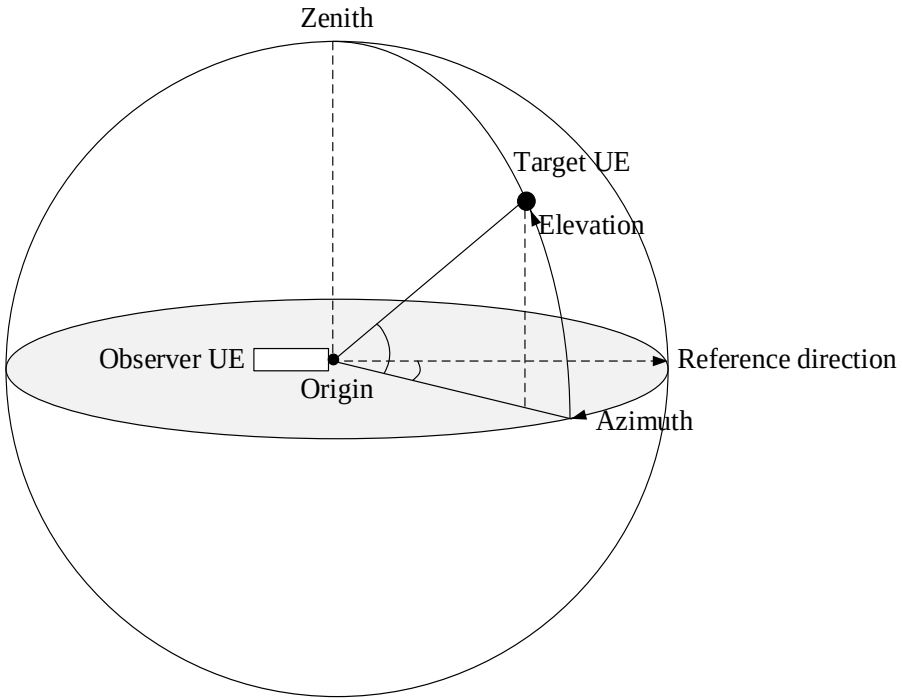
Security Aspects of Architecture Enhancement supporting Ranging-based Services and Sidelink Positioning

