IBS Enabled Authentication for IoT in ION Framework

Donghui WANG[*] and Bin DA[+]

Shield Lab[*], NGIP Lab[+], Beijing Huawei Digital Technologies Co., Ltd.

www.huawei.com

HUAWEI TECHNOLOGIES CO., LTD.

HUAWEI

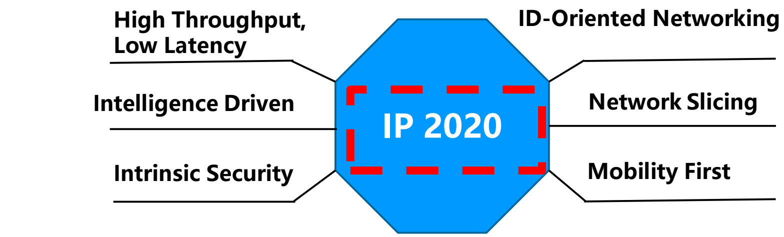
Huawei Network Technology Laboratory (NTL)

- In recent decades, network technologies have been changing the life style of human society in every aspect across the world. From analog switching, TDM and ATM, to IP-enabled networks, networking technologies have experienced four major technological leaps. How will network technologies keep evolving for a better connected world in the future? That is a key question which is destined to answer in **Net5.0**.
- Huawei has launched research on future network technologies since late 2014, which is currently positioned to be of strategic importance for Huawei company. Accordingly, Network Technology Laboratory (NTL) is formally established in 2015 for this purpose, with the mission to accomplish a smartly networking world that supports global reachability, all-time connectivity, pervasive mobility, adaptive optimization and ubiquitous security.
- As a pivotal organization for innovative research on network technologies under Huawei Central Research Institute, NTL's research areas cover Internet architecture, data center networks, mobile bearer networks, wireless core networks, Internet of Things (IoT), enterprise networks, industrial Internet and beyond.
- NTL is now cordially inviting global talents to join us for building a better connected world. Global Bases: Shenzhen, Beijing, Nanjing, Hong Kong in China; Munich in Germany; San Jose in USA; Paris in France.

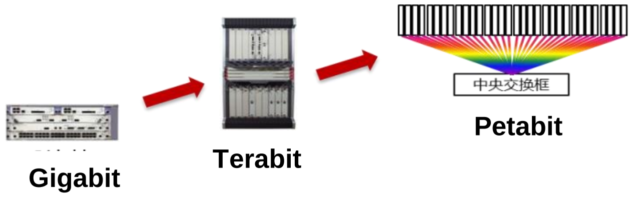
Overview of Network 5.0 - Programs

- Intelligence Driven
- P-Order Scale
- Ubiquitous Mobility
- High Throughput
- Low Latency
- Scale Up/Out
- Ethernet Everywhere

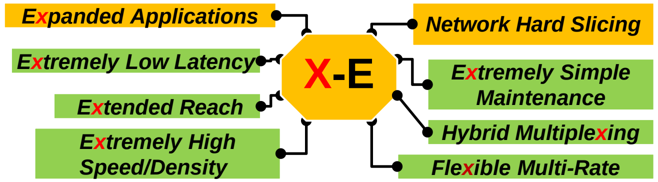
Next-Gen Internet Architecture and Protocols



All-Optical Petabit Router



X-Ethernet：More Flexible than FlexE



Network 5.0

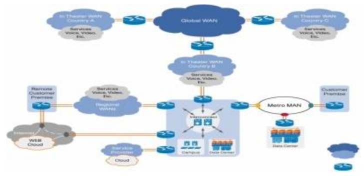
NG-DC

- Machine Learning
- Congestion Free
- Low Latency
- No Packet Loss

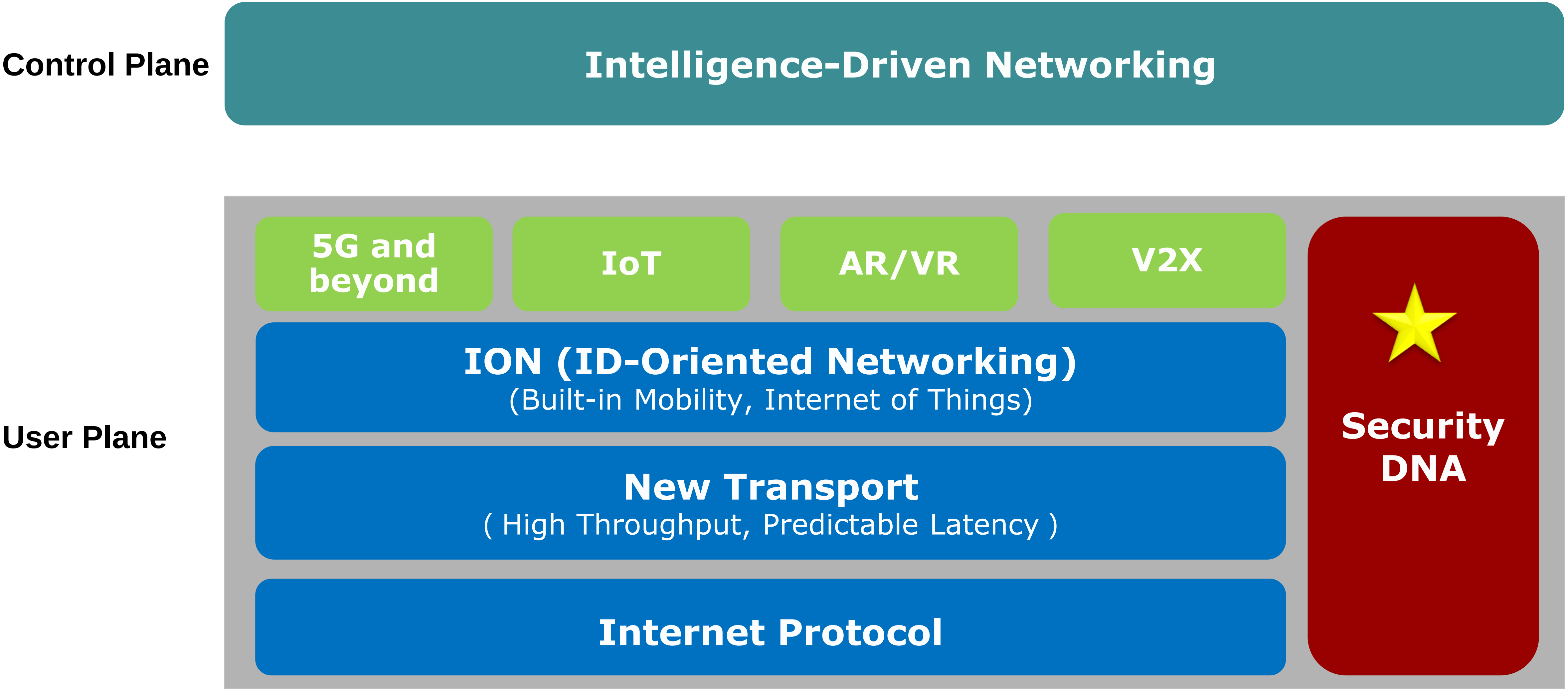
AR/VR Network

- High-throughput
- Deterministic
- Next-Gen CDN（Live – MDN）

Next-Gen Enterprise Network



IP 2020 Protocol Stack



Control Plane

Intelligence-Driven Networking

User Plane

5G and beyond

IoT

AR/VR

V2X

ION (ID-Oriented Networking)
(Built-in Mobility, Internet of Things)

New Transport
(High Throughput, Predictable Latency)

Internet Protocol

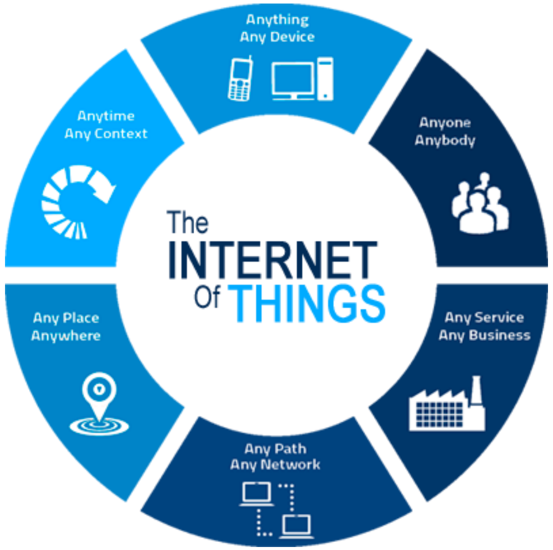
Security DNA

Outline of Paper Presentation

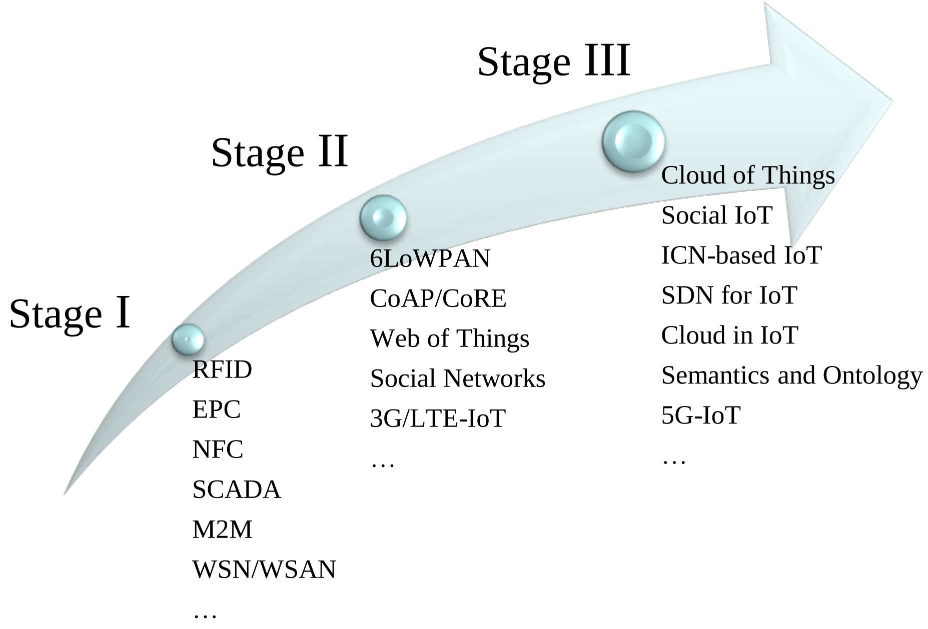
- **Introduction**
- **System Architecture Overview for Our Proposal**
- **IBS-enabled Authentication for Internet of Things (IoT)**
  - Basics of Identity Based Signature (**IBS**)
  - Partition of Trusted Zones (**TZ**s)
  - Initialization and Setup with Dynamic TZ of IBS-enabled Authentication for IoT Nodes
  - Inter-Zone Communication between Slave Nodes
  - Dual Authentication for Enhanced Security
- **Feasibility Analysis**
  - Computational Cost
  - Storage Cost
  - Transmission Cost
- **Conclusion and Future Work**

INTRODUCTION

- **Internet of Things (IoT): Things tend to get connected anytime, anyplace, with anything and anyone.**
  - Global infrastructure
  - Massive low power devices and intelligent things
  - Vulnerable for various attacks: (1) Physical attacks; (2) Simplified protocols; (3) IoT DDoS in Oct. 2016.



