AESIN
AUTOMOTIVE ELECTRONICS INNOVATION

AESIN Conference 2017

BIRMINGHAM CITY University

Title: Security Issues in LTE-enabled V2X Communication Systems

Mujahid Muhammad

PhD Student, Centre for Cyber Security, Birmingham City University

Mujahid.Muhammad@mail.bcu.ac.uk

AESIN
AUTOMOTIVE ELECTRONICS INNOVATION

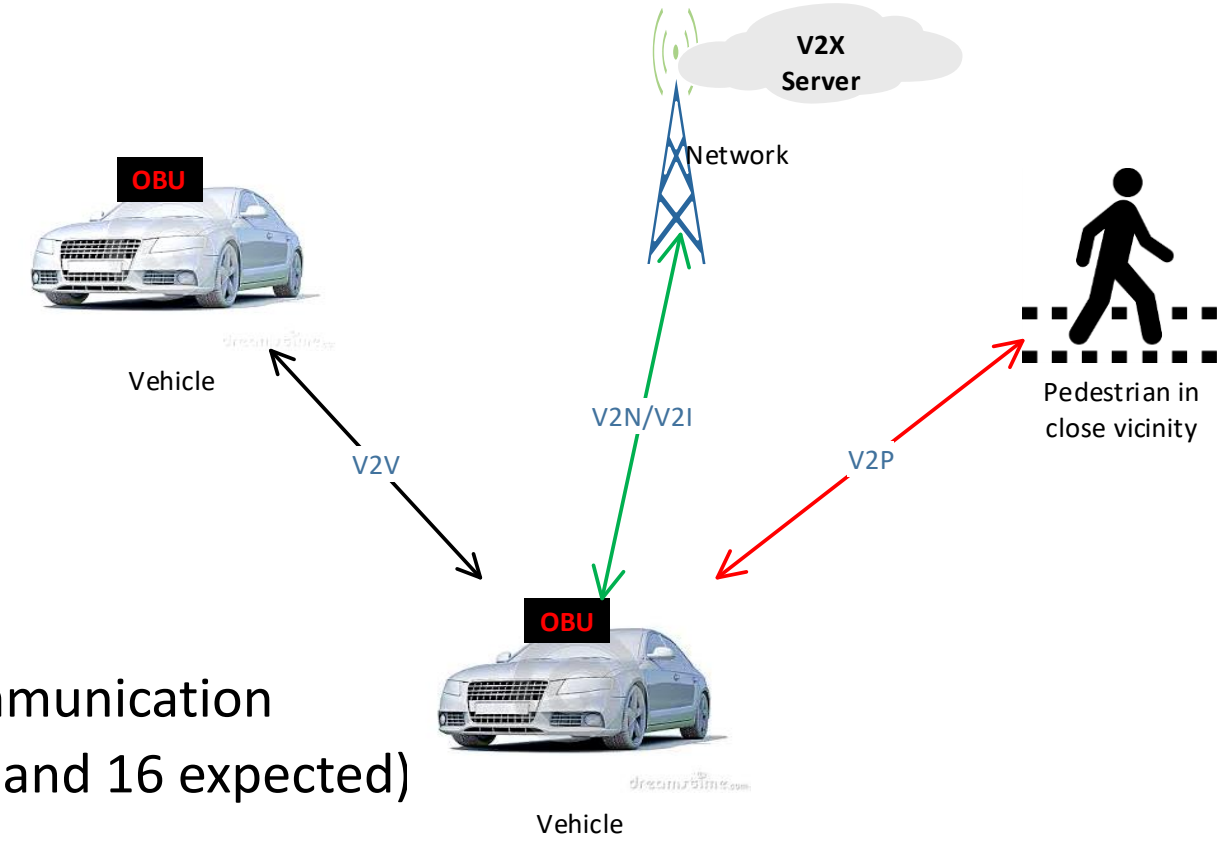
BIRMINGHAM CITY University

Content

- What is V2X Communication ?
- V2X Applications and Services
- V2X service requirements
- V2X Threats and Attacks
- Network security and privacy in V2X
- Proposed solutions
- Future work

