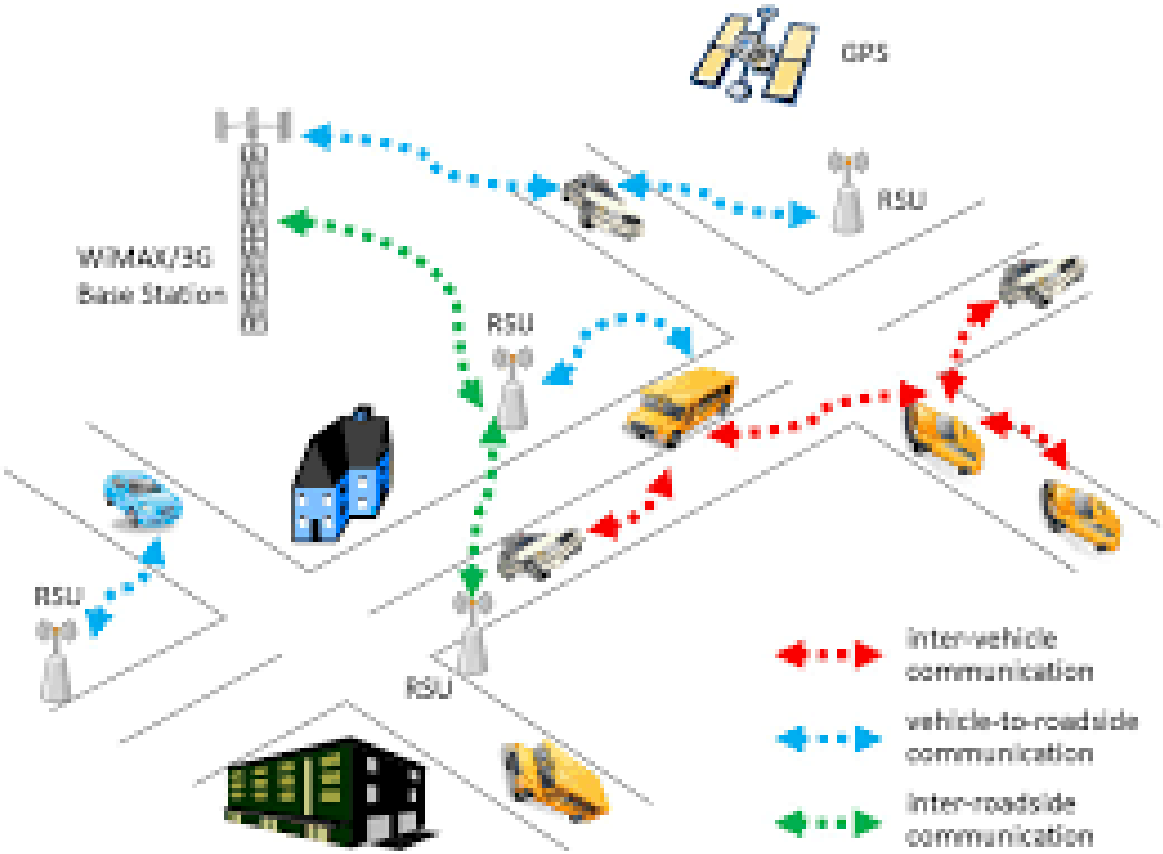
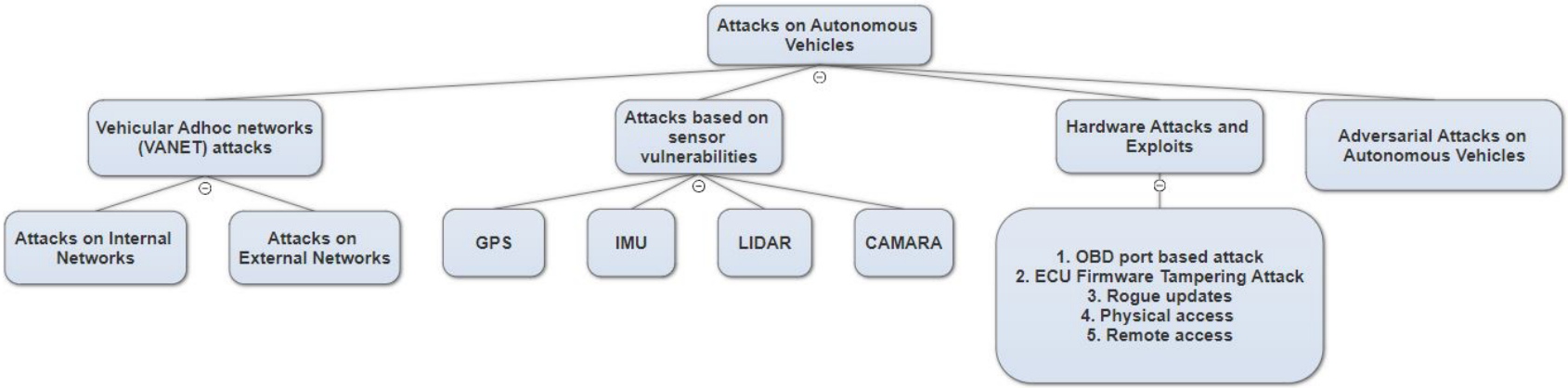
Internet das Coisas e Redes Veiculares (TP-546)