- **IoT Evolution**
  - **Stage I:** RFID and Variants (Tagged Things)
  - **Stage II:** Web of Things and Social (Web of) Things
  - **Stage III:** Cloud IoT, Social IoT, ICN-IoT, and more



OUR PROPOSAL

- **A solution for massive IoT authentication, using IBS with dynamic trusted zones in ION framework.**
  - **Global Reachability: ID Oriented Networking (ION)** has been recently proposed to satisfy future ubiquitous connectivity requirement by promoting persistent identities across heterogeneous entities (physical/virtual).
  - **Massive IoT Devices: Dynamically formulated Trusted Zones (TZs)** for relational IoT terminals, social trusted zone can reduce the complexity and suitable for massive IoT devices that are sensitive to computing and storage consumption, when resources are constrained.
  - **Authentication: Identity Based Signature (IBS)**
    - Be able to utilize all types of identification information as public keys (e.g., email, IP address, phone number) for signature and verification .
    - Does not reply on heavily centralized Public Key Infrastructure (PKI) , significantly reduces the complexity.

IBS-enabled Authentication for IoT

--- Basics of Identity Based Signature (IBS)

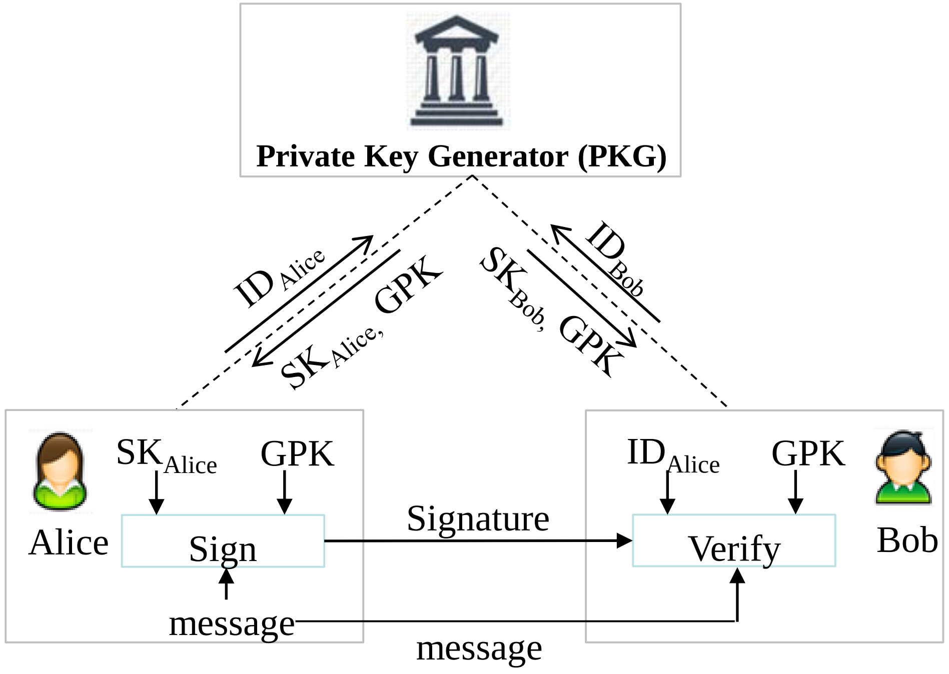
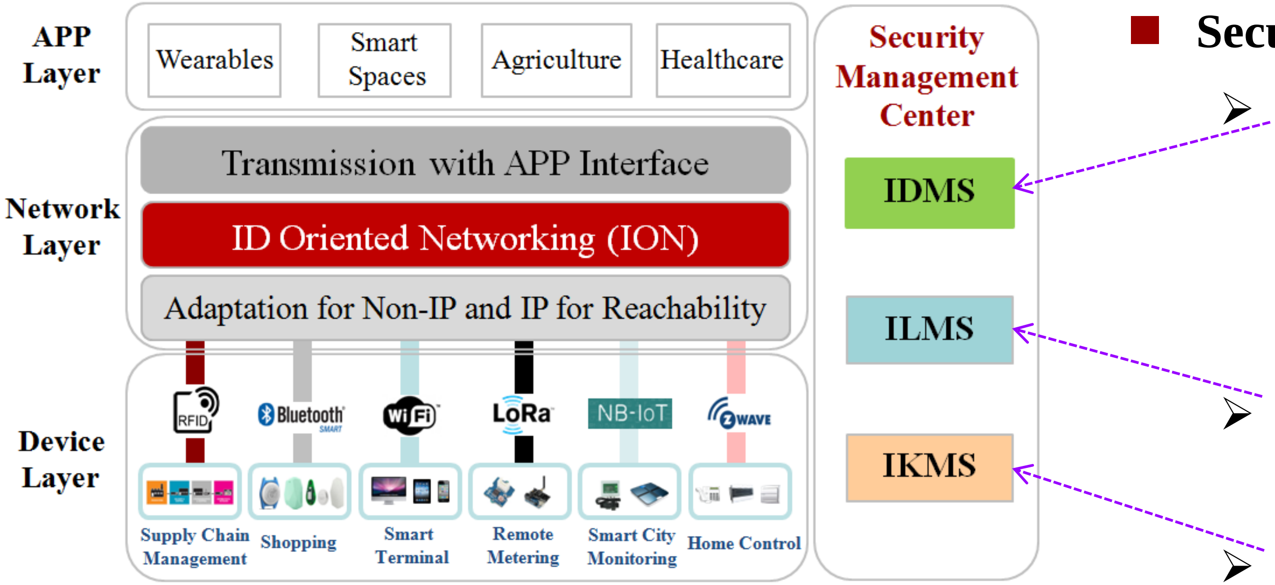


Illustration of IBS Basics

- **Brief introduction of IBS**
  - Any identification information of individual entities could be directly adopted as public key
- **Illustration of IBS Basics**
  - Alice obtains a Signing Key (SK), i.e., private key, associated with her ID information, from the Private Key Generator (PKG), i.e., IKMS.
  - Alice signs a message with Alice’s SK.
  - Bob as verifier uses Alice's ID to verify Alice's signature.
- **Merits of IBS**
  - Bob does not require Alice’s certificate for authentication.
  - Significantly reduce the system complexity and cost
  - SK and GPK can be preset, which enables the authentication to be fully distributed and to be suitable for IoT terminals.

System Architecture Overview



IBS-enabled IoT in ION Framework

- **Security Management Center (SMC)**
  - ➢ **IDMS** (IDentity Management System):
    - ✓ Manage the identities of all IoT devices
    - ✓ Handles ID registration, distribution, and ID-based relationships.
  - ➢ **ILMS** (Identity and Locater Mapping System):
    - ✓ Responsible for properly mapping IDs to locators
  - ➢ **IKMS** (IBS-based Key Management System):
    - ✓ Generate and distribute the private keys of all IoT devices.

- **The ION-based IoT Networks**
  - ➢ **Device layer:** A large number of heterogeneous IoT terminals, with distinct IoT connectivity technologies.
  - ➢ **Network layer:** Core of the architecture, while ID sub-layer is conceived for providing unique identifiers for all IoT nodes for eliminating underneath heterogeneity.
  - ➢ **Application layer:** Provides a variety of user-centric IoT applications.

Partition of Trusted Zones

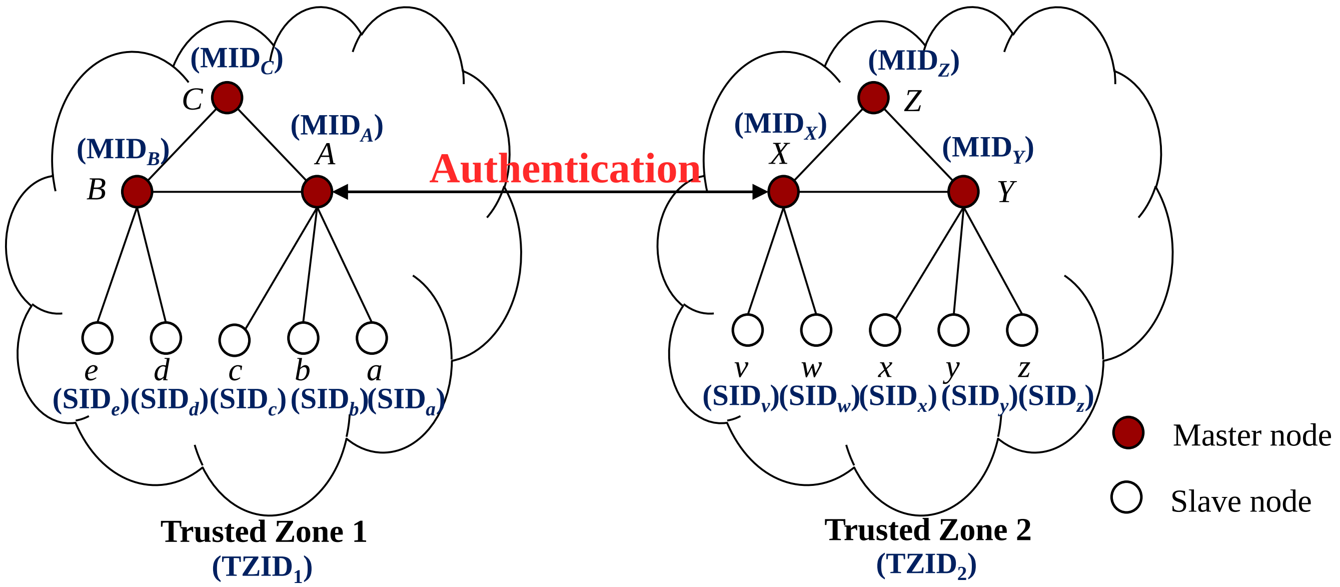
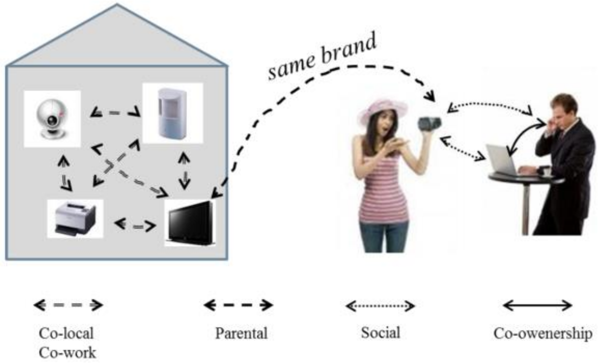