Vehicle to Everything (V2X) Communication

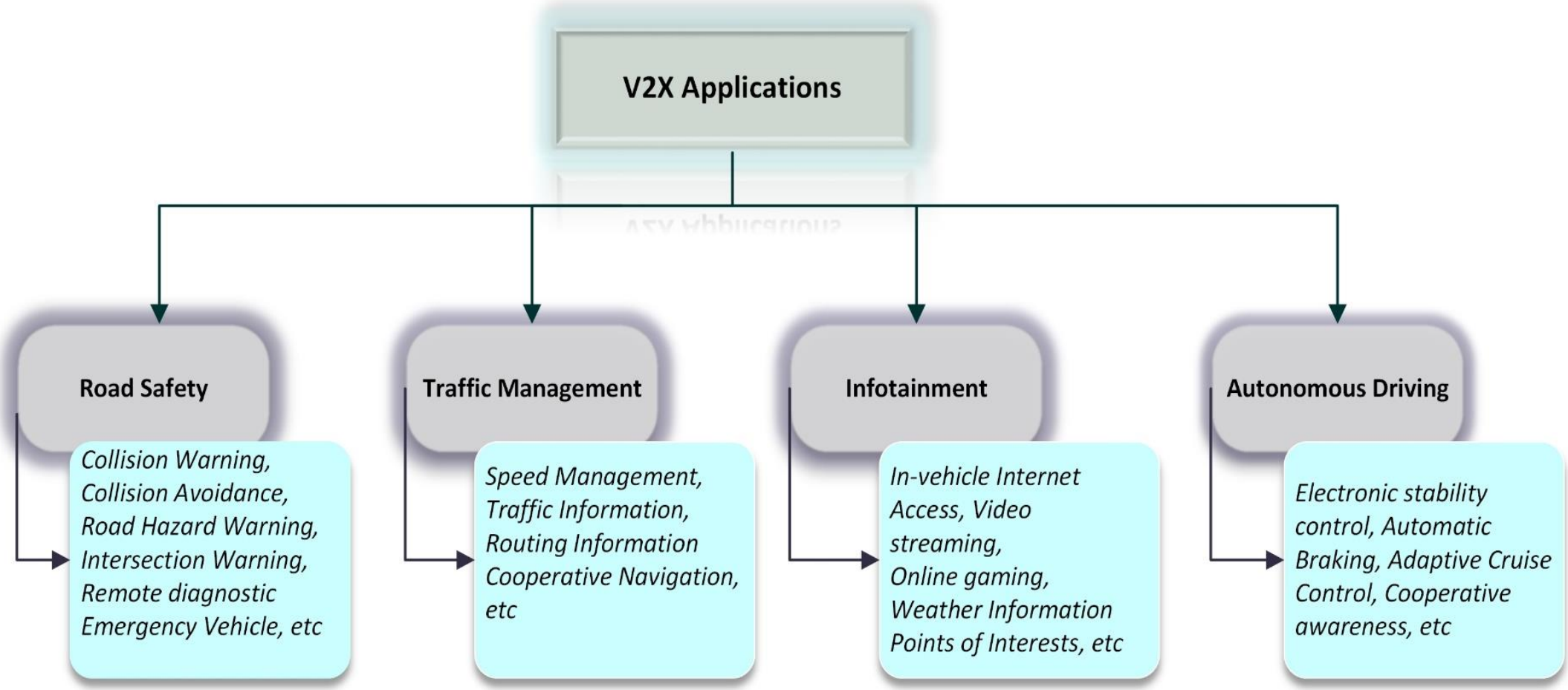
- Connecting vehicle to everything for safety and non-safety services;
  - Vehicle to Vehicle (V2V)
  - Vehicle to Network (V2N)
  - Vehicle to Infrastructure (V2I)
  - Vehicle to Pedestrian (V2P)