Samuel Baraldi Mafra

Inatel
Instituto Nacional de Telecomunicações

Segurança em redes veiculares:




Attacks on Autonomous Vehicles
Vehicular Adhoc networks (VANET) attacks
Attacks based on sensor vulnerabilities
Hardware Attacks and Exploits
Adversarial Attacks on Autonomous Vehicles
Attacks on Internal Networks
Attacks on External Networks
GPS
IMU
LIDAR
CAMARA
1. OBD port based attack
2. ECU Firmware Tampering Attack
3. Rogue updates
4. Physical access
5. Remote access

The Cybersecurity Implications of Driverless Cars
`https://youtu.be/w4V0hYjAqwU`

Os principais requisitos de segurança são os seguintes:

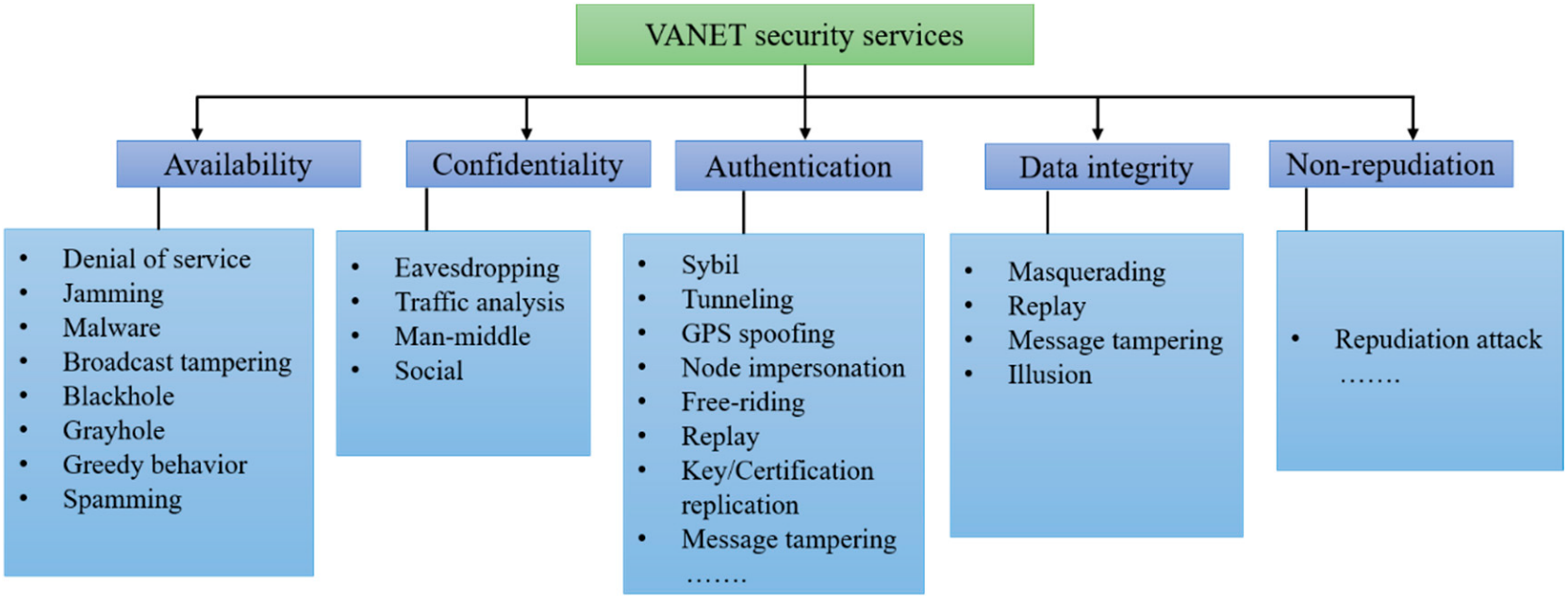
- 1) Autenticidade / identificação. O usuário, fonte e local devem ser autênticos. A autenticação do usuário é para evitar ataques de entidades falsificadas. A autenticação de origem é para garantir que os dados sejam gerados por entidades legítimas. A autenticação de localização é para garantir a integridade e relevância das informações recebidas.
- 2) Disponibilidade. As informações trocadas ou compartilhadas devem ser processadas e disponibilizadas em tempo real.