Illustration of Trusted Zones

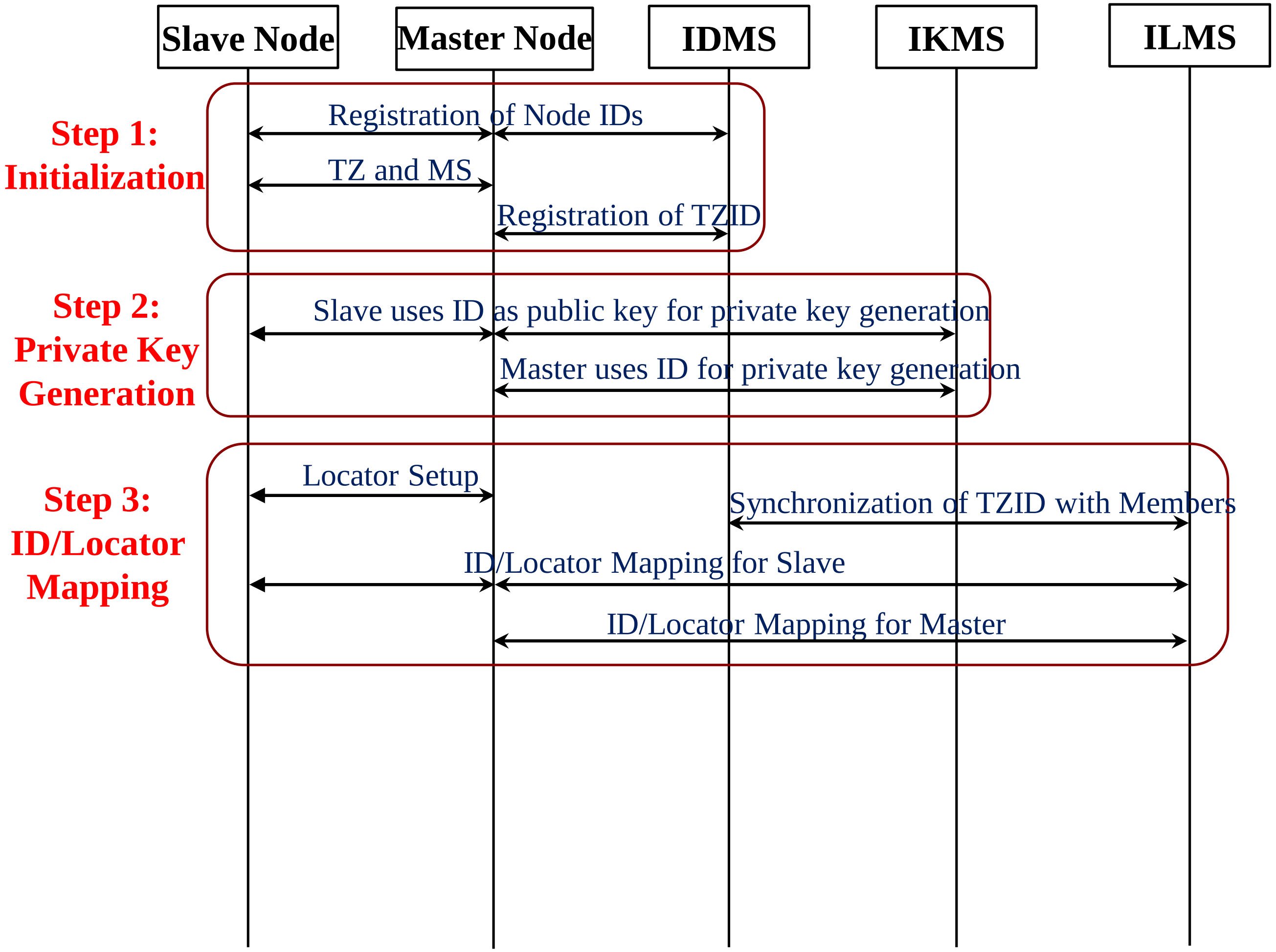
Trusted Zone, 128-bit ID	Master Node(s), 128-bit ID	Slave Node(s), 128-bit ID
Trusted Zone 1 TZID$_1$	Master Node *A*, MID$_A$ Master Node *B*, MID$_B$ Master Node *C*, MID$_C$	Slave Node *a*, SID$_a$ Slave Node *b*, SID$_b$ Slave Node *c*, SID$_c$ Slave Node *d*, SID$_d$ Slave Node *e*, SID$_e$
Trusted Zone 2 TZID$_2$	Master Node *X*, MID$_X$ Master Node *Y*, MID$_Y$ Master Node *Z*, MID$_Z$	Slave Node *v*, SID$_v$ Slave Node *w*, SID$_w$ Slave Node *x*, SID$_x$ Slave Node *y*, SID$_y$ Slave Node *z*, SID$_z$

- **Social IoT (SIoT): In terms of social relationships, some IoT terminals can be linked in advance to dynamically form a trusted zone [Ref: http://www.social-iot.org/]**
  - **OOR**: IoT nodes belong to the same owner. E.g., sensors and devices in a smart home.
  - **C-WOR**: IoT terminals in co-work relationship. E.g., farming sensors are used for actuating irrigation behaviors.
  - **SOR**: IoT devices behave like humans and form a socialized community of things in autonomy. E.g., A close friendship of two persons can lead to socialized relationship of their respectively owned devices.



- **Two kinds of nodes in a trusted zone**
  - **Master node**: Nodes with relatively better resources.
  - **Slave node**: Nodes with less computing and storage capabilities.

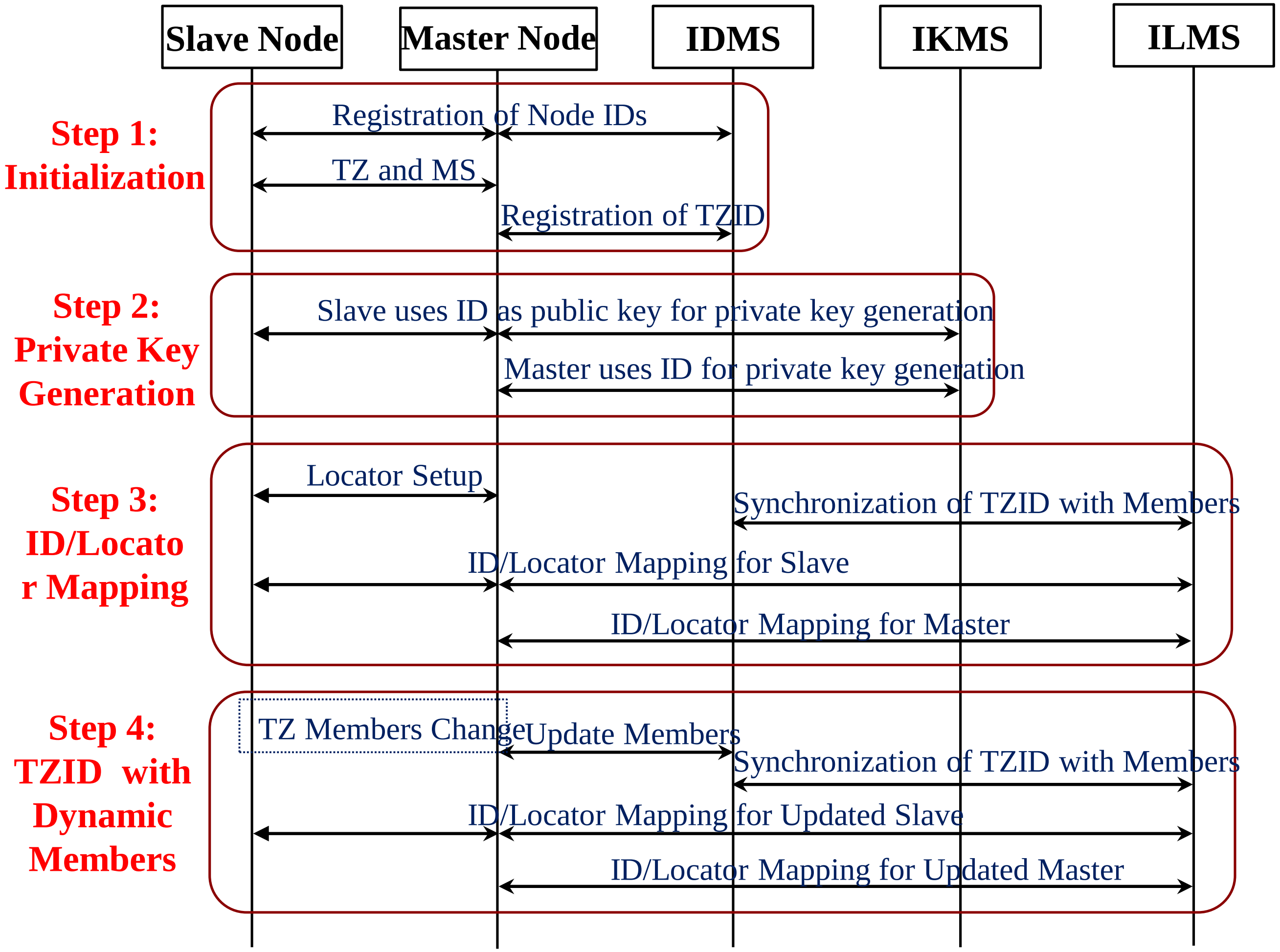
Initialization and Setup with Dynamic TZ of IBS-enabled Authentication for IoT Nodes