- One of the fastest growing type of connected devices after smart phones

- V2X is one of the core areas of IoT
- 3GPP have approved support for V2X communication in LTE-A network (C-V2X Release 14, 15+, and 16 expected)

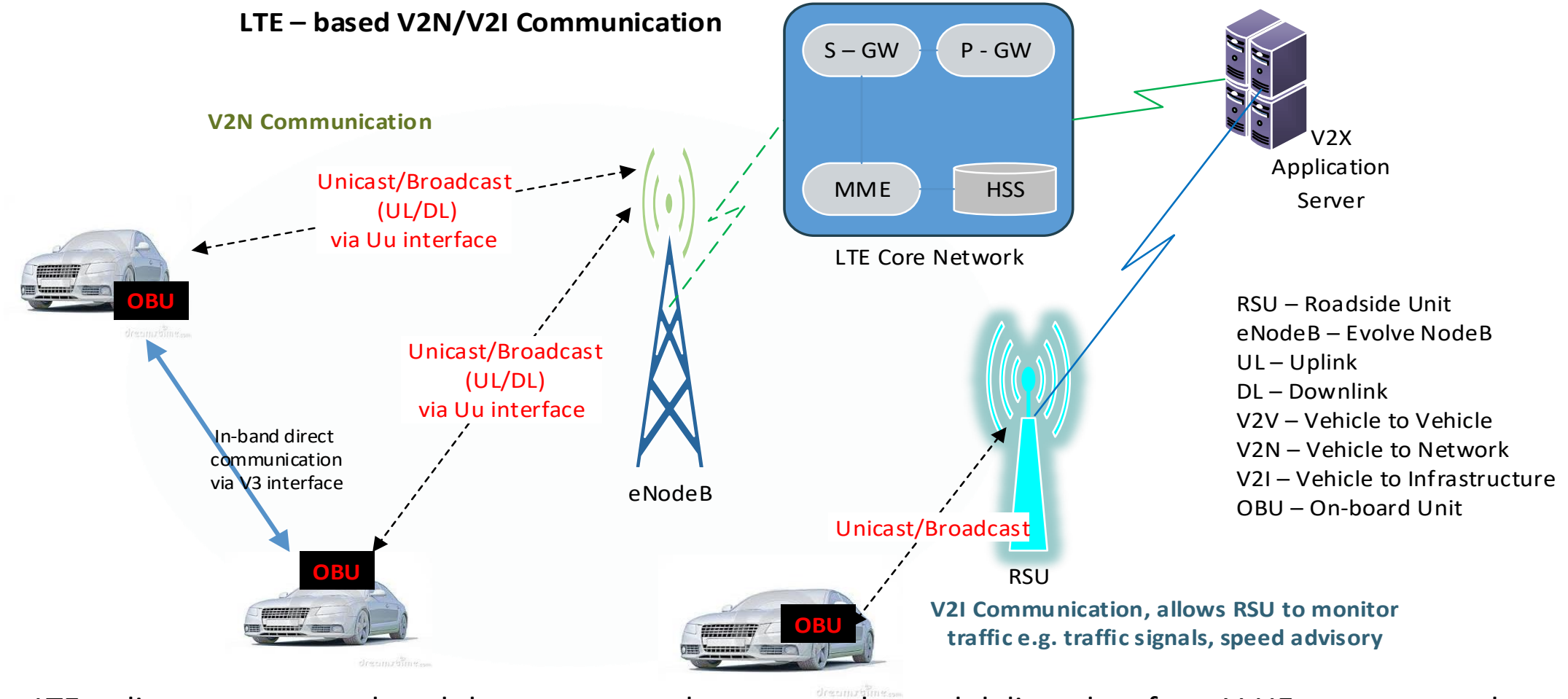
V2X Applications



Why is V2X important?

