Trablho 2 de Redes Móveis

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

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

Abstract. *This assignment summarizes the following papers:[Qian and Moayeri 2008], [Liao and Li 2009] e [Wagan et al. 2010]. We also did a comparative analysis of them.*

Resumo. *Este trabalho resume os seguintes artigos que tratam sobre segurança em VANETs: [Qian and Moayeri 2008], [Liao and Li 2009] e [Wagan et al. 2010]. Também foi feita uma análise comparativa entre eles.*

1. Resumos

1.1. [Qian and Moayeri 2008]

Em VANETs, cada veículo é equipado com um dispositivo conhecido como *On-Board Units* (OBUs). Ele permite a comunicação com outros veículos, conhecida como V2V, e também a comunicação com as *Roadside Units* (RSUs), comunicação conhecida como 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.

Ainda há um um número de problemas a serem resolvidos antes que as VANETS possam ser implementadas. Nós focamos nos dois maiores, que são a segurança e o suporte de aplicaçãoes existentes e futuras nesta tipo de rede.

VANETs possuem alguns problemas já existentes em redes *Ad Hoc* e redes de sensores. Além disso ela possui outros problemas decorrentes de suas particularidades, tais como seu tamanho e a mobilidade em alta velocidade. Esta rede deve assegurar que informação críticas para a vida dos passageiros não possam ser modificadas ou inseridas por um atacante. Ela também deve estabelecer a reponsabilidade dos motoristas e manter a privacidade de suas informações. A segurança de uma VANET deve cumprir os seguintes requisitos:

- **Autenticação e integridade de mensagens**
- **Não-repudiação de mensagens**: Nodo não pode negar não ter enviado a mensagem;
- **Autenticação de entidades**: Deve-se ter certeza que o nodo que enviou a mensagem é genuíno;
- **Controle de acesso**: Políticas para acesso de serviços;
- **Confidencialidade da mensagem**
- **Disponibilidade**: rede deve permanecer operacional após falhas ou ataques;
- **Privacidade e anonimato**: Informação deve ser protegida de acesso não autorizado;
- **Identificação de responsabilidade**: Usuários dos veículos devem ser responsáveis por suas ações deliberadas ou acidentais, as quais podem romper operações com outros nodos ou com o sistema de transportes.

Uma rede vulnerável pode sofrer ataques em várias das suas camadas, aqui estão explicados alguns dos ataques mais comums:

- **Interferência**: O atacante intencionalmente gera transmissões que interferem a recepção de transmissões autênticas;
- **Representação**: Neste ataque um nodo se mascara como uma outra instância da rede. Pode ser como um veículo de emergência, fazendo com que outros abram caminho, ele também pode se passar por uma RSU;
- **Violação de privacidade**: Feita através da captura de mensagens provenientes da comunicação de outros veículos;
- **Falsificação**: Um atacante pode forjar mensagens sobre avisos de perigo. Elas podem contaminar rapidamente uma porção da rede;
- **Adulteração de mensagens em trânsito**: Um nodo desta rede pode intencionalmente modificar ou apagar mensagens entre comunicações de outros nodos;
- **Adulteração de informação a bordo**: O atacante pode modificar informação específica do veículo ou do motorista, tais como velocidade ou localização;

O esquema de uma rede depende também do entendimento das aplicações que serão executadas nela. Elas podem diferir em vários requisitos, como largura de banda, atraso e segurança. Elas podem apresentar diferentes padrões de comunicação. Aqui estão listadas as aplicações existentes e propostas para VANETs:

- **Críticas à segurança de vidas**: Usadas para prevenção de colisões no trânsito, devem possuir a mais alta prioridade;
- **Aplicações para avisos de segurança**: Pemitem atrasos maiores na comunicação que aplicações críticas a segurança;
- **Coleta de pedágio eletrônico**: Permitem cobrança de tarifas sem que haja nenhuma parada. Podem ser feitas através da identificação do veículo;
- **Acesso a Internet**: É possível através de uma conexão unicast entre a OBU e a RSU.
- **Comunicação de grupos**: Motoristas podem compartilhar mesmos interesses quando estão dirigindo nas mesmas condições. Isto poderia ser conseguido com uma implementação de multicast em VANET, o que ainda não foi possível devido sua complexidade.
- **Busca de serviços em rodovias**

Nós propomos um *framework* de projeto de redes. Ele endereça os problemas de segurança e suportas as demandas de aplicaçãoes vistas. Separamos ele em dois componentes principais:

- **Esquema de controle de tipo de aplicação** - Este componente deve estar ciente da disponibilidade de diferentes aplicações, que podem estar em um nodo da rede ou distribuídas. Os servidores devem registrar aplicações neste componente, elas devem ser atualizadas periodicamente ou baseadas em um evento.
- **Esquema de roteamento unificado** - Possui informação sobre as diversas aplicações cadastradas. Pacotes de determinados fluxos devem ser encaminhados de acordo com os aspectos de segurança de sua aplicação.