- 3) Integridade / confiança dos dados. Os dados recebidos devem estar livres de modificação, manipulação ou exclusão maliciosa ou não autorizada durante a transmissão.
- 4) Confidencialidade / privacidade. Os dados trocados não devem ser divulgados a usuários mal-intencionados ou não autorizados.

- 5) Autenticação de dados: os dados transferidos de V2V, V2I e I2V precisam ser verificados. Assim, veículos e RSAP devem ser informados a priori que sua identificação poderá ser verificada aleatoriamente conforme a exigência.
- 6) Rastreamento de ID do veículo: a rede deve ser capaz de rastrear a identidade do veículo, que envia / recebe as mensagens.
- 7) Escalabilidade: a VANET deve ser aberta ao aceitar o número de veículos adicionais sem afetar o sistema desempenho. No entanto, isso pode aumentar a complexidade, o que diminui o desempenho do sistema
- 8) Atualidade da informação: Para evitar o uso de mensagens antigas na comunicação, as novas mensagens devem ser verificadas em intervalos regulares.

- Um invasor pode lançar um ataque, enviando dados maliciosos ou inúteis para os veículos de destino, a fim de reduzir o desempenho dos veículos.
- O invasor também cria um grande número de mensagens falsas para interromper o veículo e fazê-lo funcionar mal.
- Além disso, alguns atacantes irão distrair esses veículos bons de ataques maliciosos para que outros atacantes ataquem com sucesso

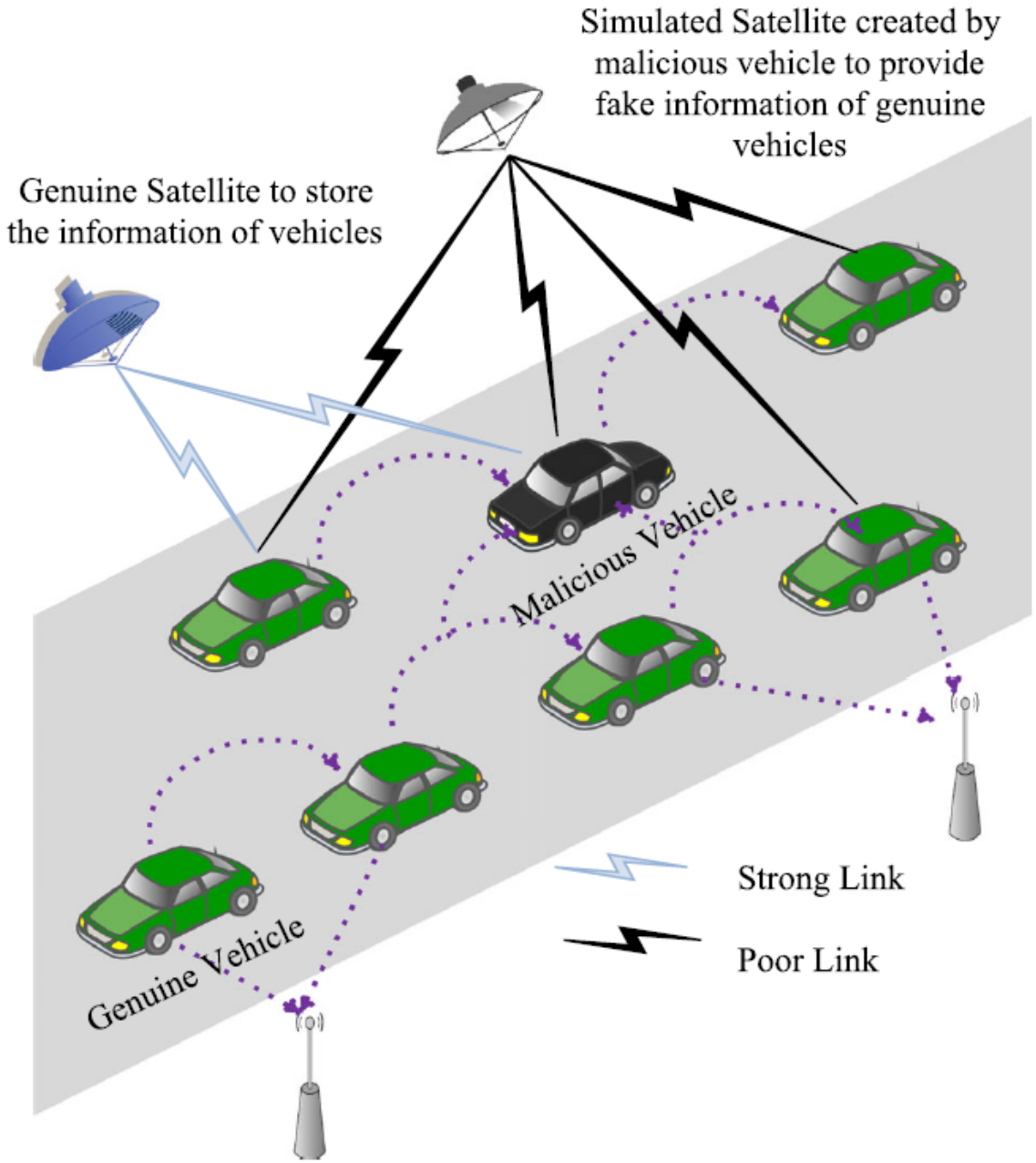
Cyberattacks Against Intelligent Transportation Systems
https://youtu.be/3u0KeJUnHvI