Slave Node
Master Node
IDMS
IKMS
ILMS
Step 1: Initialization
Registration of Node IDs
TZ and MS
Registration of TZID
Step 2: Private Key Generation
Slave uses ID as public key for private key generation
Master uses ID for private key generation
Step 3: ID/Locator Mapping
Locator Setup
Synchronization of TZID with Members
ID/Locator Mapping for Slave
ID/Locator Mapping for Master

Sequence of Initialization and Setup with Dynamic TZ

- **Step 1: Initialization**
  - Step 1.1: Each node register ID to IDMS
  - Step 1.2: Constitution of TZ and Master Selection (MS)
  - Step 1.3: Master node register TZID and inner relationship to IDMS
- **Step 2: Private Key Generation**
  - IKMS use IDs as public keys to generate private keys and distribute to nodes
- **Step 3: ID/Locator Mapping**
  - Step 3.1: Configure local locators for slave nodes.
  - Step 3.2: Set a global locator for each slave, which is simply the global locator of its master.
  - Step 3.3: A synchronization of TZID with its all member IDs, i.e., MIDs and SIDs and their instant relationships, is then carried out between IDMS and ILMS.
  - Step 3.4: The global locators for slave and master are registered at ILMS for potential queries by other corresponding nodes.

Initialization and Setup with Dynamic TZ of IBS-enabled Authentication for IoT Nodes


Slave Node
Master Node
IDMS
IKMS
ILMS
Step 1: Initialization
Registration of Node IDs
TZ and MS
Registration of TZID
Step 2: Private Key Generation
Slave uses ID as public key for private key generation
Master uses ID for private key generation
Step 3: ID/Locator Mapping
Locator Setup
Synchronization of TZID with Members
ID/Locator Mapping for Slave
ID/Locator Mapping for Master
Step 4: TZID with Dynamic Members
TZ Members Change
Update Members
Synchronization of TZID with Members
ID/Locator Mapping for Updated Slave
ID/Locator Mapping for Updated Master

Sequence of Initialization and Setup with Dynamic TZ

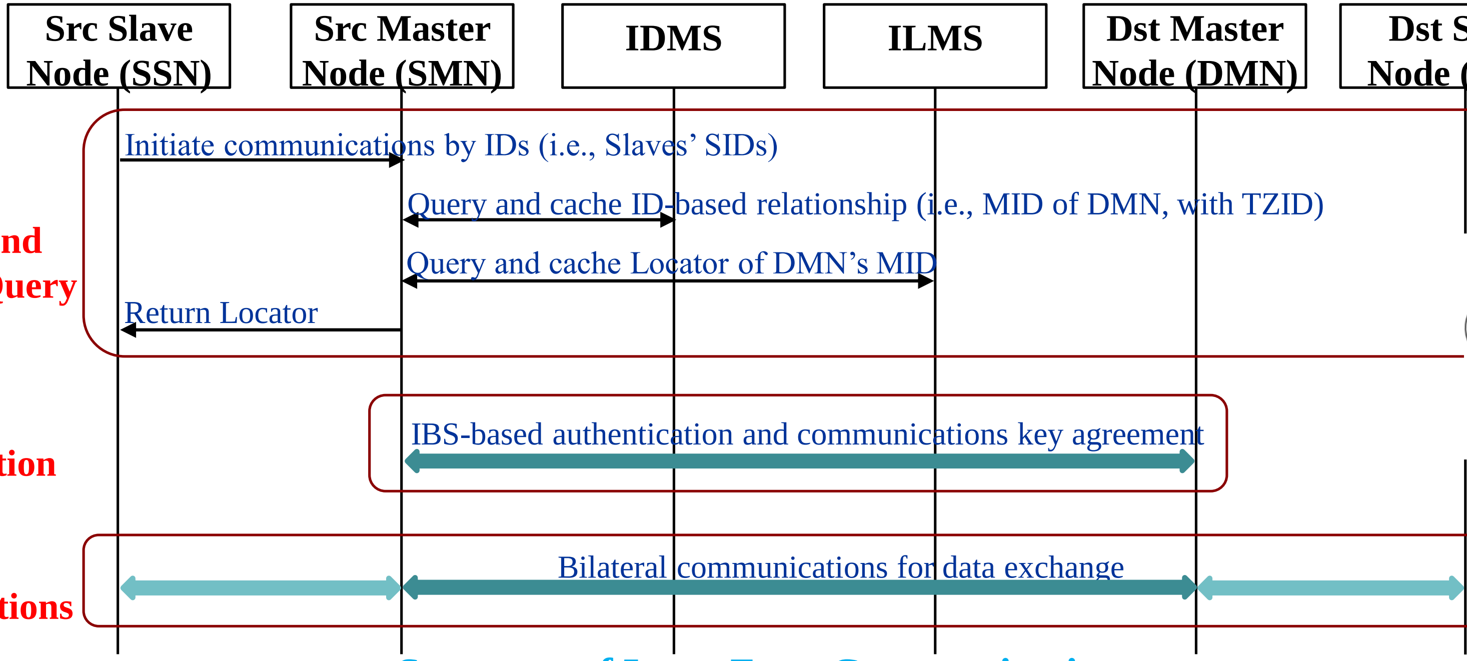
Step 4: TZID with Dynamic Members

- Dynamics of changing membership in TZs. Once a member changing event happens, relevant member changes are updated to IDMS and propagated to ILMS as soon as possible. Since TZID remains constant all the time at both IDMS and ILMS, our proposal could bring constant group reachability.

◆Collectively, all IoT devices have unique IDs, and their relational structure inside a TZ is properly managed by IDMS and mapped into ILMS.

◆Each IoT node now has its ID as public key, a generated private key based on IBS, and two locators for addressing, which paves the way for the following inter-zone communications.

Inter-Zone Communications between Slave Nodes


Src Slave Node (SSN)
Src Master Node (SMN)
IDMS
ILMS
Dst Master Node (DMN)
Dst Slave Node (DSN)
Initiate communications by IDs (i.e., Slaves' SIDs)
Query and cache ID-based relationship (i.e., MID of DMN, with TZID)
Query and cache Locator of DMN's MID
Return Locator
IBS-based authentication and communications key agreement
Bilateral communications for data exchange

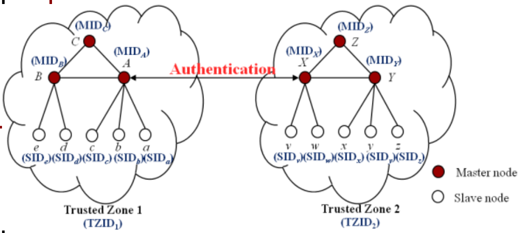
Step 1: Initiation and ID/Locator Query

Step 2: Authentication

Step 3: Communications

Sequence of Inter-Zone Communications

Effects of Cache

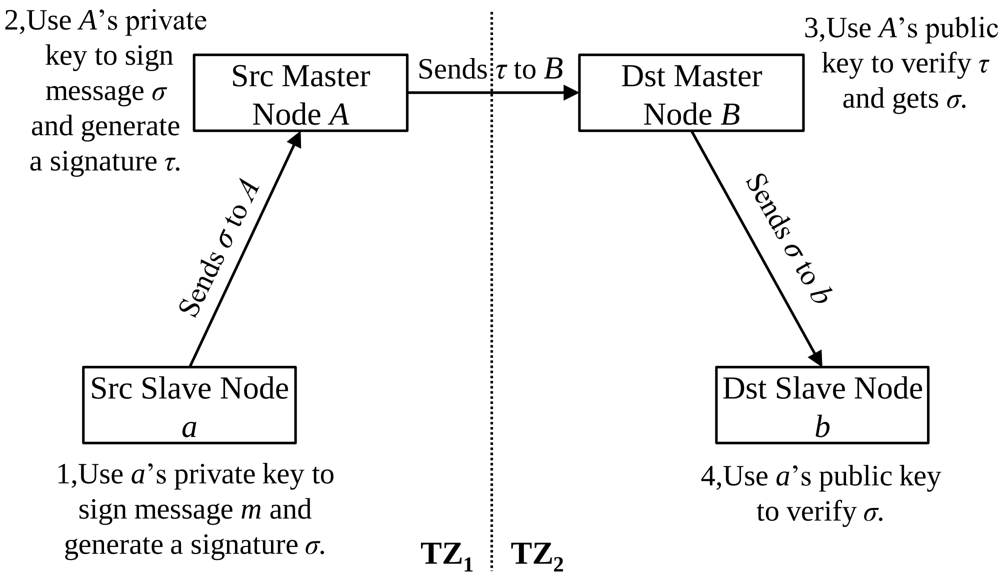


- ◆Member relationships synchronization (fully/partially) among masters
- ◆Event-triggered updating
- ◆Zone-Zone authentication for reduced complexity

- **Step 1: Initiation and ID/Locator Query**
  - ➢ Step 1.1: Source Slave Node (SSN) initiates a communication with Destination Slave Node (DSN), via using their respective identifiers, i.e., SIDs of SSN and DSN.
  - ➢ Step 1.2: SMN queries IDMS for the ID-based relational information about Destination Master Node (DMN) and Slave Node (DSN).
  - ➢ Step 1.3: SMN further queries the locator of DMN from ILMS, using DMN's MID, before returning locator query result to SSN.
  - ➢ Step 1.4: SMN returns locator of DMN to SSN.
- **Step 2: Authentication:**
  - ➢ IBS-based authentication between SMN and DMN, and also negotiates a security key for further communications between nodes for data transmission.
- **Step 3: Bilateral communication**
  - ➢ Bilateral data exchange between two TZs, which can happen between two slave nodes or between slave and master, or between master and master.

Dual Authentication

A dual authentication process is elaborated to fulfill an additional requirement, i.e., some devices may demand a higher level security, by mutual authentication.