Para desenvolver o *framework* proposto, um número de tecnologias devem ser discutidas. A primeira delas é a detecção de ameaças. Temos também o gerenciamento de chaves, que devem ser estabelecidas por sessão. E finalizando, a codificação e o roteamento de mensagens, cujos estudos recentes não consideram os cenários das VANETs.

1.2. [Wagan et al. 2010]

Segurança em comunicação é um assunto que atraiu muitas pesquisas em VANETs. Mensagens de seguranças podem ser divididas em dois tipos, mensagens periódicas e orientadas a eventos. Mensagens periódicas são trocadas por vizinhos, e contém informações sobre velocidade, localização, etc. Enquando mensagens orientadas a eventos são trocadas quando uma situação perigosa é verificada. Esta informação precisa ser entregue de maneira rápida e segura.

Um mecanismo de segurança foi proposto como padrão para VANEts, o PKI/ECDSA (*Public Key Infrastructure with Elliptic Curve Digital Signature Algorithm*). Este mecanismo, que usa chaves assimétricas, é conhecido pelo custo computacional caro. Sabendo disso, esquemas que usam chaves simétricas foram propostos, eles reduzem o custo computacional, mas comprometem a segurança. Propomos o uso de módulos de criptografia simétricos e assimétricos integrados ao *hardware*, e também o desenolvimento de confiança entro 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 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 ferada uma assinatura digital. Chaves simétricas também são usadas no envio e recebimento. No pionto 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.

Neste trabalho, a entidade de grupo não se preocupa em como ele é composto. E sim no comportamento de componentes de um grupo. Um grupo consiste de um líder (GL), membros (GMs) e uma certa área geográfica de tamanho fixo. Nós assumimos 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. Além disso uma chave simétrica é usada para apenas uma mensagem de segurança baseada em eventos.

1.3. [Liao and Li 2009]

VANEts consistem em comunicações veículo-para-veículo (V2V) e entre veículo-para-infraestrutura (V2I). Aplicações para esta rede tem o objetivo de melhorar a segurança e eficiência no transporte. Elas dependem do *broadcast* periódico de informações do estado de cada veículo.

Infelizmente este tipo de informação pode ser ser usado para 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 pode ser destinguidos 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 de nosso modelo de risco 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.

Nós propomos um algoritmo chamado algoritmo de mudança síncrona de pseudônimos. Nossa proposta é garantir que com uma alta probabilidade elo menos dois veículos com estado similar alterem simultaneamente seus pseudônimos.

Ele funciona da seguinte maneira: um veículo escolhe um pseudônimo de um dispositivo onde os pseudônimos já foram instalados. Após isto, o sistema usa esta escolha por um período mínimo, no qual este pseudônimo é considerado estável. Quando este 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, ele 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 flag $change$ 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 tabém encontrem esta condição. A razão disto é que eles estão na mesma vizinhança.

Nosso 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 nosso algoritmo possui o melhor desempenho entre os três. O nosso 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.

2. Análise Comparativa

O artigo [Qian and Moayeri 2008], assim como [Wagan et al. 2010], propõe um *framework* de segurança. Ele é o único que tenta levantar todos os problemas de segurança em VANETs, com base na autenticação de aplicações disponiveis na rede. Ele também é o único que leva em conta diferentes perfis de aplicações propostas para VANETs. Apesar disso, ele não é , muito claro como os componentes propostos de seu *framework*

endereçam cada um cada um dos tipos de ataques identificados e como eles arantem os requirimentos de segurança em VANETs.

Ele identifica quais são as tecnologias necessárias para que o desenvolvimento de sua proposta possa ser realizado. Porém nenhuma indicação de como isso seria implantado foi feita.

O artigo [Wagan et al. 2010] é mais objetivo que o mencionado anteriormente. Nele o problema de comunicação confiável entre um grupo é focado. A consideração sobre sua implementação também é feita, já que ele considera qual será a tecnologia usada, e como ela interage com outros componentes. Sua semelhança com [Liao and Li 2009] é que ambos comparam sua solução com outras alternativas, eles descrevem a vantagem de sua idéia em relação a outras. A diferença é que não são fornecidas simulações que comprovem a eficácia de uma possível implementação.

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 apresenta 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 probabílista 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.

Qian, Y. and Moayeri, N. (2008). Design of secure and application-oriented vanets. In *Vehicular Technology Conference, 2008. VTC Spring 2008. IEEE*, pages 2794 –2799.

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.