novo GL gera uma nova chave a ser distribuída. Nesta comunicação há dois tipos de mensagens que são considerados. O primeiro são as mensagens periódicas sobre o estado de um veículo. Estas mensagens serão transmitidas através do método de criptografia assimétrico. O segundo tipo são as mensagens baseadas em eventos. Elas serão transmitidas através do método simétrico, espera-se que com isto o tempo de resposta seja melhorado. Cada chave simétrica é única para determinado evento. Em trabalhos futuros, é esperado simular testes para validar o *framework* proposto.

2.3. [Liao and Li 2009]

Infelizmente informações em *broadcast* periódicas sobre o estado do veículo podem ser usadas para o rastreamento de usuários de veículos. Muitos estudos propõe uma mudança freqüente de pseudônimos na rede, o que não é efetivo com a presença de atacantes globais. Veículos podem ser distinguidos pela diferença de estado mesmo com mudança de pseudônimos. Um atacante pode usar as informações de estado ou do tempo de mudança de pseudônimos para rastrear veículos. Simplesmente mudar pseudônimos em um tempo arbitrário ou em um estado arbitrário pode desperdiçar pseudônimos e recursos. O foco deste trabalho é aumentar a eficiência na mudança de pseudônimos.

O estado de um veículo i é definido como $\{P_i, V_i, D_i\}$, que representa a posição, velocidade e direção de um veículo, respectivamente. A definição do modelo de risco proposto é a seguinte: quando um veículo i altera seu pseudônimo, se pelo menos n $(n \geq 1)$ veículos com estado similar ao veículo i alterarem seu pseudônimo no mesmo tempo, a mudança é bem-sucedida e o ataque falha, caso contrário a mudança falha. Como as mensagens de localização transmitidas por *broadcast* periodicamente juntamente com nosso pseudônimo, uma mudança dessincronizada pode levar ao rastreamento do veículo por um atacante.

Foi proposto um algoritmo chamado algoritmo de mudança síncrona de pseudônimos. A proposta é garantir que com uma alta probabilidade pelo menos dois veículos com estado similar alterem simultaneamente seus pseudônimos.

Ele funciona da seguinte maneira: um veículo escolhe um pseudônimo de um dispositivo, no qual os pseudônimos já foram instalados. Após isto, o sistema usa esta escolha por um período mínimo, no qual este pseudônimo é considerado estável. Quando o tempo expira, uma *flag change* é atualizada para 1. Esta *flag* é adicionada a mensagens de localização, avisando que este veículo está pronto para trocar seu pseudônimo. Ele entra então em um subciclo de espera-verificação. Ele espera por uma condição para mudar seu pseudônimo, checa se há k veículos, cujos estados são similares e que as *flags* $change$ são iguais a 1. Se esta condição for verificada, o veículo muda a *flags* $change$

para 0 e troca o pseudônimo. Se ele não encontra este evento em um tempo limite, ele muda o pseudônimo a força.

Se um veículo i achou k veículos com estado similar, é muito provável que alguns ou todos os k veículos também encontrem esta condição. A razão disto é que eles estão na mesma vizinhança.

O algoritmo foi simulado, e o resultado foi comparado com outros dois algoritmos que possuem a mesma função: algoritmo de estado similar e algoritmo de posição. O algoritmo proposto possui o melhor desempenho entre os três. O diferencial é que enquanto o algoritmo de posição e de estado similar consideram apenas o estado parcial e total, respectivamente, algoritmo de mudança síncrona de pseudônimos leva em conta também a simultaneidade de mudança de pseudônimos.

3. Análise Comparativa

O artigo [Samara et al. 2010] foi o que mais atrelou sua solução a outra já existente, o uso de listas CRL. Ele consegue demonstrar que sua solução é melhor que a anterior até determinado ponto. Porém a taxa de atualização dos certificados propostos por ele não são melhor descritas. Elas deveriam ter sido mais detalhadas, já que a eficiência de sua solução é um dos pontos chave destacados por este autor.

O artigo [Wagan et al. 2010] possui uma maior consideração sobre a implementação de seu *framework* que [Samara et al. 2010], já que ele considera qual será a tecnologia usada (*chip* TDM), e como ela interage com outros componentes. Em [Samara et al. 2010] não é mencionado como seria possível a RSU sobrescrever diretamente os certificados de um veículo. Não há nenhuma consideração sobre uma possível negação desta ação. Ambos não fornecem simulações que comprovem a eficácia de suas idéias, apesar de haver comparações com outras soluções.

O terceiro trabalho analisado foi [Liao and Li 2009], ao contrário dos outros, ele propõe apenas um algoritmo. Ele endereça um problema específico, que é a troca de pseudônimos. Ele é o que melhor expõe a importância de sua solução, pois identifica o problema, mostra alternativas, e é o único a apresentar resultados de uma simulação, na qual verifica-se que seu algoritmo realmente é superior. Assim como o último artigo citado, ele se preocupa com o desempenho de sua solução. A desvantagem dele é ser a única solução probabilísta proposta, uma falha pode ser considerada inaceitável em determinados cenários.

References

Liao, J. and Li, J. (2009). Effectively changing pseudonyms for privacy protection in vanets. In *Pervasive Systems, Algorithms, and Networks (ISPAN), 2009 10th International Symposium on*, pages 648 –652.

Samara, G., Al-Salihy, W., and Sures, R. (2010). Efficient certificate management in vanet. In *Future Computer and Communication (ICFCC), 2010 2nd International Conference on*, volume 3, pages V3–750 –V3–754.

Wagan, A., Mughal, B., and Hasbullah, H. (2010). Vanet security framework for trusted grouping using tpm hardware. In *Communication Software and Networks, 2010. ICCSN '10. Second International Conference on*, pages 309 –312.