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. *Abstract in English.*

Resumo. *Este trabalho resume os seguintes artigos que tratam sobre segurança em VANETs: [Qian and Moayeri 2008], [Liao and Li 2009] e [Choi and Jung 2009]. 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. Então 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 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.

References

Choi, J. and Jung, S. (2009). A security framework with strong non-repudiation and privacy in vanets. In *Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE*, pages 1 –5.

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.