- V2X services promises to improve the efficiency and safety of today's road transportation system by;
  - Reducing road accidents
  - Creating efficient traffic movement
  - Reducing Co2 emission and fuel consumption
  - Enhancing the comfort of road users

LTE – based V2X Architecture



The LTE radio access network and the core network serve to relay and deliver data from V-UE to an external V2X server

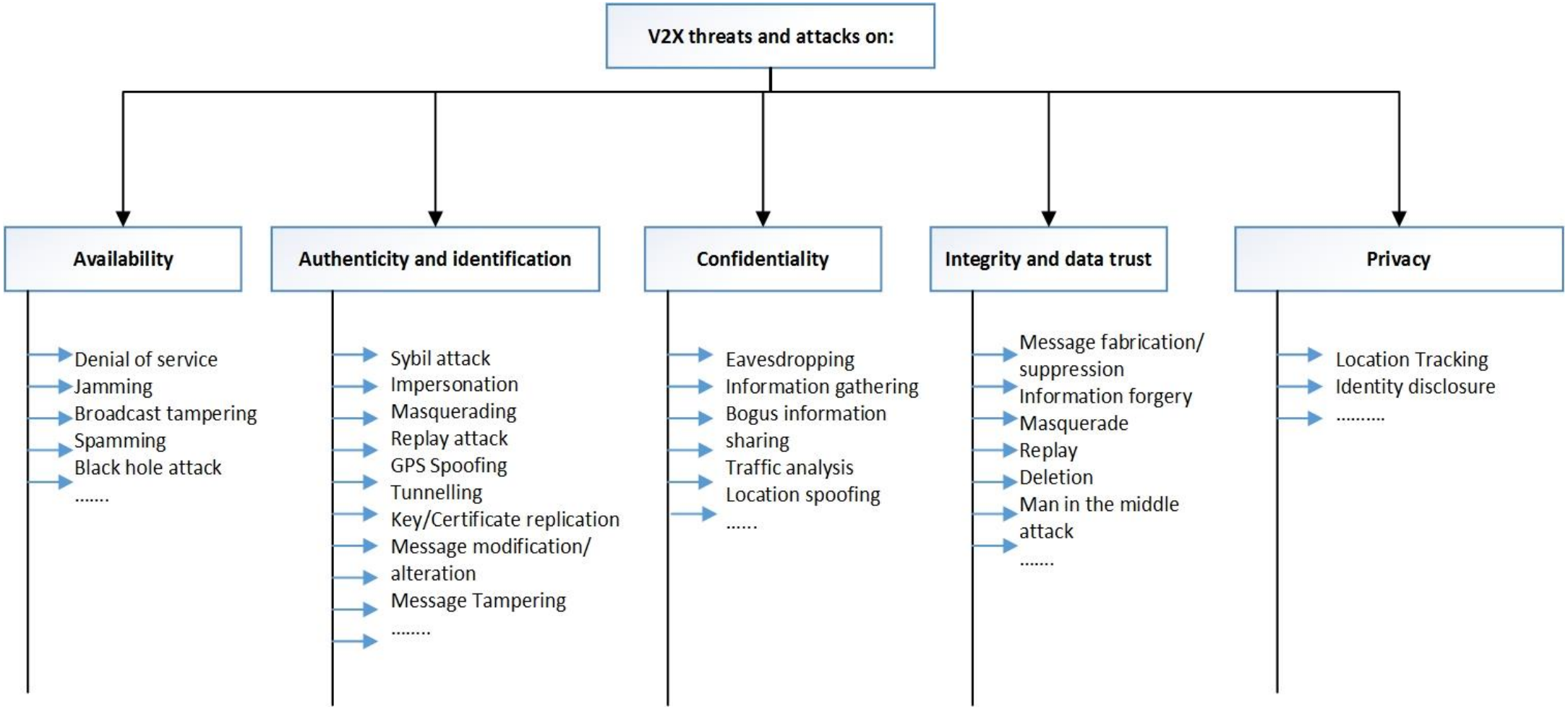
LTE-V2X offers key advantages

- Enhanced coverage
- High mobility support
- High density support
- Widely deployed Infrastructure
- Native V2N support by leveraging existing, ubiquitous cellular networks
- V2V support potentially through direct D2D technique
- Transmission mode
  - Unicast
  - Broadcast through MBMS (Multimedia Broadcast Multicast Service)
- Strong evolution path towards 5G

Characteristics of V2X Technology Evolution

- High mobility
- Dynamic network topology
- Unbounded network size
- Heterogeneous environment
- Lower latency for safety applications (e.g. maximum latency of 100ms, V-eNB-V communication)
- High reliability
- Wideband ranging and positioning