VANET security services
Availability
Confidentiality
Authentication
Data integrity
Non-repudiation
Denial of service
Jamming
Malware
Broadcast tampering
Blackhole
Grayhole
Greedy behavior
Spamming
Eavesdropping
Traffic analysis
Man-middle
Social
Sybil
Tunneling
GPS spoofing
Node impersonation
Free-riding
Replay
Key/Certification replication
Message tampering
.....
Masquerading
Replay
Message tampering
Illusion
Repudiation attack
.....

Ataques em autenticação

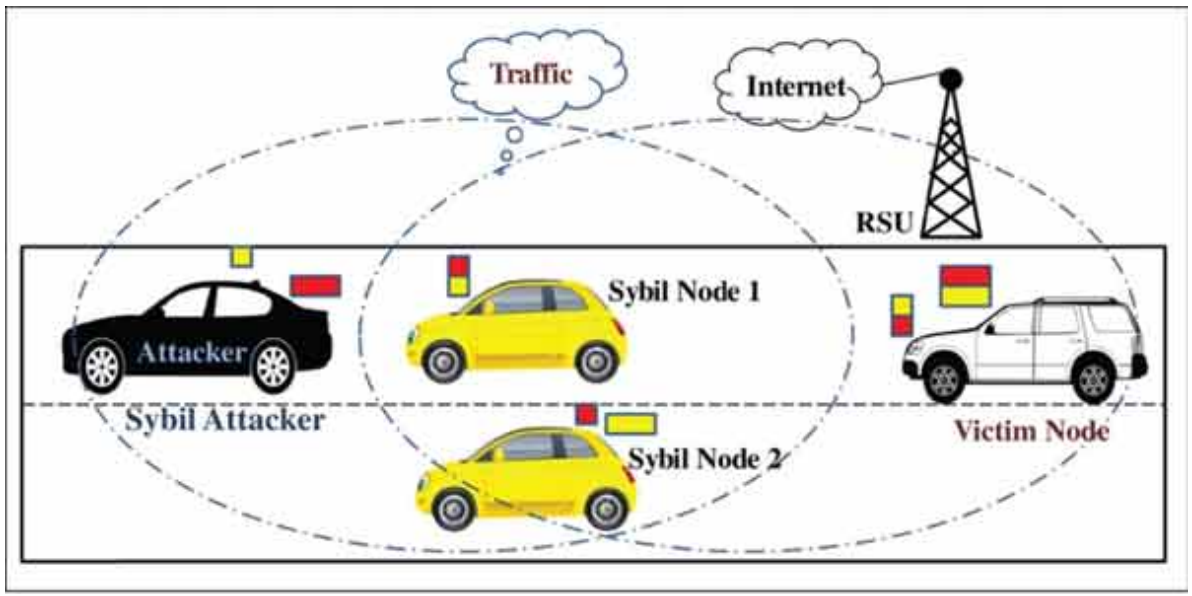
- A autenticação é considerada um requisito fundamental para proteger uma rede VANET, onde fornece integridade da mensagem para evitar manipulação.
- Isso envolve a proteção de nós legais contra invasores mal-intencionados, que penetram na rede usar uma identidade falsa, revelar sinais GPS falsificados, alterar, fabricar mensagens, injetar material incorreto para danificar e afetam a comunicação entre os veículos conectados.