Xiaomi

Definition of Ranging

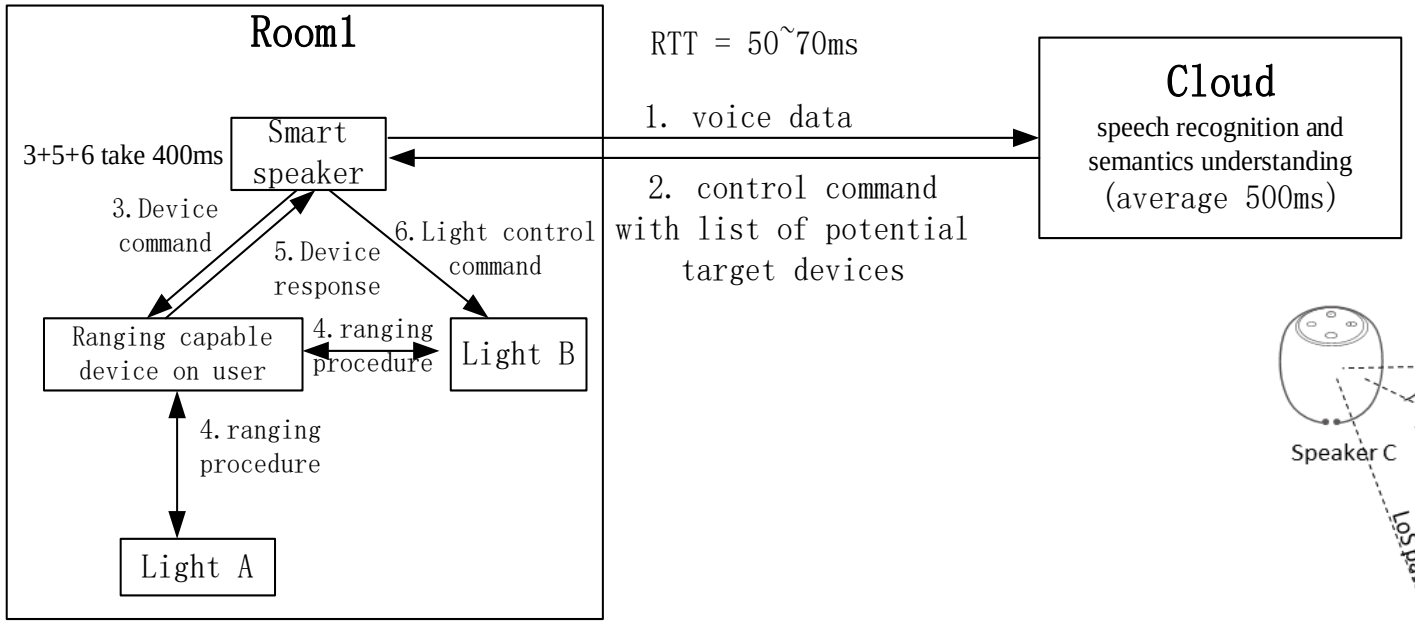
source from TS 22.261 and TR 22.855

- Ranging refers to the determination of the distance between two UEs and/or the direction of one UE (i.e. Target UE) from the other one (i.e. Observer UE), via direct communication connection
  - In 3D case, direction includes horizontal direction and elevation direction
  - Relative distance between 2 UEs can be derived based on ranging
- Ranging-based services can apply to a variety of verticals, such as consumer, smart home, smart city, smart transportation, smart retail, and industry 4.0