2,Use A's private key to sign message σ and generate a signature τ.
Src Master Node A
Sends τ to B
Dst Master Node B
3,Use A's public key to verify τ and gets σ.
Sends σ to A
Sends σ to b
Src Slave Node a
Dst Slave Node b
1,Use a's private key to sign message m and generate a signature σ.
4,Use a's public key to verify σ.
$\mathbf{TZ_1}$
$\mathbf{TZ_2}$

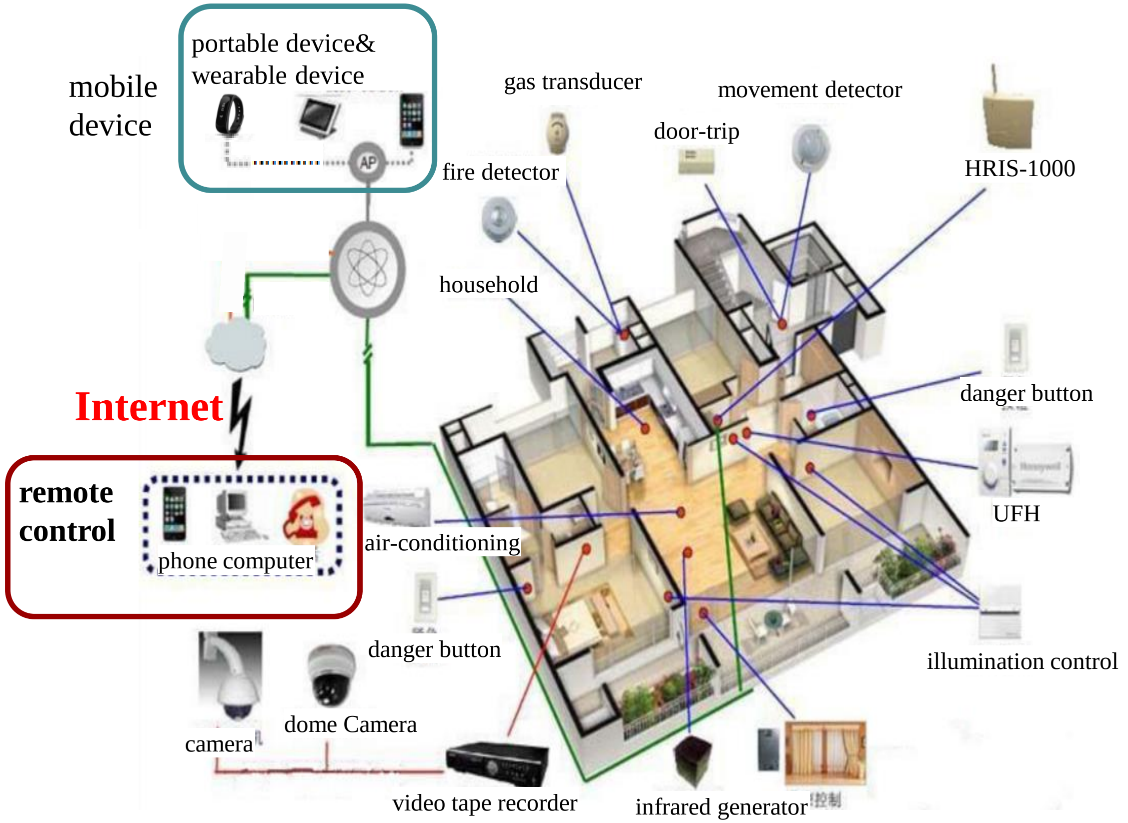
Dual Authentication for Masters and Slaves

- Slave node b is a device requiring a higher level security. It thus simultaneously authenticates master node A and slave node a.
  - Step 1, slave node a signs message m with its private key to generate signature σ, then node a sends σ to its master node A.
  - Step 2, master node A uses its private key to sign σ and generates another signature τ. Then, A sends τ to master node B.
  - Step 3, master node B uses A's public key (i.e., A's ID) to verify signature message τ sent by A, and forwards inner message σ to slave node b.
  - Step 4, slave node b uses node a's public key (i.e., a's ID), to authenticate its identity.

Similarly, node *a* can also authenticate node *b* in a reverse manner.

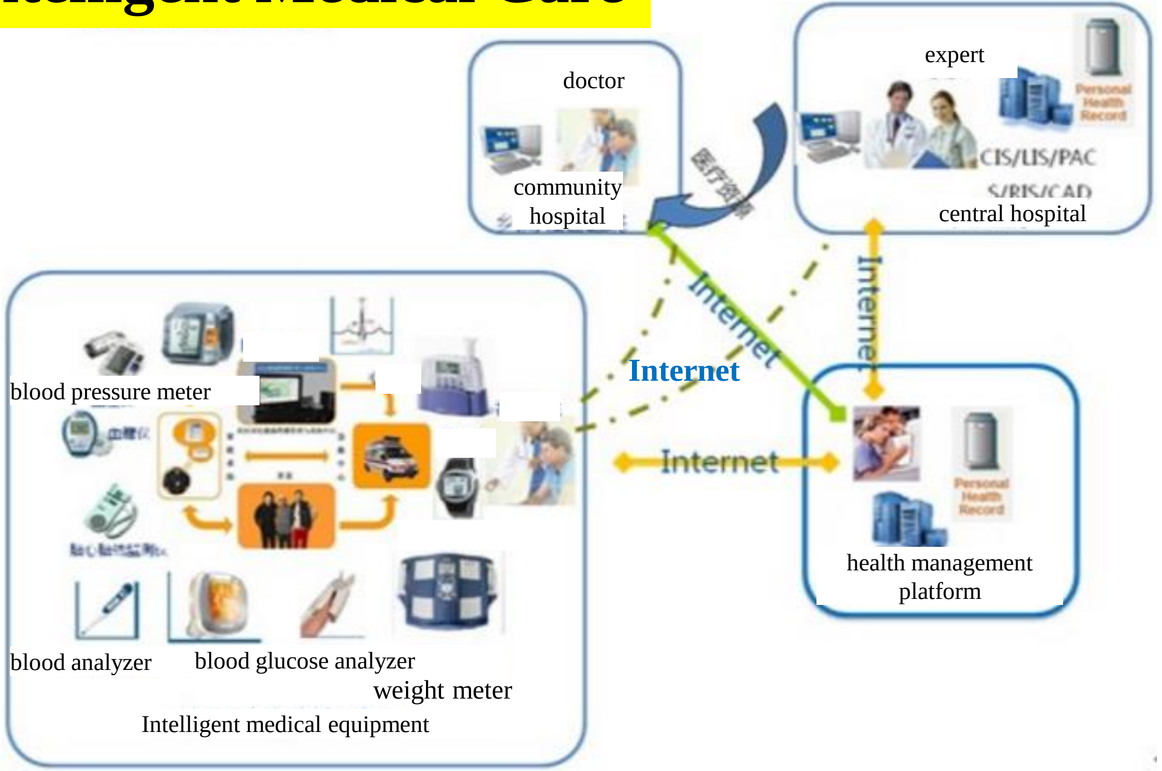
Vertical Scenarios

Smart Home



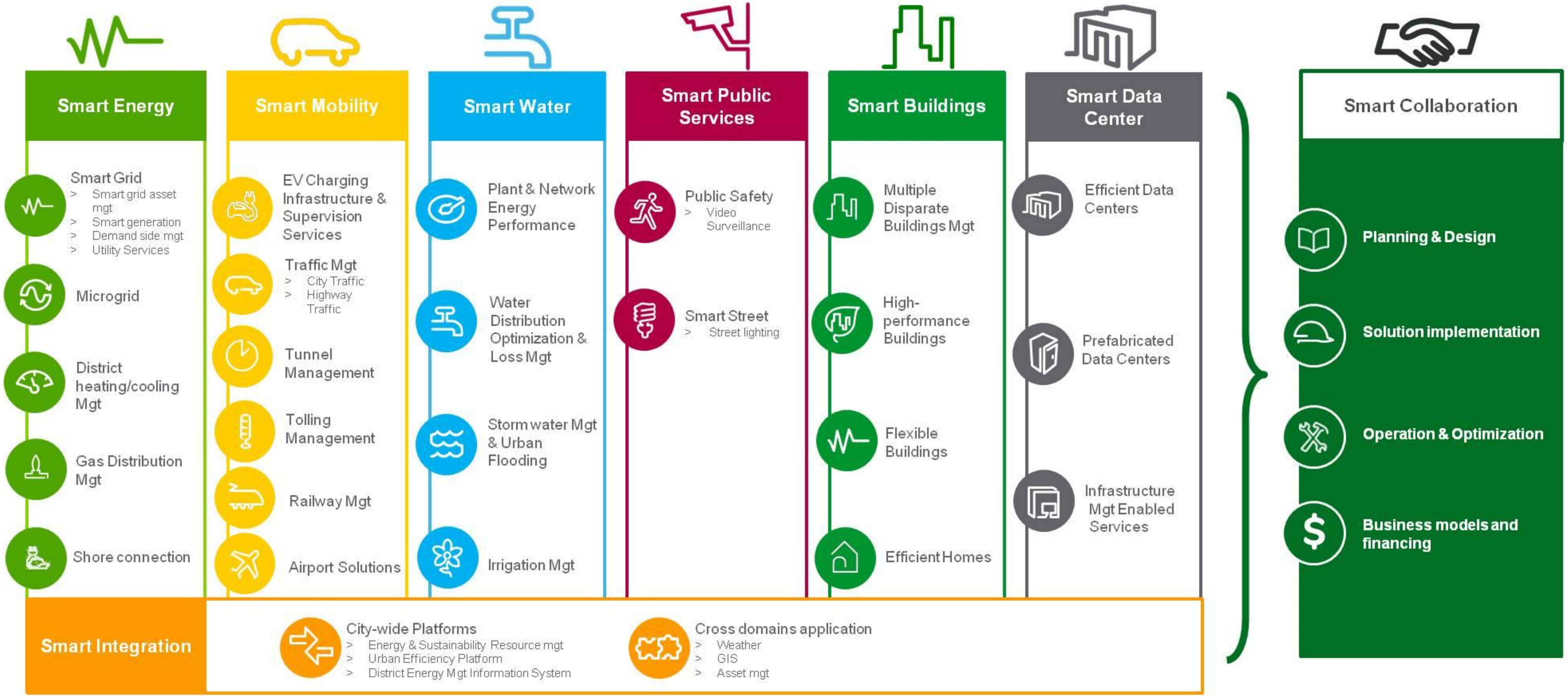
Secure communications between distinct devices (or groups) in smart home, and remote devices (or groups) in mobility (e.g., personal car).

