Ad Hoc Networks 000 (2016) 1–11

Contents lists available at ScienceDirect

Ad Hoc Networks

journal homepage: www.elsevier.com/locate/adhoc

Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT)

Oladayo Bello[a,*], Sherali Zeadally[b], Mohammad Badra[c]

[a] School of Information Technology, Monash University, South Africa campus, South Africa
[b] College of Communication and Information, University of Kentucky, Lexington, KY, 40506, USA
[c] Zayed University, P.O. Box 19282, Dubai, United Arab Emirates

ARTICLE INFO

Article history:
Received 13 April 2016
Revised 13 June 2016
Accepted 20 June 2016
Available online xxx

Keywords:
Bluetooth
Device-to-Device
Internet of Things
Interoperability
IPv6
PLC
RFID
Zigbee

ABSTRACT

The goal of the Internet of Things (IoT) is to create an integrated ecosystem for devices to communicate over the Internet. To achieve this goal, efficient inter-operation is needed among Device to Device (D2D) communication technologies that make up the ecosystem. Currently, these technologies operate in vertical silos with different protocols. We explore the challenges associated with the integration and interoperability of these D2D technologies by focusing on network layer functions such as addressing, routing, mobility, security and resource optimization. We identify the limitations of the current TCP/IP architecture for D2D communication in the IoT environment. We also discuss some of the limitations of the 6LoWPAN architecture and *describe how it has been adopted for D2D communication.* Finally, we present solutions to address the limitations we have identified for the network layer functions as applicable to D2D communication in the IoT environment.

1. Introduction

Over the years, communication between humans as well as communication between human and devices has evolved a lot. The ubiquitous deployment and use of devices of all kinds have made device to device communication increasingly important. Today, various types of devices are either attached to humans (for interaction or monitoring) or operate on their own (for control or automation). These devices are personal electronics, home appliances, health monitors, smart vehicles, industrial sensors and actuators.

The Internet of Things (IoT) ecosystem is a platform that enables these uniquely identifiable devices with Internet connectivity capability, so that they can transmit information between each other and with humans. It is a complex, vast and rapidly expanding ecosystem that enables global seamless ubiquitous intercommunication between devices.

Seamless ubiquitous connectivity between devices has been fueled by the need for easy access to data, which can be processed and utilized to provide improved services for applications such as smart grid, health monitoring, home area networking, building automation and vehicular communication and telecommunication [1]. Thus, almost all devices ranging from health monitors, sensors, industrial automation devices, vehicles and home appliances now possess Internet connectivity capability which has increased the adoption and proliferation of the IoT. Several forecasts predict that by 2020, the number of everyday objects/devices (things) that will be connected to the Internet will reach about 50 billion [2]. Fig. 1 shows how the number of connected devices continues to rise significantly in comparison with the world's population. The increase started with the proliferation of consumer devices (e.g., smartphones, tablets, laptops, TVs and home appliances). However, over time, most connected devices deployed will be in industrial and public sectors (e.g., RFID tags, soil monitoring sensors, building sensors, street lights, and smart meters).

The strong interest in IoT began with the emergence of smart phones, which have been used to create new applications/services that are generating new revenue streams. Subsequently, more device manufacturers got motivated to develop even more smart devices to support emerging applications and services such as mobile-money and mobile crowd-sensing (where data is collected for decision and policy making). The IoT also promotes new business models for telecommunications (e.g., pay per use) [1]. Semantics and intelligent sensing coupled with learning algorithms can also be used to develop new applications. For example, a smart device can use semantics to infer user's intentions and

* Corresponding author.
E-mail addresses: oladayo@ieee.org (O. Bello), szeadally@uky.edu (S. Zeadally), mbadra@gmail.com (M. Badra).

http://dx.doi.org/10.1016/j.adhoc.2016.06.010
1570-8705/

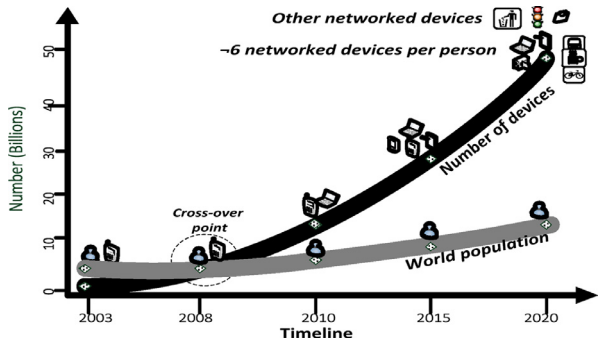

Fig. 1. Growth of connected devices [2].

provide services based on the inferences without user's involvement. Such an application can be provided by a smart home entertainment system that has the ability to determine which service(s) to provide according to the user's preferences.