- Ataque de spoofing de GPS: A integridade dos sinais de GPS de nós veiculares na VANET é de grande importância, pois desempenha um papel vital. Esses ataques baseiam-se em restringir os receptores de adquirirem as informações de horário e localização dos nós veiculares. Isso faz com que os atacantes mal-intencionados manipulem a leitura do sinal GPS e alterem as informações arbitrariamente, dominando o sinal GPS conforme ele chega. Em seguida, os receptores dos nós comprometidos são sincronizados com o sinal de tempo falsificado mais recente do sinal de GPS falso.


Simulated Satellite created by malicious vehicle to provide fake information of genuine vehicles
Genuine Satellite to store the information of vehicles
Malicious Vehicle
Genuine Vehicle
Strong Link
Poor Link

Sybil attack

- O atacante malicioso pode injetar informações falsas através da rede e controlar todo o sistema VANET. Devido a isso, os nós veiculares podem tomar decisões incorretas. Também prejudica a eficiência e a consistência do sistema. Se houver nós afetados por SAs, o relatório gerado pode ser diferente do cenário de solo real por causa da injeção falsa de informações.



Falsified entities attack

- Ataque de entidades falsificadas significa que o invasor passa informações para os nós legítimos por meio de um identificador de rede válido.
- O identificador de rede é o certificado necessário para a troca de dados na rede. Assim, as entidades falsificadas constroem uma violação do processo de autenticação.
- Solução: Melhorar os sistemas de autenticação.

- Ataque de replicação: há uma tentativa de um nó malicioso de adicionar nós na rede.
- Esses tipos de ataques usam a identidade de outro nó presente legalmente na rede para transmitir mensagens falsas na rede.

Ataque de carona: No ataque de carona, um nó veicular utiliza os serviços de outros nós da rede, mas não retorna à rede. Ele canaliza a carga útil real em um cabeçalho TCP, que é um cabeçalho falso que mascara uma transmissão.

Ataque de adulteração de mensagens:

- A integridade das mensagens que estão sendo enviadas deve ser protegida por todo o período.
- Aqui, a mensagem é recebida por um nó malicioso, violada e enviada ao nó de destino.
- Esta parece ser uma mensagem válida que leva a problemas na rede, já que todos na vizinhança ou na mesma zona podem ouvir as mensagens que são enviadas por nós veiculares nos arredores.

Ataques de repúdio

- Nos ataques de repúdio (RUA), um veículo nega a transmissão ou recepção de uma mensagem quando atua como remetente ou receptor, respectivamente.
- Requer retransmissão dos remetentes, consome recursos da VANET e causa atrasos na rede. Finalmente, ele usa em excesso a largura de banda da rede

Ataques à integridade dos dados

- Os ataques à integridade dos dados transmitidos são denominados ataques à integridade dos dados.

- Ataque de mascaramento: os atacantes maliciosos se fazem passar por um veículo para injetar informações falsas ou inúteis de um veículo específico em outros veículos. Isso leva a problemas de comunicação do veículo, mesmo quando os veículos de comunicação estão distantes. Por exemplo, um veículo pode fingir ser uma ambulância e atinge o caminho prioritário em comparação com outros veículos.

- Ataque de ilusão (ILA): os invasores mal-intencionados espalham o aviso falso sobre as condições das estradas, como congestionamentos, acidentes e degradação do sistema, o que dá um conceito errado para outros veículos. Esses tipos de ataques podem ser tratados usando uma rede de validação de plausibilidade. Essas redes fornecem um banco de dados de regras e um módulo de verificação de dados. A mensagem é transmitida apenas quando passa por todos os testes de verificação para evitar os ILAs.

- Ataque de repetição: são os ataques em que os atacantes maliciosos armazenam e / ou recebem beacons enviados por um nó membro da rede. O nó armazenado é reproduzido novamente com uma intenção maliciosa, com informações antigas na mensagem levando a efeitos desastrosos.
- Quando um usuário se move ao longo de uma trilha, com uma velocidade s, um invasor malicioso captura e armazena os beacons.
- Quando o veículo para, o invasor injeta as informações do beacon armazenadas no sistema, o que cria uma intuição para outros veículos de que o veículo está se movendo na mesma velocidade s, o que pode levar a problemas perigosos, como colisão potencial.