Intelligent Medical Care



Secure communication between a variety of medical sensing devices (or groups), and remote devices (or groups) in intelligent medical care system.

CROSS-DOMAIN SCENARIO: SMART CITY



Smart Energy

- Smart Grid
  - > Smart grid asset mgt
  - > Smart generation
  - > Demand side mgt
  - > Utility Services
- Microgrid
- District heating/cooling Mgt
- Gas Distribution Mgt
- Shore connection

Smart Mobility

- EV Charging Infrastructure & Supervision Services
- Traffic Mgt
  - > City Traffic
  - > Highway Traffic
- Tunnel Management
- Tolling Management
- Railway Mgt
- Airport Solutions

Smart Water

- Plant & Network Energy Performance
- Water Distribution Optimization & Loss Mgt
- Storm water Mgt & Urban Flooding
- Irrigation Mgt

Smart Public Services

- Public Safety
  - > Video Surveillance
- Smart Street
  - > Street lighting

Smart Buildings

- Multiple Disparate Buildings Mgt
- High-performance Buildings
- Flexible Buildings
- Efficient Homes

Smart Data Center

- Efficient Data Centers
- Prefabricated Data Centers
- Infrastructure Mgt Enabled Services

Smart Collaboration

- Planning & Design
- Solution implementation
- Operation & Optimization
- Business models and financing

Smart Integration

- City-wide Platforms
  - > Energy & Sustainability Resource mgt
  - > Urban Efficiency Platform
  - > District Energy Mgt Information System
- Cross domains application
  - > Weather
  - > GIS
  - > Asset mgt

Cross-domain interconnection for heterogeneous communications between vertical groups in smart city (Traffic with Energy) demands securely trusted communications.

Feasibility Analysis: Computational Cost

Signature	Cortex-M0(+) (48MHz)	Cortex-M3 (96MHZ)	Mobile Phone (Cortex-A9, 1200MHz)
IETF-ECC-IBS (curve25519)	80ms	40ms	3.2ms
ISO-ECC-IBS (curve25519) ECC - Elliptic Curve Cryptography	Offline: 30ms Online: 15ms	Offline: 15ms Online: 8ms	Offline: 1.2ms Online: 0.6ms
ISO-Pairing-IBS (BN Pairing)	669ms	335ms	26.8ms

Verification	Cortex-M0(+) (48MHz)	Cortex-M3 (96MHZ)	Mobile Phone (Cortex-A9, 1200MHz)
IETF-ECC-IBS (curve25519)	225ms	113ms	9.04ms
ISO-ECC-IBS (curve25519)	224ms	112ms	8.96ms
ISO-Pairing-IBS (BN Pairing)	2324ms	1162ms	92.96ms

TABLE - Computing Time for 128-bit IBS Signature and Verification.

- **Cortex-M0(+)**: Targeted for low-resource IoT terminals, such as low-power Bluetooth, Ultraviolet (UV) sensor, livestock acid sensor, smart lock etc.
- **Contex-M3**: Used for low-middle resource IoT terminals, such as smart bracelet, smart necklace, smart watch etc.
- **Contex-A9**: For high-resource terminals, such as mobile phones (e.g., iPhone) and tablets.

Cortex-M0(+) and Contex-M3: Mainly used by slave nodes, without authentication calculation or with a limited chance of implementing IBS-based authentication.

Contex-A9 and more powerful ones: Can be used for master nodes.

Conclusion: **Feasible** for occasional IBS-based authentications of Low and Middle Power IoT Terminals, and not an obstacle for High Power Devices.

Feasibility Analysis: Storage & Transmission Cost

	TZID	MID	Locator	SID	Sum
Slave Node 1	128bits	128bits	128bits	128bits	64bytes
…	**…**	**…**	**…**	**…**	**…**
Slave Node 200	128bits	128bits	128bits	128bits	64bytes
Master Node	3.13KB	3.13KB	3.13KB	3.13KB	12.5KB

TABLE - Additional Storage for Slave and Master Node.

- In a typical IoT scenario, as in smart home or vehicular system, with a single master, the peripheral size usually in the scale of tens of nodes.
- We assume one trusted zone has 200 slave nodes, each slave node is assumed to maintain one session.
- Cost is increased accordingly, if more nodes are deployed.

Slave Node: Should additionally store 64 bytes of the corresponding information.
Master Node: Should additionally have information of about 12.5K bytes for storage in a specific TZ. (**Max**)
Conclusion: The added cost on storage is **acceptable** for slave and master nodes.

	ZigBee (IEEE 802.15.4)			Bluetooth	
	US (908MHz)	**UE (860MHz)**	**US/UE (2.4GHz)**	**Ver. 4.0**	**Ver. 4.2**
Slave Data Rate	40kbps	20kbps	250kbps	270kbps	800kbps
Master Data Rate	7.81Mbps	3.90Mbps	48.83Mbps	52.73Mbps	156.25Mbps

TABLE - Embodiment of Extreme Data Rates for Master Node.

- With the assumption of 200 slave nodes in one trusted zone, an extreme bandwidth requirement is summarized above, for a single master, considering two typical IoT enabling technologies (i.e., ZigBee and Bluetooth).

Conclusion: There may exist multiple masters for load balance, and IoT nodes with constrained resources are in power saving mode in most of the time (>95%) , the transmission burden on master nodes is also feasible, when they adopt primary networking capabilities (Wi-Fi, 3G/LTE, or Wired Networking). In addition, buffer can be used as well.

Conclusion and Future Work

Merits of Our Proposal in Summary

- **Simplified Secure Authentication:** Under ION framework, applying globally unique ID of IoT devices, as public keys for IBS-based authentication, greatly reduced the complexity of utilizing PKI-based certificates. This type of authentication also significantly enhances the security of IoT, in addition to existing pairing methods in link layer.
- **Socialized Feature** of IoT devices is fully exploited, while dynamic trusted zones are formulated through unique IDs.
  - ✓ Each zone maintains the social relationship of the masters and slaves inside, and updates the relationship on-demand.
  - ✓ Via IDMS, this relational feature facilitates the authentication between any two IoT nodes, especially in the case of multiple masters with credibility propagation.
  - ✓ With the introduced TZID, a relational group of IoT devices is persistently available, which is desirable for many use cases such as smart building, e-healthcare and vehicular systems.
- **IoT Mobility:** The introduced master's and slave's IDs can be directly used for setting up communications, regardless of their specific locations, which fully supports IoT mobility.
- **Heterogeneity Inclusion:** For practical data exchange, local and global locators are maintained (cached) by master nodes and the mapping from IDs to global locators is in ILMS. This configuration eliminates the heterogeneity of IoT enablers.

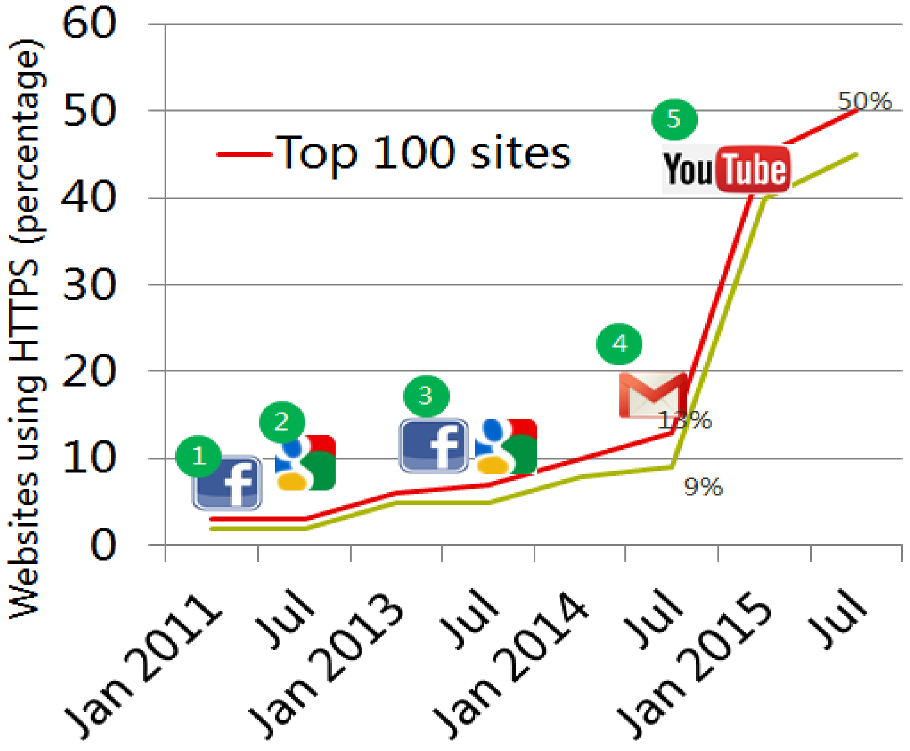
Future Work

- Due to lack of large-scale field tests, we would further explore the actual effects on large-scale deployment.
- The optimized master selection algorithm should be further designed as well.
- Dynamic node changes should also be modeled with on-demand update for IDMS.
- The overall architecture needs a generic network mapping system, i.e., ILMS, and its performance could be a new bottleneck in large scale implementation, which is worthy of more exploration. [Ref: IETF IDEAS]