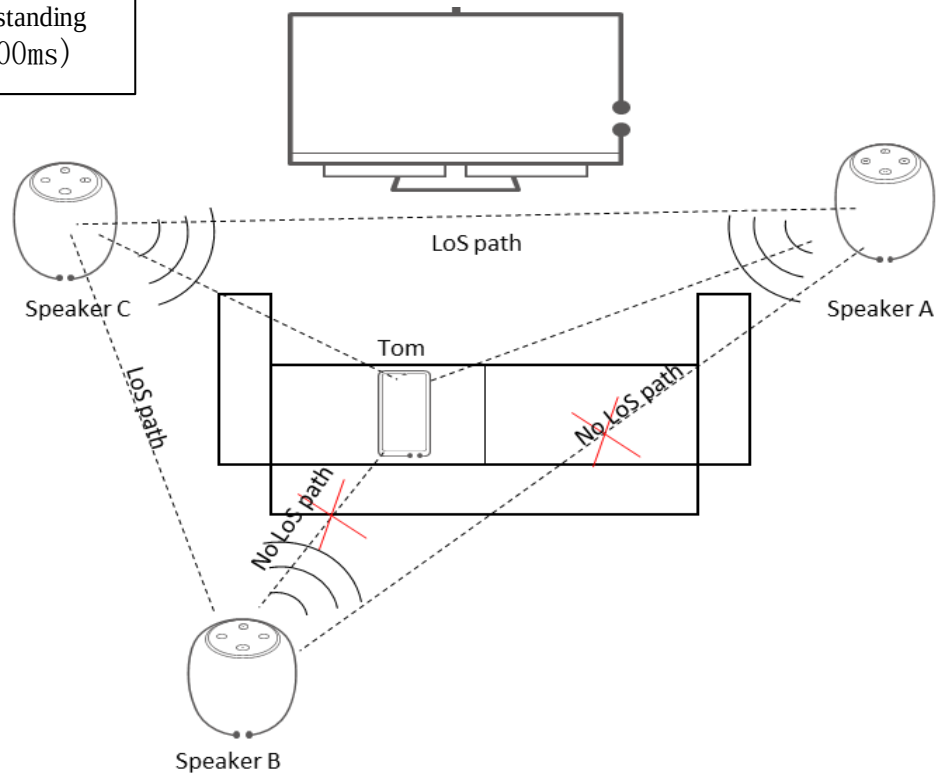
Use Cases

source from TR 22.855



Distance-based Smart Home Device Control

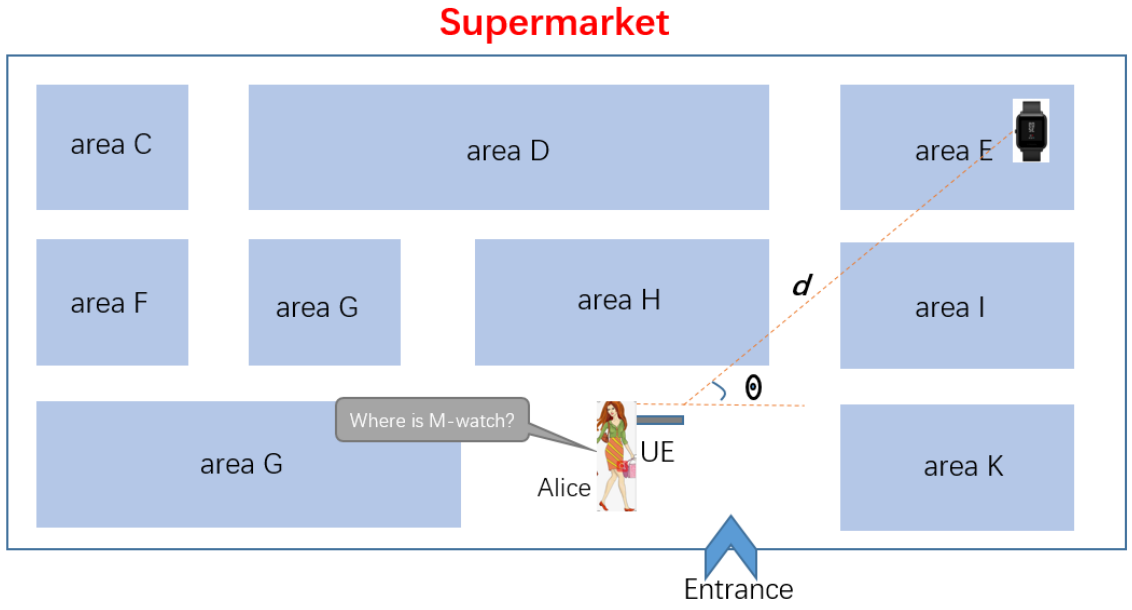
Immersive sound based on multiple-UE ranging