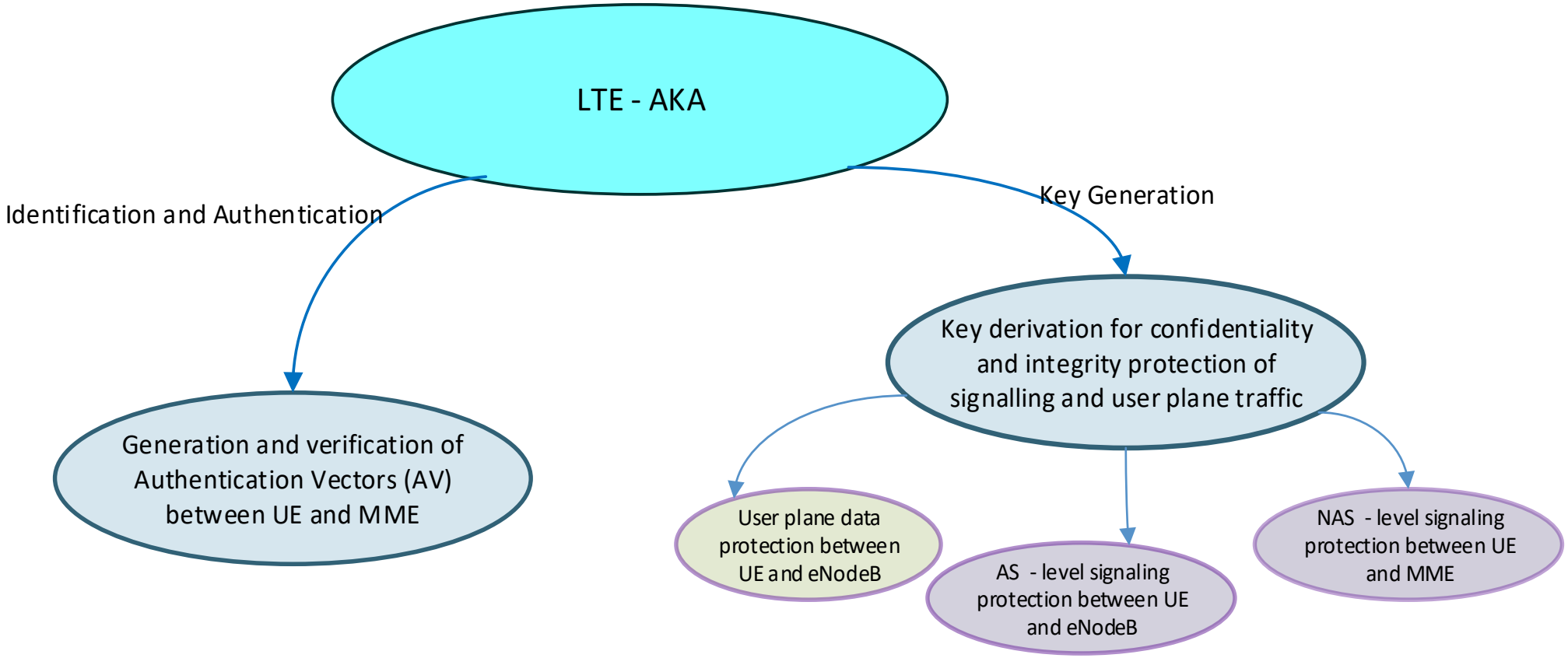
V2X Security: Types of Attacks on V2X



Network Security and Privacy in V2X

- Security is important in V2X communication, because V2X messages conveys sensitive, life critical real-time information that needs to be secured against attacks.
- Vehicles need to ensure the authenticity of the received message before reacting to the received information
- Security requirements between V-UE and the EPC network
  - Mutual authentication between V-UE and the serving network
  - Confidentiality and integrity protection of V2X messages
  - Privacy protection of vehicles and vehicle users
- Vehicles need to authenticate and verifies their legitimacy with network
- Providing secure communication in LTE-based V2X system is essential for the success of V2X services over LTE
- LTE – based V2X entities shall rely on the existing LTE access network security mechanism (i.e. LTE AKA)

LTE-AKA (Authentication and Key Agreement) Protocol



Subscriber credentials (permanent Key K, IMSI) resides on embedded UICC

V-UE

eNodeB

MME

HSS

Subscriber credentials

Access_request

ID_request

ID_response (IMSI)

Auth data_request (IMSI, SN Id)

Generate RAND and SQN, then Compute AV for the V-UE

$MAC = f_1(K,SQN||RAND||AMF)$

$XRES = f_2(K,RAND)$

$CK = f_3(K,RAND)$

$IK = f_4(K,RAND)$

$AK = f_5(K,RAND)$

$AUTN = SQNXORAK||MF||MAC$

$K_{ASME} = (CK||IK||SQN||RAND||AMF)$

Auth data_response (RAND, XRES, K_{ASME}, AUTN)

Auth_request (RAND, AUTN)

Retrieves SQN, MAC from AUTN and then Computes

$XMAC = f_1(K,SQN||RAND||AMF)$

$RES = f_2(K,RAND)$

$CK = f_3(K,RAND)$

$IK = f_4(K,RAND)$

$AK = f_5(K,RAND)$

Compares XMAC = MAC?

If successful, then computes

$K_{ASME} = (CK||IK||SQN||RAND||AMF)$