Q&A

www.huawei.com

Security and Encrypted Traffic in Higher and Higher Demand



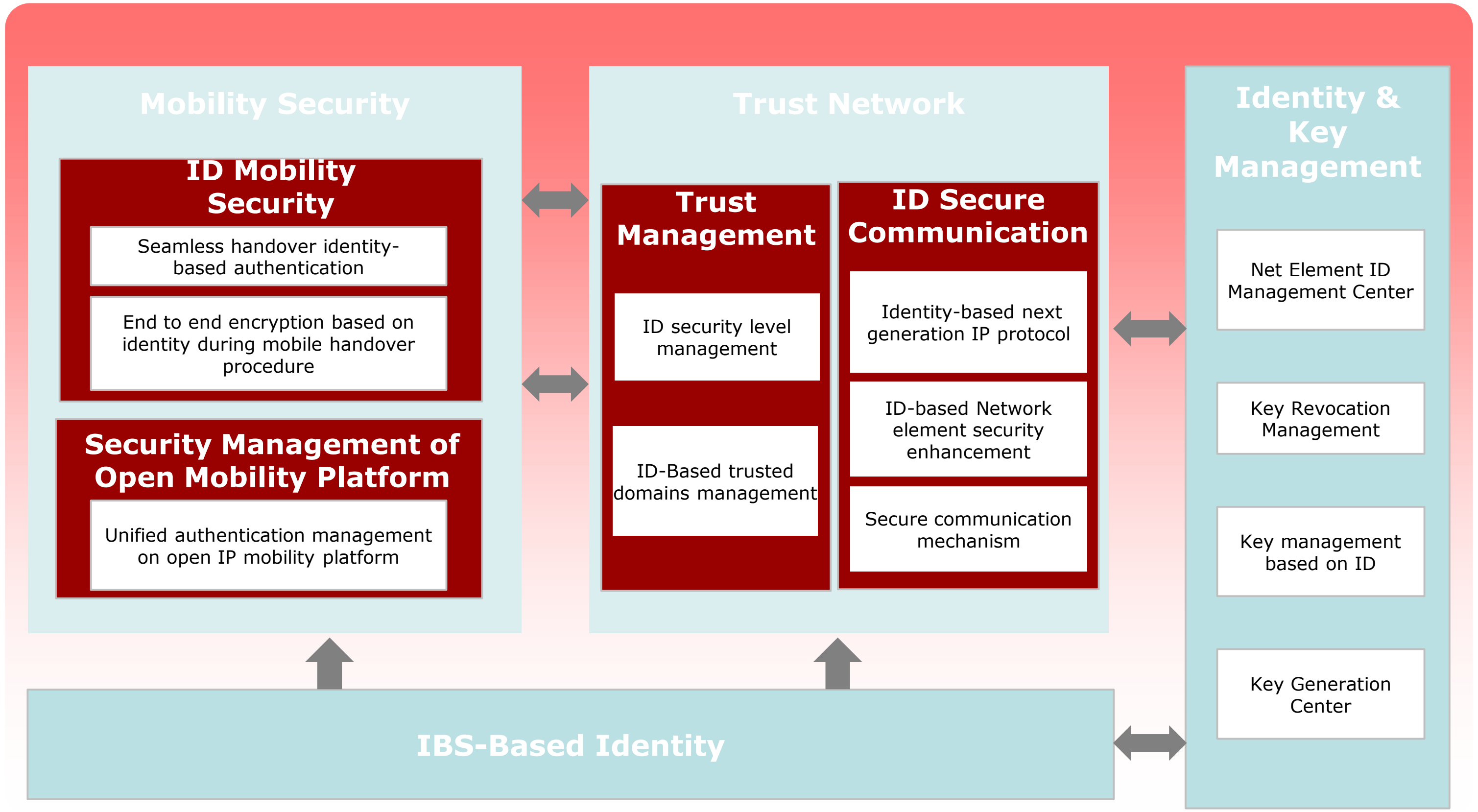
Data sourced from httparchive.org. Top 100 and million sites as ranked by Alexa

1. **2011: Facebook adds an option for secure login**
2. **2011: Google Search provides secure search**
3. **2013: Facebook, Google Search are encrypted**
4. **2014: Gmail is encrypted**
5. **2014: YouTube traffic is encrypted**

- Internet traffic encryption are implemented and provided by Google, FB, Twitter, Yahoo and Snapchat, which accounts for 45-50% (source from VDF, Mozilla)
- Content providers are increasingly planning to provide encryption for their traffic, for example, Netflix and BBC are testing their networks for encryption

Encrypted traffic is growing at a faster pace after 2011
Now it accounts for 45-50% of the total Internet traffic, and it continues to grow

Next Generation IP Intrinsic Security Architecture



Mobility Security

ID Mobility Security

- Seamless handover identity-based authentication
- End to end encryption based on identity during mobile handover procedure

Security Management of Open Mobility Platform

- Unified authentication management on open IP mobility platform

Trust Network

Trust Management

- ID security level management
- ID-Based trusted domains management

ID Secure Communication

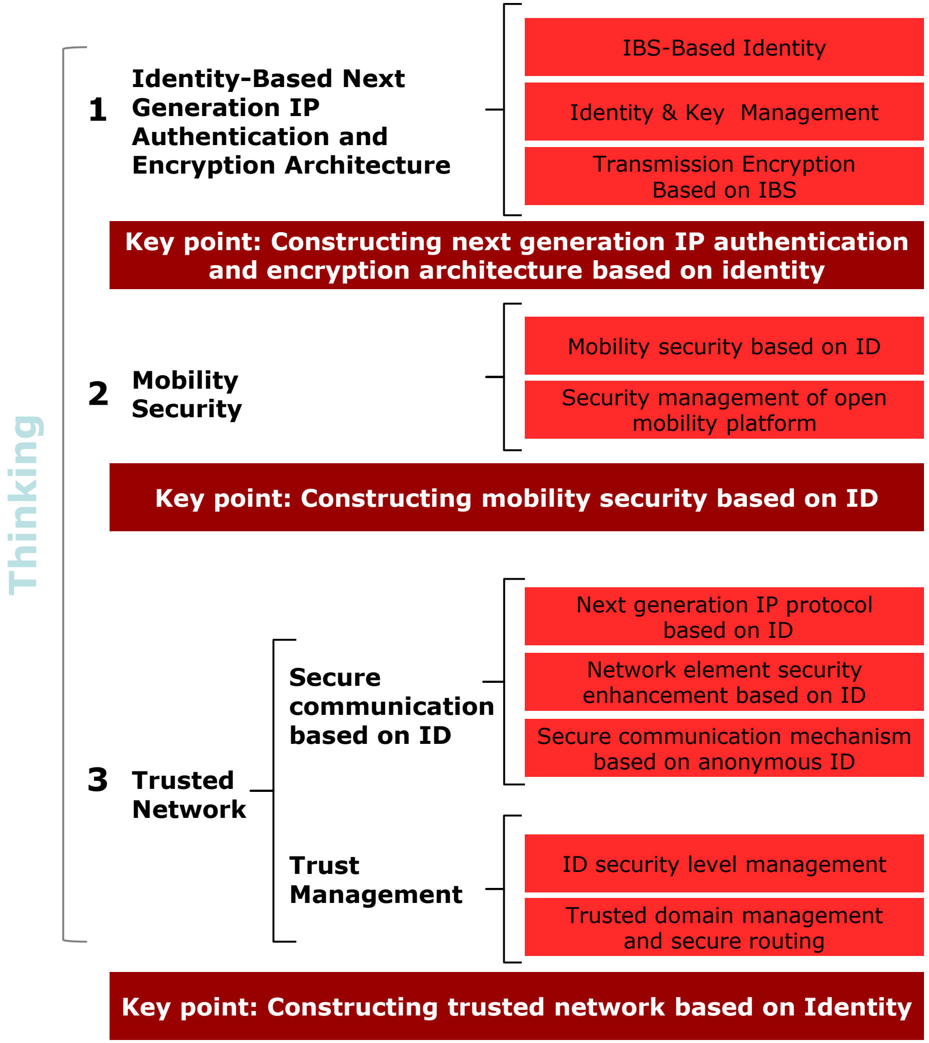
- Identity-based next generation IP protocol
- ID-based Network element security enhancement
- Secure communication mechanism

Identity & Key Management

- Net Element ID Management Center
- Key Revocation Management
- Key management based on ID
- Key Generation Center

IBS-Based Identity

Next Generation IP Intrinsic Security Architecture Based on Identity



Thinking

1 Identity-Based Next Generation IP Authentication and Encryption Architecture

- IBS-Based Identity
- Identity & Key Management
- Transmission Encryption Based on IBS

Key point: Constructing next generation IP authentication and encryption architecture based on identity

2 Mobility Security

- Mobility security based on ID
- Security management of open mobility platform

Key point: Constructing mobility security based on ID

3 Trusted Network

Secure communication based on ID

- Next generation IP protocol based on ID
- Network element security enhancement based on ID
- Secure communication mechanism based on anonymous ID

Trust Management

- ID security level management
- Trusted domain management and secure routing

Key point: Constructing trusted network based on Identity

INTRODUCTION

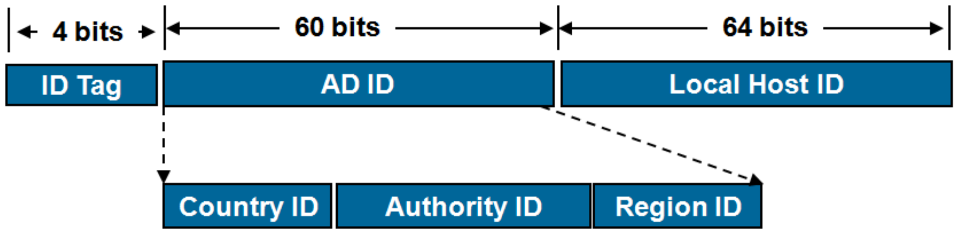
- With the IoT evolution, socialized IoT and cloudified IoT require complete interoperations and **globally unified IoT communications**.

→ **Requirement 1: Global reachability for all types of IoT devices**

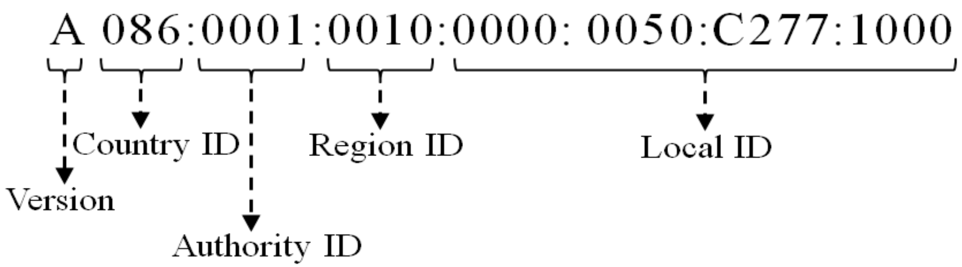
- And, IoT security is a particular concern.
- **Authentication** is one major problem
- Currently, the below **Two Types of Authentication** mechanisms can not satisfy massive IoT devices, especially with constrained resources.
  - ➢ **Symmetric key authentication:** frequent communications, and large storage
  - ➢ **Asymmetric key authentication:** based on traditional Public Key Cryptosystem (PKC), which could be too complex for IoT

→ **Requirement 2: Secure authentication for massive resource constrained IoT devices**

IDMS: An Example of ID Format



a. Embodiment of IBS-based ID Format.



b. Example of IBS-based ID.

