Cross-Silo and Cross-Eco IoT Communications with ID Oriented Networking (ION)

Bin Da, Richard Li, Xiaofei Xu, Xiaohu Xu
NGIP Laboratory, Beijing Huawei Digital Technologies Co., Ltd.
No.156 Beiqing Street, Haidian District, Beijing, P.R.China, 100095
Email: {dabin, renwei.li, xuxiaofei, xuxiaohu}@huawei.com

Abstract—**This paper reviews basic IoT architectures, the corresponding evolution at different stages, and presents generalized IoT interoperations under the trend of cross-silo and cross-ecosystem communications. In line with these trends and requirements, ID Oriented Networking, with the detailed background and implementation framework, is elaborated, which contributes to achieve unified IoT communications in future networks. Specifically, ION has the following key components: Network Mapping System, ID Management System, and ID Relationship Management System. And additionally, ION is able to naturally support universal mobility of IoT terminals and enhance intrinsic security of IoT networks, while also can facilitate internetworking of all virtual and physical things over distinct domains, for a fully connected world. At the end of this paper, the merits, challenges and future work of ION are briefly discussed as well.**

Keywords- Internet of Things; IoT; Identifier Locator Split; ID Oriented Networking; ION; Cross-Silo; Cross-Eco.

I. INTRODUCTION

The Internet of Things (IoT) originates from RFID (Radio Frequency IDentification) and relevant technologies in 1980s, which is formally coined as IoT in 1999 [1]. Since then, the IoT paradigm has evolved in several generations, from the vast usage of tagged things and sensor networks [2], to ubiquitously connected smart things over Internet [2][3], and to recently proposed socialized and cloudified internet of things [4][5]. Along with such evolution direction, IoT is envisioned to become a global infrastructure that is able to interconnect everything in the world, which finally fulfills the objective of Everything as a Service (EaaS) [6].

As surveyed in the literature [2]-[7], the essential components of IoT should consist of: physical things with unique identifiers (IDs) for data capturing and local storage; routing mechanism for remote storage and processing; protocols for interoperability and service provision; and trustworthiness among things for security and privacy. Recently, virtualized entities become a prominent feature or candidate component of IoT's further evolution, which associates the Real World Objects (RWOs) with Virtual World Objects (VWOs) [8], for improved communication response and efficiency. All these components are widely practiced in various scenarios such as wearables, smart home, smart city, connected cars, supply chain, cyber physical system, and so forth.

Furthermore, lots of IoT Alliances or Groups have been emerging in the past few years, such as oneM2M established in 2012, Thread launched in 2014, and Open Connectivity Foundation (OCF) newly formed in 2016 [7]. The typical feature, in the infancy of these alliances or groups, is to unite distinctly siloed IoT enabling technologies for achieving full interoperability, inside their respective ecosystems. However, for IoT to be consumed in a ubiquitous manner and be always accessible, these ecosystems are also required to communicate with each other. Henceforth, referred to as cross-ecosystem or cross-eco, this paper concentrates on providing mechanisms to enable cross-silo and cross-eco communications, in a fully connected IoT world.

In line with aforementioned application scenarios and tendencies, the vision of a smart world can be imagined, where cross-silo and cross-eco interconnections become pervasive as a hidden infrastructure. As a result, for achieving this vision, this paper introduces the concept of ID Oriented Networking (ION), and its specific usage for globally unified IoT communications, while all IoT terminals are assumed to be with intelligence in a foreseen trend.

The remainder is organized as follows: in Section II, the IoT architectures are briefly reviewed, with current IoT interoperation status. Then, the ION is elaborated in detail in Section III, with the corresponding building blocks, implementation framework, essential merits, and key features for IoT interoperability. Afterwards, Section IV discusses the challenges and future work, and Section V finally concludes this paper.

II. ARCHITECTURE, EVOLUTION AND INTEROPERATION

This section firstly reviews traditional IoT architectures which are prominent in industry and academy, then the evolution directions of IoT in the past decades are described. After which, a summary for the current status of generalized IoT interoperations is presented. Finally, the trend of cross-silo and cross-eco IoT communications is highlighted.