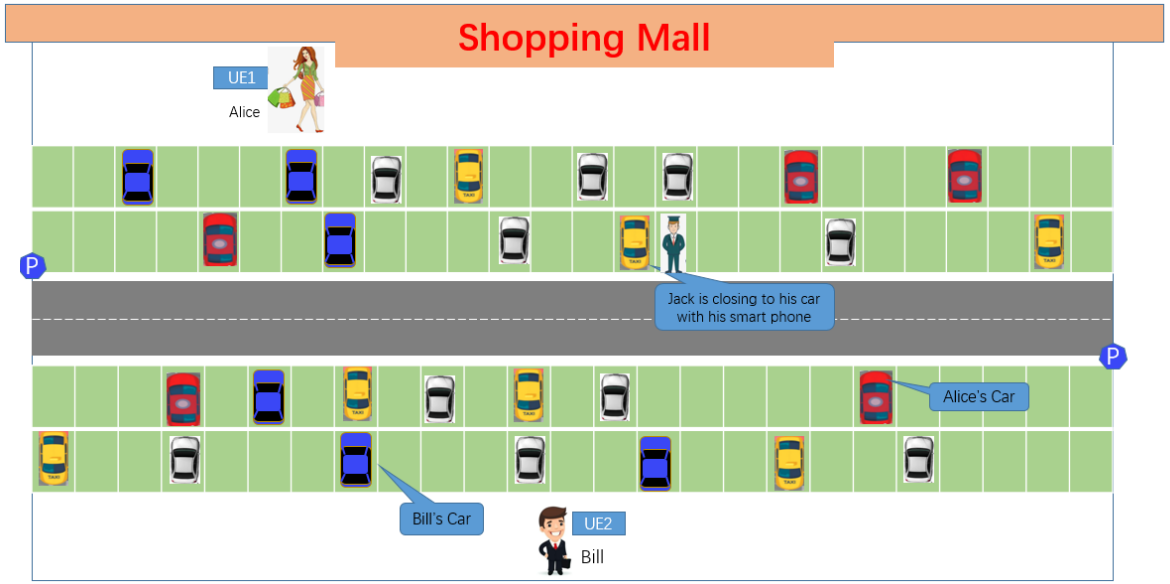


Use Cases

source from TR 22.855

Finding items in a Supermarket

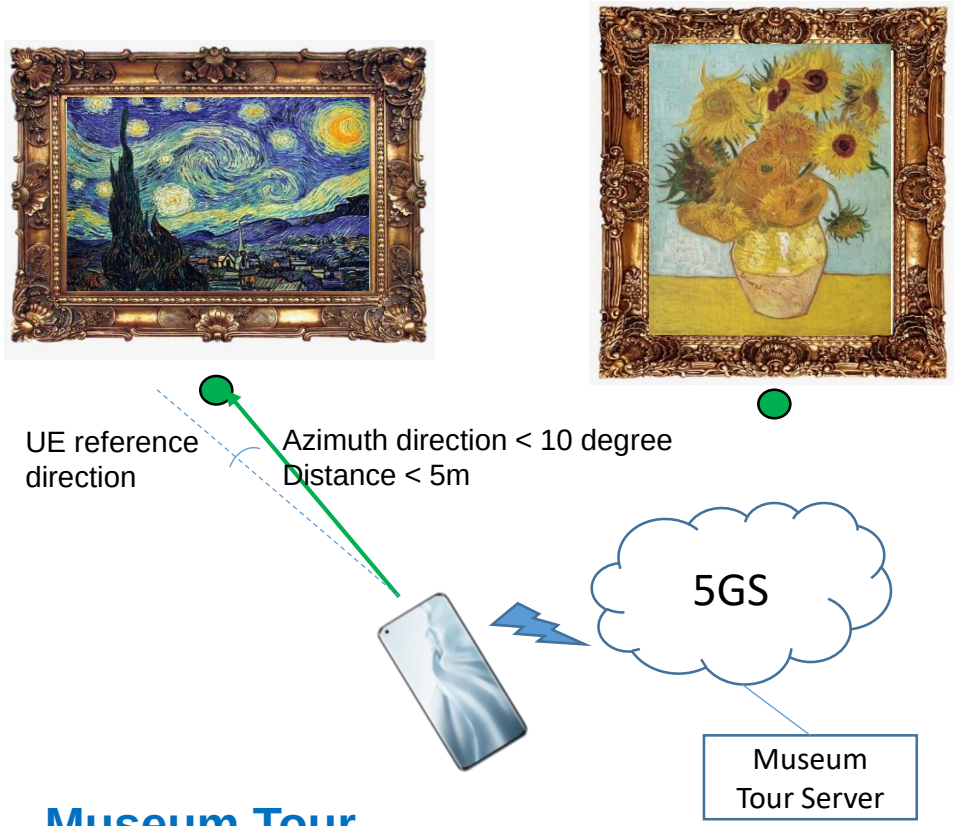




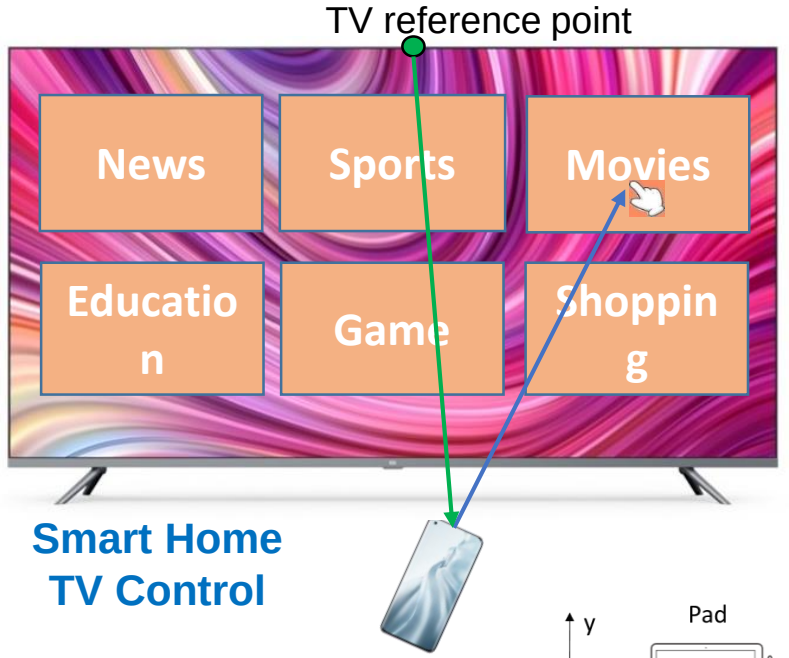
Smart Vehicle Key

Use Cases

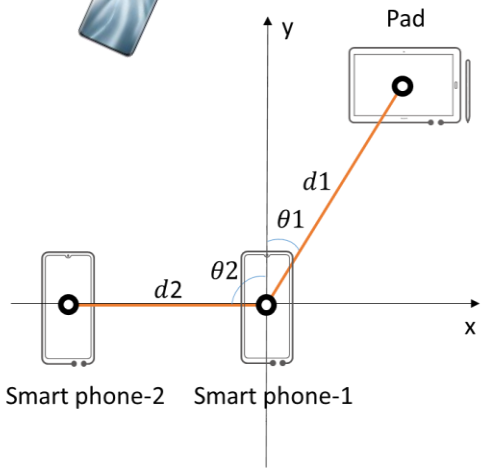
source from TR 22.855



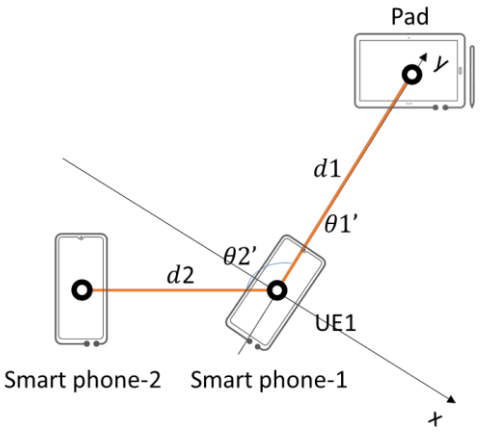
Museum Tour



Smart Home TV Control



(a) Smart phone-1 points nowhere at t1



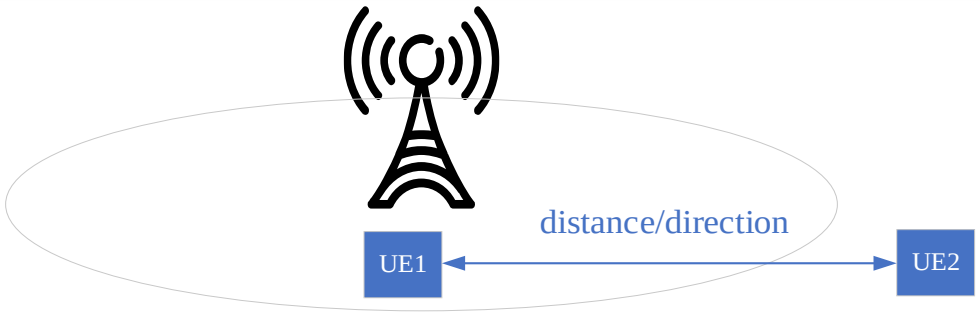
(b) Smart phone-1 points to Pad at t2

Picture and video sharing based on ranging results

Scenarios

source from TS 22.261 clause 6.37.1

In 5G coverage



Partial 5G coverage

Out of 5G coverage

- Ranging-based positioning and services can be supported with 5G coverage, with partial 5G coverage, or without 5G coverage.
- Both licensed and unlicensed spectrum can be used for ranging. If licensed spectrum is used, it shall be fully under operator control.