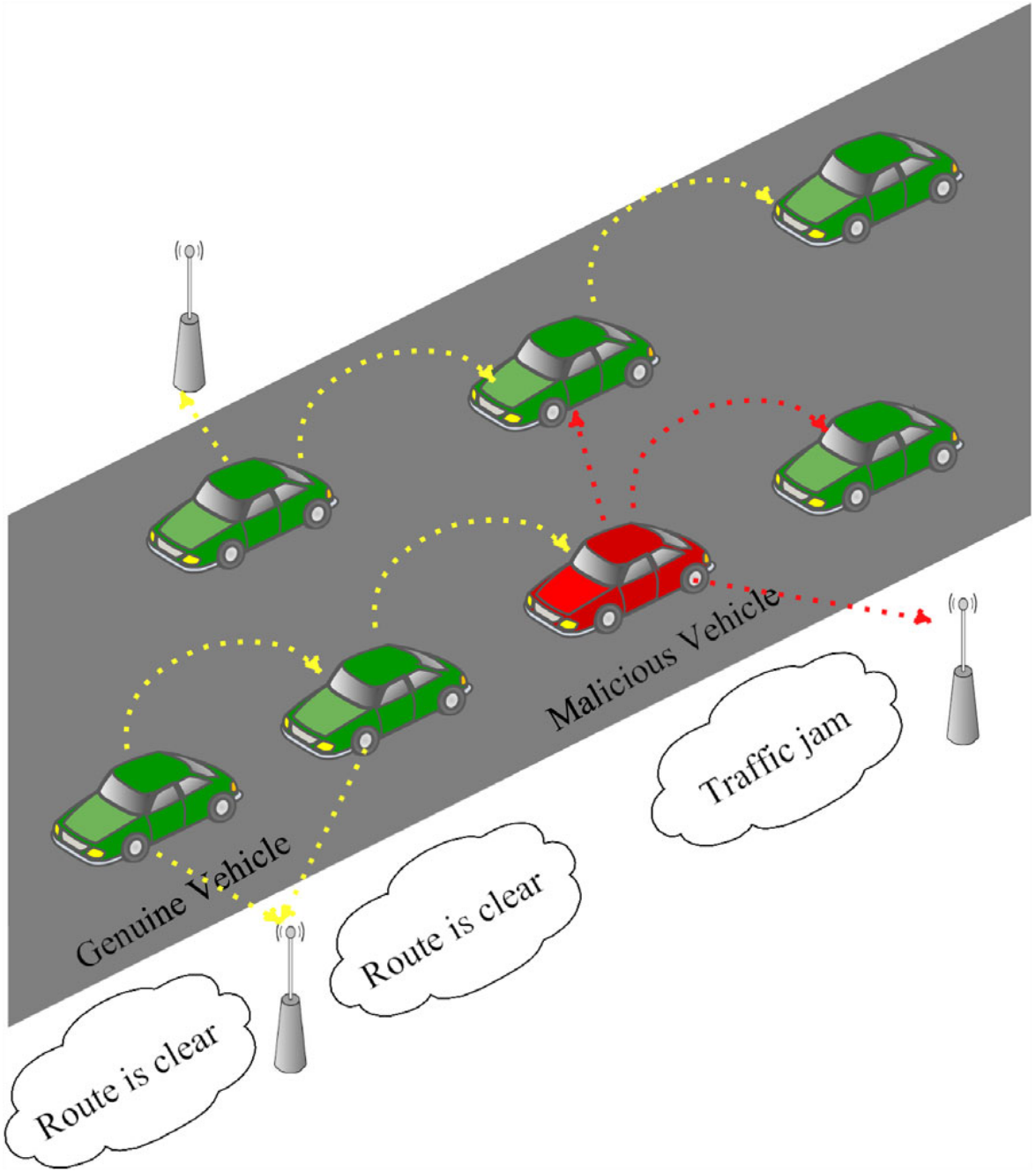
Solução:

- As assinaturas digitais protegem a integridade dos dados para que você saiba que a mensagem que lê não foi alterada ou alterada, acidental ou maliciosamente. Tecnicamente, uma assinatura digital inclui um hash de todo o documento que está sendo assinado. Qualquer alteração no documento depois de assinado invalida esse hash digital.
- As assinaturas digitais garantem a confidencialidade dos dados de um e-mail criptografado - apenas o destinatário pretendido pode recuperar e ler a mensagem.