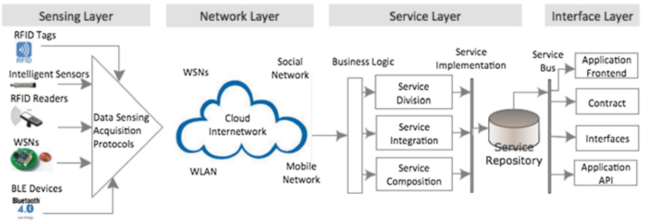


Figure 1. Service Oriented Architecture (SOA).

A. *IoT Architecture Review*

Traditionally, the Service Oriented Architecture (SOA) and its variants are designed for IoT [2], which generally has

ISBN: 978-1-61208-550-0

four layers (Sensing, Network, Service, and Interface layers). As shown in Fig.1 [2], the sensing layer normally contains a variety of hardware objects (e.g., RFID tags, sensors and actuators), for acquiring data. The network layer practically facilitates the data transfer over wired or wireless networks. In addition, the service layer generates and manages services whenever required. Lastly, the interface layer presents universal methods that are used by specific applications. Besides this fundamental SOA design, there proposed lots of IoT architectures, with distinct focuses on the applied scenarios [7]. Among which, IoT-A reference model forms a sophisticated architecture, with hundreds of practical IoT requirements into consideration [9].

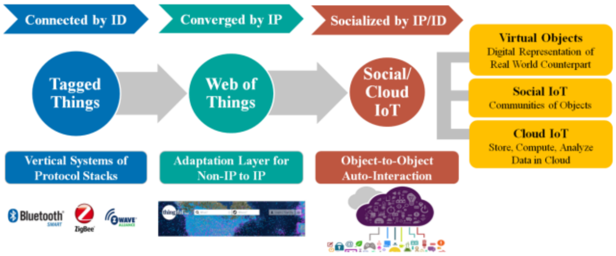

Connected by ID
Converged by IP
Socialized by IP/ID
Tagged Things
Web of Things
Social/ Cloud IoT
Virtual Objects
Digital Representation of Real World Counterpart
Social IoT
Communities of Objects
Cloud IoT
Store, Compute, Analyze Data in Cloud
Vertical Systems of Protocol Stacks
Adaptation Layer for Non-IP to IP
Object-to-Object Auto-Interaction
Bluetooth SMART
ZigBee
ZWAVE

Figure 2. Evolution of Internet of Things (IoT).

B. IoT Evolution

As aforementioned, the term of Internet of Things (IoT) formally emerges in 1999 [1], which mainly builds on the previously developed RFID technologies. Since then, IoT's connotation has been continuously expanding, in particular, the corresponding IoT evolution is briefed in Fig. 2, in line with our analysis. The first generation of IoT is early contributed by the RFID technology, which connects things by RFID tags and transfers data relevant to the things being tagged, for generating meaningful information flows (e.g., for Supply Chain Management). Furthermore, other IoT connectivity technologies are devised [7], including Bluetooth, ZigBee, Z-Wave and so forth, for satisfying vertical applications, as exemplified by connected things indoor or outdoor. However, these distinguished verticals cannot be operable with each other, since they are addressed by different identifiers and interconnected by different mechanisms or protocols [2]. Thus, in the second generation, different vertical technologies usually resort to a gateway for protocol translation, so as to enable cross-silo IoT communications at local scale. Recently, adaption layers are developed (e.g., 6LoWPAN) for further extending vertical IoT domains to be connected with the Internet, which becomes Web of Things after Non-IP and IP convergence [3]. As a result, siloed IoT enabling technologies are able to be interconnected globally via the Internet.

There is also a tendency towards evolution of IoT to be socialized and cloudified. Accordingly, socialized means IoT terminals tend to establish social links just as humans do [4], cloudified implies to build virtual counterparts of physical things in the cloud and to be equipped with cloud computing technologies [5]. The rationales behind such a tendency are multifold: Thing-to-Thing connections are expected to far exceed Human-to-Human connections in near future; Thing-to-Thing connections are also becoming more intelligent and autonomous, with little or no human intervention; Moreover, the data associated with ubiquitously intelligent things and their interconnections will continue exponentially increasing, which finally leads to a large share of IoT data in the cloud. Thus, everything will be intelligent to smartly associate themselves with other things, for on-demand requirements in various applications, which may even resemble human-to-human interactions to formulate thing-to-thing communities with autonomy. The Social IoT (SIoT) is then proposed [4], for systematically describing thing-to-thing relationships and interactions, along with some essential functionalities. Similarly, cloudified IoT solutions are also implemented by different platforms, for integrated data analytics and management over IoT entities [5].