Ranging related Work in 3GPP

Unique ID	***Title***	***Nature of Relationship***
880039	Study on Ranging-based Services	SA1 study item on use cases scenarios and service requirements of Ranging-based Services
910034	Stage 1 for Ranging	SA1 work item on service requirements of Ranging-based Services
820024	Improvement of V2X Service Handling	SA1 work item on requirement on relative position between UEs supporting V2X application
880075	Study on scenarios and requirements of in-coverage, partial coverage, and out-of-coverage NR positioning use cases (RP-201518)	RAN2 study item (Rel-17) on use cases and service requirements of sidelink positioning between UEs supporting V2X and public safety services
940069	Study on Ranging based services and sidelink positioning (SP-211647)	SA2 study item (Rel-18) on architecture enhancement for supporting Ranging based services and sidelink positioning
N/A	NR Positioning Enhancements (RP-212706)	RAN work item (Rel-18) on NR Positioning Enhancements

Requirements from SA1

source from TS 22.261 clause 6.37.2

- The 5G system shall be able to protect privacy of a UE and its user, ensuring that no identifiable information can be tracked by undesired entities during ranging.
- The 5G system shall be able to ensure the integrity and confidentiality of ranging information used by ranging-enabled UEs.
- The 5G system shall be able to ensure that user privacy is not violated during ranging, e.g., subject to regional or national regulatory requirements.
- The 5G system shall be able to ensure security protection (e.g., interworking security) when the ranging concerns UEs subscribed with different operators.
- The level of security provided by the existing 5G system shall not be adversely affected when ranging is enabled.
- The 5G system shall support means to securely identify other ranging capable UEs, with which a certain UE can perform ranging.

Objectives of SA2 SID

source from SP-211647

- Work Task: Architecture enhancements to enable Ranging Service and sidelink positioning, which include:
  - Authorization and policy/parameter provisioning for a UE or a group of UEs;
  - Ranging device discovery and service operation procedures between two UEs, between one UE and multiple UEs or via the assistance of another UE;
  - Ranging and sidelink positioning service exposure to a UE or an Application Server who has requested the service.
- NOTE 1: For direct communication related aspects, V2X or ProSe architecture is used as the basis, and V2X and ProSe solutions will be reused as much as possible. Coordination with FS_5G_ProSe_Ph2 study may be required if any impact to R18 ProSe solution is identified.
- NOTE 2: This study is focusing on providing ranging and relative positioning result of the target UE based on PC5 measurement or absolute positioning of the target UE based on PC5 measurement and an already known location of the observer UE.
- **NOTE 3: Privacy protection and other security aspects will be tasked to SA3, and the related impact to architecture enhancement will be based on SA3 conclusion.**
- NOTE 4: Architectural implications to RAN or RAN dependent aspects will be coordinated with RAN WGs.
- NOTE 5: Energy efficiency aspect need to be taken into account for ranging and sidelink positioning operation.

Proposals in SA3

- Identify the security key issues, threats, and potential requirements for Ranging based services and sidelink positioning;
- Analyse the gaps between the security key issues for Ranging based services and security key issues for ProSe and V2X applications;
- Study the potential solutions addressing the security key issues specific to Ranging based services and sidelink positioning;
- Align with SA2 / RAN for security implications on architecture enhancement / RAN dependent aspects.

NOTE: For security protection on discovery and direct communication, the existing solutions for ProSe and V2X will be reused as much as possible.