Controller Area Network

The Controller Area Network (CAN) has been the automotive standard for connecting Electronic Control Units (ECU’s) for more than 25 years.
- Connects all ECU’s within the vehicle through a common bus
- Broadcast Nature allows every node to see all transmitted messages
- Message Priority field determines order of transmission
- Fault-Tolerant, Unencrypted, 1Mbps transfer rate

Entry Points
- Bluetooth and Wi-Fi connections
- CD Media Player
- On-Board Diagnostics Port

Potential Attacks
- Priority Flooding (Availability)
- Suppress Target Node (Availability)
- Modify Target Message (Integrity)

Vehicular Sensor Network

A Vehicular Sensor Network (VSN) represents the interconnectivity of smart vehicles and the infrastructure supporting them. VSN’s support Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication to share information on road and traffic conditions. Integrity of this information is vital in order to prevent traffic congestion and vehicle collisions.

Communication Protocols
- Dedicated Short-Range Communication (DSRC)
- Wireless Access in Vehicular Environment (WAVE)
- Ad-hoc On-demand Distance Vector (AODV)

Vulnerabilities
- Malicious vehicles can provide false information (Integrity)
- Black Hole attackers may interrupt data transmission (Availability)

Definitions

ECU = Electronic Control Unit
CAN = Controller Area Network
OBD = On-Board Diagnostics Port
VSN = Vehicle Sensor Network
RSU = Roadside Sensor Network

Solution

CAN Security Scheme
Most vulnerable interfaces are part of the Infotainment system. These devices should be separated from safety-critical features by the security module. Additionally, a two-phase encryption scheme is implemented (1).

1. ECU Authentication (Public Key): Upon startup, the Security Module (SM) broadcasts its certificate \( K_{SM} \) and Public Key \( K_{PUB} \) across the network. Each ECU on the network should verify SM’s authenticity using \( K_{SM} \) before responding with a registration message. The registration message for node \( n \) includes its certificate \( f_n \) and a symmetric key \( k_n \) to be used during Stream Authorization. All registration messages are encrypted with \( K_{PUB} \). The Security Module decrypts registration messages with its Private Key \( K_{PUB} \) and saves \( k_n \) for each ECU with a valid certificate.

2. Stream Authorization (Symmetric Key): During operation, CAN messages are authorized using lightweight Symmetric Key Encryption. When CAN node wants to transmit a message, it must first request stream access. If the Security Module recognizes \( n \) as an authenticated ECU, it provides a symmetric key \( k_n \) to the source ECU, as well as all intended destinations. ECU \( n \) will encrypt its message with \( k_n \) and transmit the stream. Now only the message’s intended destinations have \( k_n \) and may decrypt the message.

VSN Security Scheme

Registration: In order to prevent an infinite number of malicious nodes from freely accessing the VSN, each user must register with valid identification such as Driver’s License/SSN, before being issued a smart card which enables access to the network.

Login: When a valid user wishes to access a VSN, they must first login with their smart card and credentials. The user is then issued a Public Key \( K_{PUB} \) and Private Key \( K_{PRV} \) to encrypt, decrypt, and sign messages with.

Management: Road-Side Units (RSU’s) act as the computation hubs of a VSN. RSU’s are responsible for validating users, distributing keys, collecting information, and authenticating messages. Batch message authentication may be used to improve performance. To authenticate a message, its signature must be checked against the list of valid users. If a batch contains any illegitimate signatures, the batch is rejected (2).

Removing Attackers: A Black Hole Attacker, for example, is one who always claims to have the freshest route to a destination, but drops packets instead of routing them. This can be detected by sending a ping to the intended destination. If no valid response is received, the node claiming to have a route can be reporting as suspicious. The RSU will then issue a fake route request to the suspicious node as bait, as seen in figure three. If the suspicious node responds to the fake request, it will be considered malicious and removed from the network (3).

Encryption

Symmetric Key Encryption:
Each pair of nodes shares a secret key value. This shared key is used to both encrypt and decrypt messages between two nodes.

Public Key Encryption:
In a public key system, each node \( n \) has a public key \( K_{n}^{*} \) and a private key \( K_{n} \). Public key \( K_{n}^{*} \) is used by other nodes to encrypt a message destined to node \( n \). Then, \( n \) uses its private key \( K_{n} \) to decrypt the messages. Private keys are also used for message signatures.

Bibliography