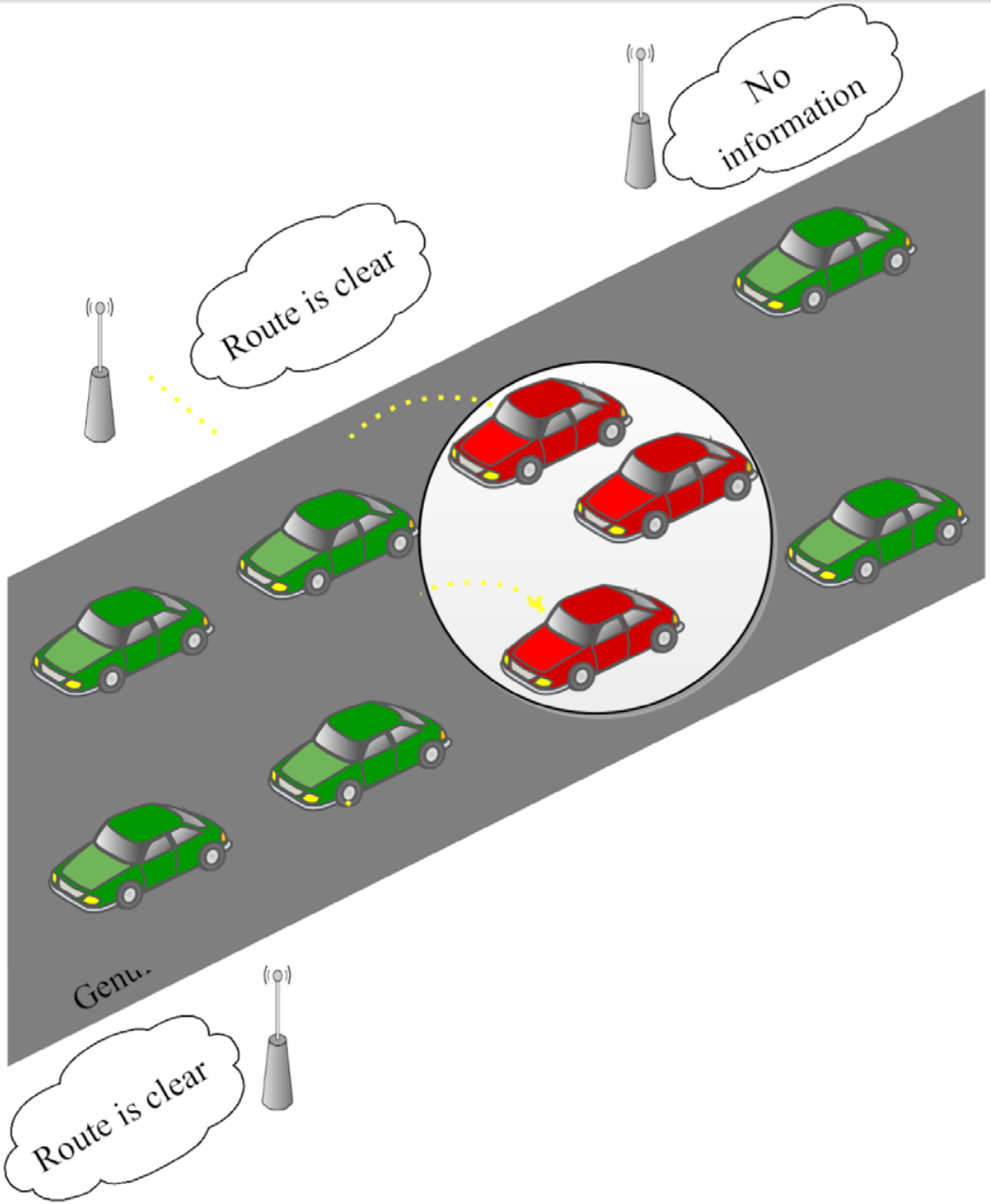
Ataques à disponibilidade:

- Os ataques à disponibilidade de serviços são denominados ataques de negação de serviço (DoSA), nos quais os serviços não são fornecidos aos nós da rede como deveriam. Existem vários tipos de ataques que ocorreram na disponibilidade.

- Ataque DoS: O usuário não consegue realizar as tarefas necessárias devido ao uso contínuo do nó pelo nó malicioso. Afeta diretamente a utilização adequada dos recursos disponíveis para verificar as mensagens. Com a natureza ampla da rede na VANET, ataques distribuídos de negação de serviço (DDoS) também são estendidos.


Malicious Vehicle
Genuine Vehicle
Traffic jam
Route is clear
Route is clear

- Ataque de buraco negro (black hole attack): No ataque de buraco negro, os nós do veículo são feitos para descartar todos os pacotes recebidos por eles em vez de encaminhá-los os pacotes para o próximo veículo que conduz ao veículo de destino. Tem três objetivos:
  - a O encaminhamento de vários pacotes fica comprometido de um nó veicular para outro.
  - b A recepção de pacotes de uma mensagem é inibida para um nó veicular.
  - c Todos os pacotes recebidos podem ser descartados pelo receptor.