Auth_response (RES)

Compares XRES = RES?

Mutual Authentication and Key Establishment

Issues with LTE-AKA

- Reveals client identity
- Delay authentication procedure
- Absence of quick re-authentication during handover situation
- Overhead calculation
- Desynchronization attack

What is required

- Enhancement and optimisation to the authentication procedures of LTE-AKA are necessary
- Security protocols must be implemented with low communication overhead due to time constraint and low computation complexity to exchange quick and safe information
- The security protocols should have minimal impact to core network
- The security protocols should comply with the 3GPP standard with minimal modification

Existing Solutions Proposed in the Literature

- Group – based authentication and key agreement schemes
  - Reduce authentication time and signalling load to HSS and MME
  - Avoid congestion
  - Group formation is a bottleneck in V2X context due high mobility of vehicles and rapid network topology changes
- Enhancing LTE-AKA using PKI
  - Incurs high computational, communication, storage and management overheads
- Current methods not fully satisfactory

Proposed Solutions

- Moving the AV generation to MME using virtualization technologies
- Optimization of the signalling handshake for connection management and authentication procedures
- Leveraging LTE security mechanisms with SDN and NFV towards 5G security innovations

Future Work

- Design and Implementation of enhanced security algorithms using appropriate components
- Testing and performance analysis to demonstrate security features

AESIN
AUTOMOTIVE ELECTRONICS INNOVATION

BIRMINGHAM CITY University

Thanks for listening, any question please?