- **One specific illustration of IBS-based ID Format**
  - ID tag : 4 bits, shows the version;
  - Administration Domain (AD) ID: 60 bits ,handles different domains in customized granularity;
  - Local Host ID: 64 bits, may directly adopt the local identifiers or addresses used in IoT verticals or indirectly use after a translation or padding.
- **Example of IBS-based ID**
  - The first 4-bit A shows ID tag, the following 60 bits specify the corresponding domain IDs, and the last 64 bits contains a local ID such as a local IoT address of 00:50:C2:77:10:00.

An Example of Bilateral Communication (S2S)

ID_{SSN}	Local Locator $_{SSN}$	ID_{DSN}	Global Locator $_{DMN}$
SRC ID	SRC Locator	DST ID	DST Locator

a. SSN → SMN

ID_{SSN}	Global Locator $_{SMN}$	ID_{DSN}	Global Locator $_{DMN}$
SRC ID	SRC Locator	DST ID	DST Locator

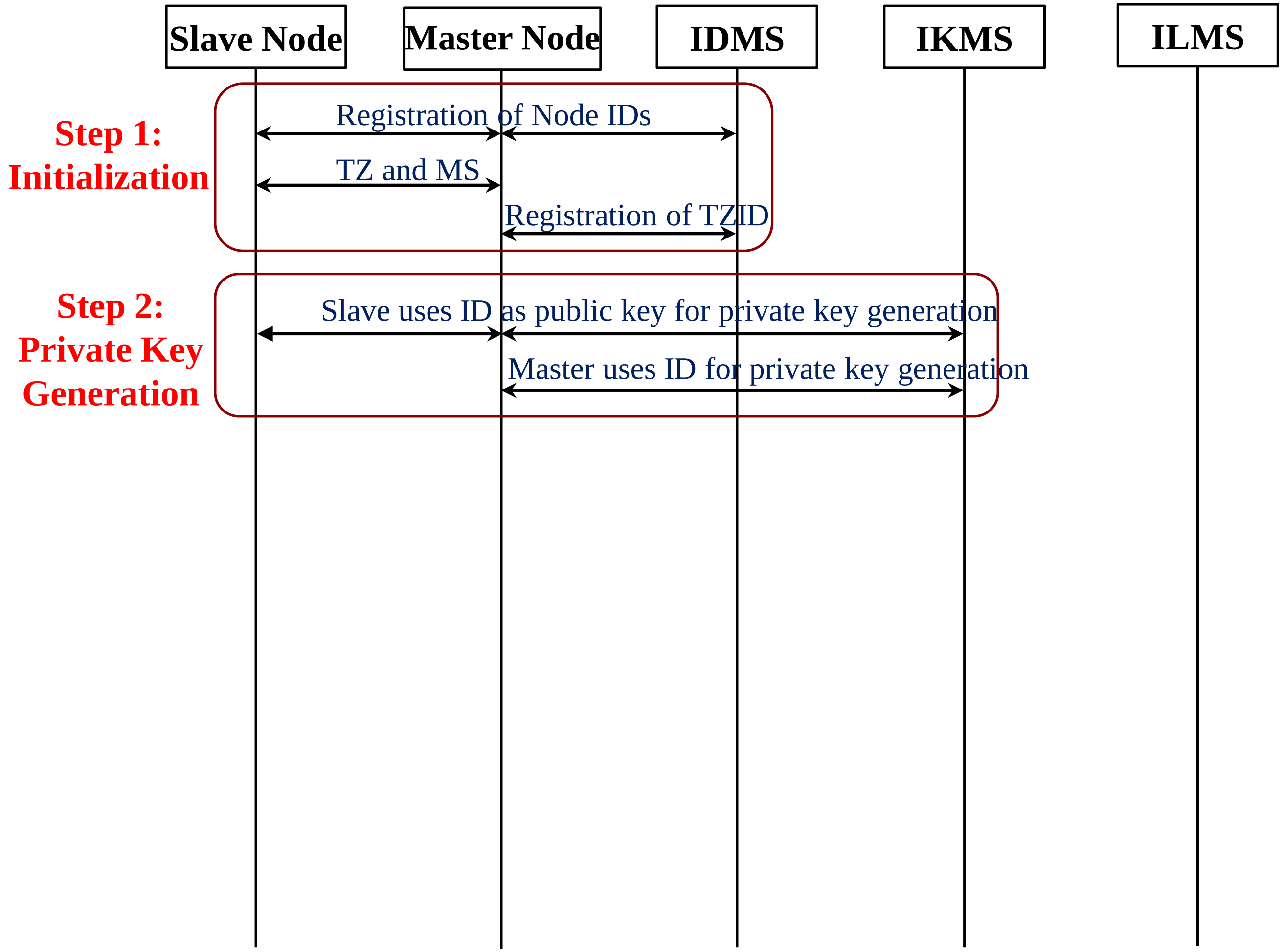
b. SMN → DMN

ID_{SSN}	Global Locator $_{SMN}$	ID_{DSN}	Local Locator $_{DSN}$
SRC ID	SRC Locator	DST ID	DST Locator

c. DMN → DSN

- **One specific illustration for bilateral communication**
  - SSN structures a packet and forwards it to SMN
  - SMN translates the Local Locator of SSN to SMN’s Global Locator
  - DMN determines the destination according to the ID, and queries the Local Locator through the ID, then forwards it to DSN.

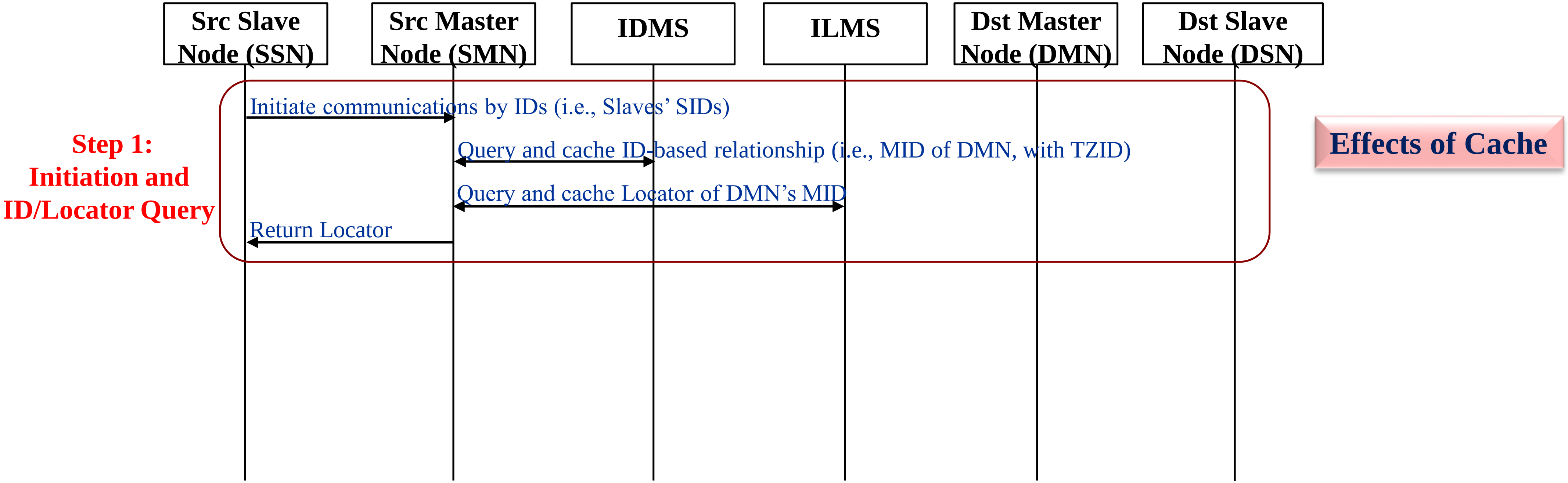
Initialization and Setup with Dynamic TZ of IBS-enabled Authentication for IoT Nodes


Slave Node
Master Node
IDMS
IKMS
ILMS
Step 1: Initialization
Registration of Node IDs
TZ and MS
Registration of TZID
Step 2: Private Key Generation
Slave uses ID as public key for private key generation
Master uses ID for private key generation

Sequence of Initialization and Setup with Dynamic TZ

- **Step 1: Initialization**
  - Step 1.1: Each node register ID to IDMS
  - Step 1.2: Constitution of TZ and Master Selection (MS)
  - Step 1.3: Master node register TZID and inner relationship to IDMS
- **Step 2: Private Key Generation**
  - IKMS use IDs as public keys to generate private keys and distribute to nodes

Inter-Zone Communications between Slave Nodes


Src Slave Node (SSN)
Src Master Node (SMN)
IDMS
ILMS
Dst Master Node (DMN)
Dst Slave Node (DSN)
Step 1: Initiation and ID/Locator Query
Initiate communications by IDs (i.e., Slaves' SIDs)
Query and cache ID-based relationship (i.e., MID of DMN, with TZID)
Query and cache Locator of DMN's MID
Return Locator
Effects of Cache

Sequence of Inter-Zone Communications

- **Step 1: Initiation and ID/Locator Query**
  - Step 1.1: Source Slave Node (SSN) initiates a communication with Destination Slave Node (DSN), via using their respective identifiers, i.e., SIDs of SSN and DSN.
  - Step 1.2: SMN queries IDMS for the ID-based relational information about Destination Master Node (DMN) and Slave Node (DSN).
  - Step 1.3: SMN further queries the locator of DMN from ILMS, using DMN's MID, before returning locator query result to SSN.
  - Step 1.4: SMN returns locator of DMN to SSN.