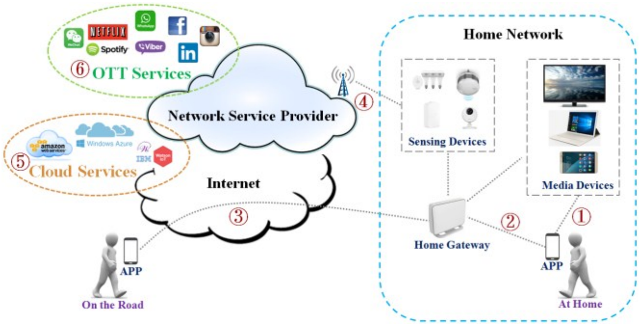


Figure 3. Generalized IoT Interoperations.

C. Current State of Generalized IoT Interoperations

As previously described for the trend of IoT evolution, IoT-based interactions tend to become pervasive, anytime and anywhere, which is not merely for simple data collection but for meaningful service-oriented control. However, in real word, there exist entirely different demands for and types of IoT interoperations, in the manners of Thing-to-Thing and Human-to-Thing connections.

To be more specific, some IoT terminals with fixed positions serve for collecting data locally or remotely, which is usually for centralized data storage and analytics along with few associated actuations (e.g., sensor configuration in remote metering). However, in lot of scenarios, especially with the involvement of human and smart things (i.e., generalized IoT terminals with intelligence), the nearby or remote interactions are aimed for achieving certain services. Without loss of generality, a smart device as the intelligent IoT terminal is exemplified in Fig. 3, for human-involved control on potential interconnections with terminals in a home network, which normally needs an application running in the device as control interface. In Fig. 3, six service-oriented control manners are illustrated with sequential numbers, which are briefly explained below one by one:

① *Direct Point-to-Point (P2P) Operation*: In the first case, the device is able to directly control the surrounding devices via P2P connections, which may use Wi-Fi Direct, Bluetooth Low Energy (BLE), Near Field Communications (NFC) [7]. In this P2P mode, the signal flows are not redirected from any other third parties, and are often used for content sharing, direct actuation, wireless payment.

② *Interaction via Adjacent Gateway*: The device also can go through a nearby gateway to control other IoT terminals, while the gateway practically shields the difference among different IoT technologies such as Wi-Fi, ZigBee, Z-Wave. As in Fig. 3, this is a typical scenario for smart home or smart office. Note that, for Wireless Sensor Network (WSN), there still uses a gateway for collecting data from all sensor nodes through specific IoT enablers, however the interactions are much less as compared to smart home case.

③ *Remote Operation via Internet*: Besides the above two cases for proximity control, the device is able to operate remote IoT terminals through traditional Internet, such as turning on the air conditioner at home on the road.

④ *Interaction via Operator's Gateway*: With the arising of Low Power Wide Area Network (LPWAN) technologies in recent years, the device is entitled to directly connect various IoT terminals at home via the operator's gateway at a remote distance (e.g., 10km away from home), which resembles the home gateway in the second case but with much longer operation distance. Note that these LPWAN technologies are also known as cellular IoT enablers, which are embodied by NB-IoT, LoRa, SigFox and so forth [10].

⑤ *Remote Operation via Cloud*: The cloud service is now integrated with IoT technologies at different levels, which is in line with three cloud types in particular, known as public, private, and hybrid services. These cloud-based services enable centralized control over IoT terminals with data view and data analytics, regardless of the distance. As a result, the device can easily control remote IoT terminals through the cloud services, with hidden underlying IoT technologies.

⑥ *Operation via Over The Top (OTT) Applications*: The human social network applications, like WeChat, Whatsapp, Facebook, are penetrating into all domains of our daily life, including controlling IoT terminals as well. For instance, WeChat is able to perform wireless payment and remote control over smart devices now, and Facebook also can adjust IoT terminal behavior through aforementioned Web of Things. This type of OTT-based operation is actually built upon individual vertical ecosystems with hybrid usage of previous cases.