No information
Route is clear
Route is clear

- Ataque de spam: A latência de transmissão na VANET aumenta muitas vezes, se um nó malicioso começa a enviar mensagens de spam para outros nós. Isso pode levar ao consumo ineficiente de vários recursos críticos, como o consumo de largura de banda.

- Ataque de interferência (jamming): em VANETs, o meio sem fio é compartilhado, o que permite que invasores mal-intencionados observem facilmente a comunicação e iniciem DoSAs por meio do processo de interferência ou interferência no caminho de comunicação. DoSAs baseados em interferência não podem ser endereçados por mecanismos ortodoxos. Os invasores podem desconsiderar o protocolo de acesso ao meio e transmitir continuamente no mesmo canal sem fio, evitando que o nó do usuário cometa operações MAC legais.

Ataque de medusas (Jellyfish attack): Um nó intermediário pode introduzir uma vulnerabilidade crítica para congestionar a rede TCP, o que pode alterar seu comportamento de encaminhamento. Os tipos de JFAs são os seguintes:

- a Ataque de Reordenamento: o nó reordena os pacotes antes de encaminhá-los; as confirmações não são recebidas em sequência. Portanto, as mensagens precisam ser enviadas novamente.
- b Ataque de queda periódica (PDA): os pacotes são descartados aleatoriamente durante os processos de comunicação e informações de congestionamento de rota são relatadas. Esta informação faz com que o nó tome a decisão de descartar uma fração de pacotes, por alguns milissegundos, o que aumenta o tempo limite de retransmissão.

- Ataque de buraco cinza (GHA): a camada de rede da VANET é direcionada e todos / alguns pacotes recebidos por um nó veicular são descartados. Algumas redes enfrentam o problema da taxa de entrega de pacotes e um aumento na sobrecarga ocorre durante o ataque de cinza. Os GHAs são difíceis de detectar devido à sua natureza dupla; isto é, uma rede normal e maliciosa pode encaminhe todos os pacotes para um nó de destino durante a transmissão.

- Ataques de comportamento ganancioso: ataques a VANETs também ocorrem com intenções gananciosas, em que um motorista visa usar recursos de rede apenas para si mesmo, criando uma ilusão para outros nós veiculares e fazendo-os passar por rotas alternativas e obter um caminho claro para o destino.

Ataques à confidencialidade

- A confidencialidade dos dados deve ser mantida em redes, visto que os dados são altamente confidenciais, devido à consideração do comunicações de dois veículos e seus padrões de movimento. Isso pode ser ainda mais dificultado ou verificado por meio de intenções maliciosas.

- Ataque man-in-middle: em ataques man-in-middle, o invasor malicioso se envolve na rede e recebe uma mensagem do remetente. Esta mensagem é modificada e enviada ao destinatário. Devido a isso, o remetente / receptor obtém as informações erradas do invasor, enquanto presume que a mensagem é verdadeira e confiável. Esse ataque pode ser detectado usando uma chave de sessão individual para cada transferência de mensagem para criptografar a mensagem. Se a mensagem for interceptada no meio, ela não poderá ser descriptografada pelo invasor. Portanto, não há espaço para realizar atividades maliciosas.

- Ataque de espionagem: No ataque de espionagem (EA), os invasores mal-intencionados tentam obter a chave de sessão de comunicação em andamento e começam a escutar sem autorização ou roubar os parâmetros de comunicação.

- Ataque de análise de tráfego: aqui, o conhecimento sobre os veículos é coletado de forma maliciosa com base nas informações interceptadas da rede com intenções maliciosas. É uma forma de ataque passivo, que analisa o fluxo do pacote de tráfego e categoriza os nós por sua importância e os ataca estrategicamente.

Soluções

Type of Attacks	Security Aspect	Cryptographic Solution
Eavesdropping	Confidentiality	Symmetric encryption of secure messages
Denial of Service	Availability	Digital Signature
Jamming	Availability	Frequency hopping technique
Traffic Analysis	Confidentiality	Securing Traffic Pattern
Message Tempering	Integrity	Similarity algorithm, integrity matrics
Impersonation	Authentication	Variable MAC and IP addresses
Unlawful Tracking	Privacy	Set of anonymous key changes, certified Authority
Brute Force	Confidentiality	Strong encryption and key generation algorithm
Fake Position	Authentication	Using signature with GPS
Sybil Attack	Availability	Deploy central validation authority

Cybersecurity in Tesla — The Future of Security in Car Automation `https://youtu.be/RHOyOFG0Th8`

Trabalho

Fazer um resumo sobre o trabalho final da disciplina. Qual o tema? Como será explorada a ideia? O que pretende-se mostrar na apresentação?