Note that all the above six interoperation manners continuously generate data, which fully demonstrates the IoT's demand of being integrated with advanced cloud services, forming Cloud of Things (CoT) [5].

D. *Trend of Cross-Silo and Cross-Eco IoT Communications*

In Section I, the fundamental concept of cross-silo and cross-eco IoT communications is briefly introduced. In this sub-section, a more detailed view is presented in Fig. 4, for elaborating such trend for IoT interoperability. Specifically, in Fig. 4 - (a), it shows the current status of IoT industrial layers with protocol stack, from which, it can be observed that there generally exist two types of IoT channels. One type covers relatively long distance, such as LoRa, SigFox, NB-IoT, which are known as LPWAN. Meanwhile, the others target on short distance connectivity like Bluetooth, ZigBee, Z-Wave. Obviously, these distinct IoT enabling technologies result in siloed operations in various applicable scenarios. Thus, to eliminate the underlying differences below Transport layer, an Adaptation layer can be utilized to link Non-IP and IP enablers with the Internet, the cloud or simply the centralized applications for achieving cross-silo IoT communications. As shown in Fig. 4 – (b), in line with previous philosophy, lots of ecosystems are established accordingly, such as Apple HomeKit, Google Weave, Open Interconnect Consortium, AllSeen Alliance and so forth, for IoT interoperations in Application layer or in Cloud. However, these independently formulated ecosystems become individual bigger silos at their infancies. As a result, for fulfilling the vision of complete interoperability of IoT, the trend of cross-eco communications is arising recently, which is diversely through merging, liaison, asset transfer, or interworking protocols as explicitly illustrated in Fig. 4 – (c) for exemplifying the newly formed Open Connectivity Foundation (OCF). Note that Huawei has established its own IoT ecosystem, which consists of OpenLife Platform, HiLink Protocol, LiteOS, and IoT chipsets.

Based on the observations in Fig. 4, we have proposed a generalized type of internetworking denoted as ION, which adopts the identifier locator split framework and constructs an additional layer below Transport layer for horizontally universal connections, including cross-silo/eco IoT cases. The following section will introduce the details of ION.

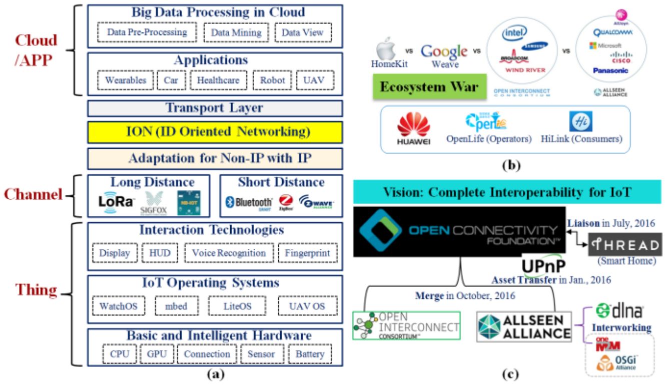


Figure 4. Trend of Cross-Silo and Cross-Eco IoT Communications.

III. ID ORIENTED NETWORKING

This section introduces ID Oriented Networking (ION) concept and architecture in detail, with the background, implementation framework, essential merits, and relevance to cross-silo and cross-eco IoT communications.

A. *ION Background*

Future networks need to satisfy many demanding requirements such as high throughput, extremely low latency, flexible mobility, intrinsic security, networking automation, and so forth. Recently, at the European Telecommunications Standards Institute (ETSI) Next Generation Protocol (NGP) forum [11], Huawei introduced IP2020 which aims to meet these requirements for various future life scenarios (e.g., autonomous driving, tactile internet, AR/VR). IP2020 is a holistic solution that includes a high-throughput transport layer, Self-X networking automation, intrinsic network security and ID Oriented Networking.

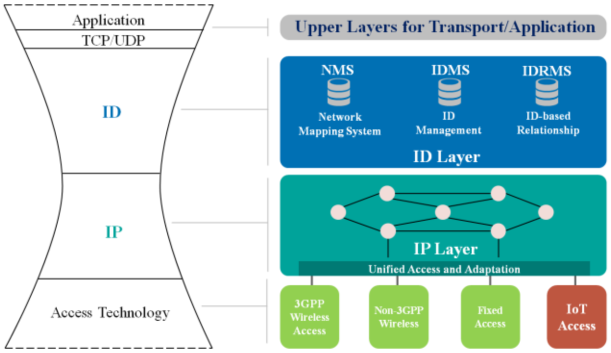


Figure 5. ID Oriented Networking (ION) Overview.

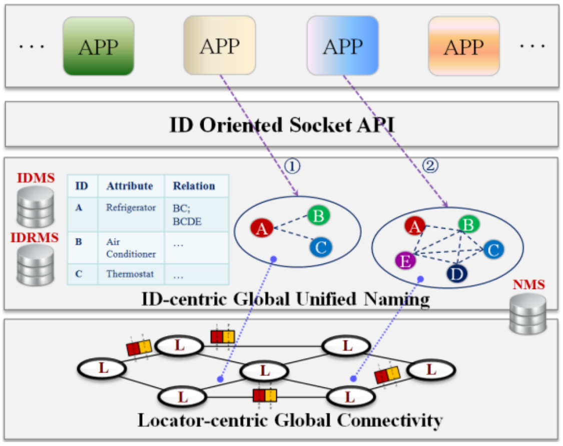
B. *ION Overview*

As shown in Fig. 5, ION follows the idea of Identifier (ID) and Locator Split (ILS) in general [12]. As is well known, the traditional Internet Protocol (IP) address assumes overloaded semantics of being both endpoint identifier and routing locator. Over past years, several proposals have been formulated to decouple the IP into two layers, which contributes to ID and IP layers as shown in Fig. 5 [11]. The IP layer aligns with the successful Internet practices to establish global reachability while ID layer performs functions essential for an endpoint's identity. The ID layer in ION framework has three components: Network Mapping System (NMS) for translating ID to locator whenever queried; ID Management System (IDMS) for centralized or distributed management of universal identifiers; ID Relationship Management System (IDRMS) for maintaining proper relations among ID-labeled physical or virtual entities. In addition, the data or information associated with all these indentified entities should be managed as well, which might resort to cloud-based solutions for vast data storage and analytics and is currently beyond the scope of ION.

As previously mentioned, the idea behind ILS is not novel for usage in ION, which can be observed in many existing ILS research [12]. In the literature, identifiers could be categorized into three classes: IDs over pure IP addresses having different connotations, as in LISP and ILNP; flat IDs based on PKI with self-certifying features, including HIP and MobilityFirst; hierarchical or hybrid IDs, as designed in RANGI [13]. Moreover, for translating ID to locator, many mapping systems are proposed accordingly, such as RVS for HIP and GNRS for MobilityFirst, while our previous work presents a comprehensive summary as well [14].

C. *ION Implementation Framework (IONIF)*

In this sub-section, an ION Implementation Framework (IONIF) towards globally unified IoT communications is elaborated. IONIF is the realization of ION architecture, which integrates ID management, NMS, and IP reachability, to deliver ID aware networks. Applications benefit from ID aware transport using ID-oriented API, and the enabled sockets are location agnostic and can preserve end-to-end connections even the underlying locator layer attributes change. As in Fig. 6, the IONIF has four layers, which are locator, ID, ID-oriented socket API, and application layers, which comply with the previously layered ION overview.



ID	Attribute	Relation
A	Refrigerator	BC; BCDE
B	Air Conditioner	…
C	Thermostat	…

Figure 6. ION Implementation Framework (IONIF).

More specifically, the locator layer aims at achieving global connectivity via locator-based addressing and routing. As shown in Fig. 5, the most promising candidate of such global connectivity locator should be IP and its variants, which specify the destinations for packet-based deliveries [2]. The ID layer, as the core of IONIF, presents unique features for building flexible on-demand relationships horizontally, and satisfying upper layers' demands vertically. With the assistance of a global-scale ID Management System (IDMS), a worldwide unified ID management can be realized, which potentially supports distinct ID formats as well. Along with IDMS, on-demand relationships are created and managed according to specific application requirements in ID Relationship Management System (IDRMS), in a proactive or reactive manner. Furthermore, IDMS and IDRMS could be integrated to manage the identifiers with their respective semantic attributes and relationships, such as ID 'A' indicates a refrigerator associating with other entities in Fig.6.

Furthermore, as previously observed in Fig. 5, the access and IoT hardware heterogeneity has been shielded by the function of unified access and adaptation, thus the ID layer is able to enable Radio Access Technology (RAT) agnostic functions such as ID-based access control, ID-enabled privacy protection, ID-aware AAA, and other policies. In addition, for properly locating communication endpoints and supporting RAT-agnostic mobility management, NMS is dynamically used to map identifiers to locators. The NMS may be maintained by dedicated organizations, working in centralized or hierarchical decentralized manner, resembling the traditional DNS or some new design paradigms [14]-[16].

Above the ID layer, there exists an ID-oriented socket API for ID-aware data transmissions, which provides the interface to application layer and has adaptability to lower-layer ID-based on-demand relationships. Moreover, in application layer, individual applications may request to establish tailored relationships for their operating things through this ID-oriented API. For example, a control application for home appliances, including refrigerator, air conditioner, thermostat etc., requires to build a same-owner relationship among these appliances belonging to different manufacturers. Note that some fundamental Thing-to-Thing relationships are well investigated in Social IoT (SIoT) [4], which can be referred to for relation establishment in IONIF.

As illustrated in Fig. 6, the horizontal relationship for an IoT community may further embrace a new feature of automatic relation-aware self-expansion, which determines useful and useless relationships for upper layer services by dynamically enrolling new members or removing existing members in a relational cluster. For instance, the relation formulated by pointer ① for one application could be expanded to a renewed relation initiated by the same application, through involving new members with updated relations. Alternatively, individual applications with different services may also activate distinct relationships having partially shared members, as pointed by ① and ② for two applications sharing three common members. For IONIF, these horizontal ID-based relationships are maintained in IDRMS, being assisted by IDMS.

Currently, the IONIF is still under development and refinement, and its core implementation components presented in this sub-section are able to accelerate global connectivity for unified IoT communications in near future. In which, Thing-to-Thing relations are maintained just like human society, and these things' relations are expected to be further intertwined with human behavior and services.

D. *ION for IoT Interoperations*

Based on above description, IONIF shows the potential for the future IoT interoperations in Fig. 7, other than integrated operations in the application layer. Previously, the IoT evolution has shown the trend towards cross-silo and cross-eco communications. In near future, with the help of ION, a unified IoT cross operation could be easily built upon ID layer, facilitating all the actions demonstrated in Fig. 3. In particular, regardless of IoT enabling technologies (e.g., Bluetooth, Z-Wave, LoRa, etc.), the universal adaptation layer normalizes the data transmitted among different IoT verticals, and further enables the connection with IP layer for global reachability. In addition, IDs defined in ION can persistently label all communication endpoints, without considering their specific routing locations. Note that the dynamic binding from ID to IP for smooth data transmission could be at the level of individual things supporting IP or at the level of IoT gateways with local locators other than IP.

As a result, the heterogeneity of IoT technologies become hidden beneath ID layer, as in Figures 5 and 6, and upper services can request any type of on-demand relationship over IoT terminals, which fully satisfies the future trend.

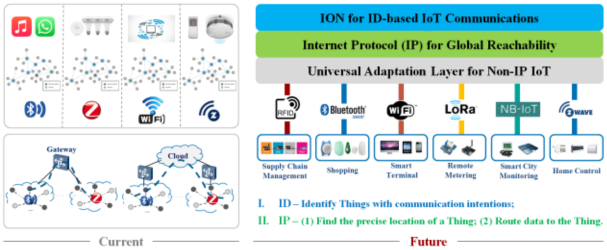

ION for ID-based IoT Communications
Internet Protocol (IP) for Global Reachability
Universal Adaptation Layer for Non-IP IoT
RFID
Bluetooth
WiFi
LoRa
NB-IoT
Z-WAVE
Supply Chain Management
Shopping
Smart Terminal
Remote Metering
Smart City Monitoring
Home Control
I. ID – Identify Things with communication intentions;
II. IP – (1) Find the precise location of a Thing; (2) Route data to the Thing.
Gateway
Cloud
WiFi
Current
Future

Figure 7. ION for ID-based IoT Communications.

E. *ION Merits*

As shown in Figures 5-7, the merits of introducing ION for IoT interoperations, other than the present IoT integration in application layer, are multifold, which are concisely summarized below:

- *Labels of Communication Entities*: Currently, the communication identifiers of IoT terminals are in different formats in individual IoT enabling technologies. Thus, a unified identifier naming paradigm is highly desirable in the ID layer as shown in Figures 5-7, for consistent labeling of communicating IoT entities across various domains or ecosystems. Although this unified identifier could be a long-term multilateral effort, there exist a few trials of promoting such type of identifier [13], [15]-[17]. For example, a PKI-based hash value in binary format may be used as a unique 128-bit identifier as suggested in RANGI scheme [13].
- *Intrinsic Security*: Besides the link-level security in pairing stage of individual IoT technologies (e.g., Bluetooth and ZigBee), an intrinsic level of security built upon Identity Based Signature (IBS) scheme is under development, for the purpose of enforcing future mobility security, network trust, and identity and key management [11]. As expected, authentication before establishing a transport layer connection may close many security holes nowadays in TCP/IP protocols, while further reducing the burden of deep packet inspection and the consequent overhead [18].
- *Mobility Support for IoT Terminals*: ION largely follows the ILS paradigm, as described in previous sections, it thus naturally supports mobility of IoT terminals. Note that the fundamental principle behind mobility support is consistent communication identifiers regardless of location changes [12].
- *Social Community of Things*: This is a prominent feature in line with IoT evolution in Section II, as Thing-to-Thing interconnections become pervasive. Based on the observation in Fig. 6, a social community with on-demand relationships among smart things could be established upon specific service requests. Meanwhile, such social community can be managed similarly as human society, with dynamic enrollment or removal and intelligent interaction, for achieving valued-added functions in autonomy.

IV. FUTURE WORK

For ION utilization in large scale, many challenges are inevitable in front, and are briefly discussed in this section, for the purpose of future work.

As highlighted in Fig. 6 for IONIF, two essential elements of ION, i.e., IDMS and IDRMS, are logically intertwined for managing the universal identifiers and their on-demand relationships. However, unifying distinguished identifier formats of various IoT regimes under a single framework may take unexpected effort to achieve, and the consensus over atomic relationship definition for IoT terminals may encounter similar difficulty. Thus, the ID format definition with various ID support should be revisited, along their potentially dynamic relationships in a socialized community. Meanwhile, an extended universal adaptation plane might be utilized to bridge existing siloed identifier domains, based on the adaptation layer shown in Fig. 7, which also needs a further study.

As noticed, ION naturally support mobility due to constant communication identifiers, however, the mapping from identifier to locator may take additional time and becomes a new bottleneck. Thus, the NMS in ION should be further explored to fully support mobility of IoT terminals in distinct scenarios, which may accommodate all current ID formats in a unified way. Accordingly, an IDEAS group has been recently formulated in IETF, with the target of new mapping system design with novel principles and proof-of-concept verifications for ILS schemes in general [19]. As a result, a generalized IoT mobility may be enhanced through a united endeavor over NMS design in near future.

Furthermore, the security imposed by ION over IoT communications should be well designed so as to enable all-round protections. As aforementioned, IoT security can be boosted after the introduction of ION in ID layer for future networks. However, since the interconnections and the accompanying data with the IoT terminals continue to be dramatically increasing, the security in every phase could be threatened, which occurs either in cross layer or in a hybrid manner. Thus, formulating a holistic security scheme, with consideration of identification, authentication, integrity, privacy, trust, safety, reliability, responsiveness, immunity, autonomy and so forth, is always a challenging work for candidate research [18].

ION socket, for broadly enabling ION implementation, may require modifications on host side. Thus, the problem of smooth adoption of ION in large scale, with minimum impacts on other layers is worthwhile to be further examined. The viable solutions might be either through a middleware for properly linking legacy and ION-based transmissions, or through an ID-aware socket that understands intrinsic connotations when legacy and ION-based IDs are actually utilized.

As previously observed in IoT evolution, integrating IoT technologies with cloud computing is also a desirable trend for ION to serve IoT practices with hugely manageable data behind identifiers. Thus, hierarchical cloud enabled (i.e., fog/edge/core clouds) IoT under ION framework is a valuable extension as well.

In summary, for achieving unified IoT communications, the functional components and key enabling technologies under the proposed ION framework are of importance for future refinement and study.

V. CONCLUSION

In this paper, the basic IoT architectures with its evolution stages are firstly introduced, which is followed by the driving forces and trends for cross-silo and cross-eco IoT interoperations. Subsequently, ID Oriented Networking (ION) with the corresponding background, core functional components, and implementation framework are elaborated. Finally, the merits and future work are briefly discussed.

Overall, a smart world with unified communications under ION framework is imaginable, where generalized intelligent things in all types are agilely interconnected for providing integrated services to numerous local and global demanders.

REFERENCES

[1] Kevin Ashton, “That ‘internet of things’ thing,” RFID Journal, pp. 97-114, 2009.

[2] S. Li, D. Li, and S. Zhao, “The internet of things: a survey,” Information Systems Frontiers, pp. 243-259, 2015.

[3] D. Zeng, S. Guo, and Z. Cheng, “The web of things: a survey,” Journal of Communications, pp. 424-438, 2011.

[4] L. Atzori, A. Iera, G. Morabito, et al, “The social internet of things (SIoT) - when social networks meet the internet of things: concept, architecture and network characterization,” Computer Networks, pp. 3594-3608, 2012.

[5] S. Distefano, G. Merlino, and A. Puliafito, “Enabling the cloud of things,” in Proceedings of IEEE Sixth International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2012, pp. 858-863.

[6] A. Botta, W. Donato, et al, “Integration of cloud computing and internet of things: a survey,” Future Generation Computer Systems, pp. 684-700, 2016.

[7] A. Al-Fuqaha, M. Guizani, et al, “Internet of things: a survey on enabling technologies, protocols, and applications,” IEEE Communications Surveys & Tutorials, pp. 2347-2376, 2015.

[8] I. Farris, R. Girau, et al, “Social virtual objects in the edge cloud,” IEEE Cloud Computing, pp. 20-28, 2015.

[9] IoT-A Reference Model: http://www.iot-a.eu

[10] J. P. Bardyn, T. Melly, et al, “IoT: The era of LPWAN is starting now,” in Proceedings of IEEE European Solid-State Circuits Conference (ESSCIRC), Oct. 2016, pp. 25-30.

[11] Huawei IP 2020 Project Introduction is available: http://www.layer123.com/download&doc=Huawei-1016-Renwei-Towards_2020-Challenges

[12] W. Ramirez, X. Masip-Bruin, et al, “A survey and taxonomy of ID/Locator Split Architectures (ILSA),” Computer Networks, pp. 13-33, 2014.

[13] Y. Jia, X. Lu, et al, “A novel host mobility support method in IPv4/IPv6 network of RANGI architecture,” in Proceedings of IEEE International Conference on Fuzzy Systems and Knowledge Discovery (FSKD), 2012, pp. 2083-2087.

[14] Bin Da, X. Xu, K. Bi, and X. Zheng, “DNS with mapping service in identifier locator split architecture,” in Proceedings of 22nd APCC Conference, 2016, pp. 470-475.

[15] A. Sharma, X. Tie, et al, “A global name service for a highly mobile internetwork,” ACM SIGCOMM Computer Communication Review, vol. 44, no. 4, pp. 247-258, 2014.

[16] V. P. Kafle, Y. Fukushima, and H. Harai, “ID-based communication for realizing IoT and M2M in future heterogeneous mobile networks,” in Proceedings of IEEE International Conference on Recent Advances in IoT, 2015.

[17] Felice Armenio, Henri Barthel, et al, “The EPCglobal architecture framework,” 2005.

[18] J. Granjal, E. Monteiro, and J. S. Silva, “Security for the internet of things: a survey of existing protocols and open research issues,” IEEE Communications Surveys & Tutorials, pp. 1294-1312, 2015.

[19] IETF ID EnAbled networkS (IDEAS) Mailing List: https://mailarchive.ietf.org/arch/search/?email_list=ideas