New paradigms stimulating the rapid deployment of IoT include Software Defined Networking (SDN), Information Centric Networking (ICN), Network Functionality Virtualization (NFV), Bluetooth Low Energy (BLE), Nearby Field Communication (NFC), and Wireless Fidelity-direct (WiFi-direct). Fog networks and big data analytics are also emerging concepts advancing the adoption of IoT [1].

Many IoT applications involve the pervasive aggregation of data from devices in order to manage the physical world [3]. Predictive analytics and real-time optimization models can be applied to such data for the creation of the wealth of knowledge that will enable a "smart world", which is the main goal of the IoT [1]. However, this data collection and analysis are possible if the data can be accessed over the Internet. To achieve this goal, interconnectivity and interoperability are required among different types of heterogeneous devices that co-exist in the IoT ecosystem. Most IoT devices are expected to be self-configuring and adaptive thereby reducing human intervention. As such, Device-to-Device (D2D) communication is expected to be an intrinsic part of the IoT ecosystem. Typically, D2D communication involves direct short-range communication between devices without the support of a network infrastructure (e.g., base stations or access points). In D2D communication, devices co-operate to exchange information among each other via multi-hop transmissions. Most applications/service in the IoT ecosystem will be realized by D2D communication networks such as the Digital Enhanced Cordless Telecommunications Ultra Low Energy (DECT ULE), Zigbee, Bluetooth Low Energy (BLE), Power Line Communication (PLC), Radio Frequency Identification (RFID) and Near Field Communication (NFC) [4]. However, these are proprietary communication technology standards, which have existed in vertical silos. Besides, they were designed for applications that did not require Internet connectivity for devices.

Although D2D communication will be predominant in the IoT, yet much of the attention on D2D communication has focused primarily on the Long Term Evolution (LTE) cellular network. Cellular networks are a part of the IoT ecosystem, but most D2D communications will be carried out by devices such as sensors and actuators. Since diverse IP and non-IP technologies will co-exist in the IoT, it is vital to understand the integration challenges that need to be addressed at the network layer in order to enable seamless ubiquitous connectivity among D2D communication devices in the IoT.

Basically, the IoT ecosystem's platform can be divided into three levels namely, the sensing level (for data generation), communication level (for device connectivity and data transmission) and management level (for data collection, storage, processing and management) [5]. The sensing level includes mobile or stationary devices that can generate data in various formats while the communication level includes existing and emerging wired or wireless communication networks. At the management level, data collection, storage and analysis technologies are needed.

1.1. Main research contributions and organization of this work

With reference to the communication level and a focus on D2D communication in the IoT, (a) we highlight some inherent limitations of the current Internet-based protocol stack; (b) we provide some insight into the inter-operation issues, limitations of some D2D technologies including the adoption of IPv6 over Low power Wireless Personal Area Networks (6LoWPAN); (c) we identify some open issues of 6LoWPAN and recommend solutions for them; and (d) we present the challenges and solutions for network layer inter-operation protocols for D2D communications.

The remainder of this paper is organized as follows. Section 2 discusses the limitations of the TCP/IP architecture that makes its implementation on resource constrained D2D communication devices problematic. Section 3 focuses on inter-operation approaches, the adaptation of 6LoWPAN in some D2D technologies and its limitations. In Section 4, proposed solutions that address the network layer protocol challenges for D2D communications are presented. Finally, Section 5 concludes the paper.

2. Implementation challenges of the TCP/IP architecture for D2D communication in IoT

Generally, devices in any communication network use a set of rules (protocols) for data transmissions [6]. The TCP/IP architecture is the framework that underpins the communication rules within the Internet. It breaks down data transmission between any two devices into five functional layers, namely: the physical, data-link, network, transport and application layers. Many networking technologies have been developed based on these functional layers. As data moves between layers, extra framing and control data is added to the main data. Such additional information requires processing and thus incurs substantial processing power and memory capacity. However, most of the IoT devices cannot meet this requirement. In addition, D2D communication in the IoT is characterized by the heterogeneity and mobility of a plethora of devices. Thus, the ecosystem will have to be scalable to enable the reliable transmission of information between devices [7]. However, the TCP/IP protocols for the Internet are not designed to support the high level of scalability, high amount of traffic and mobility presented by the IoT ecosystem [7]. They are significantly limited in satisfying these new requirements [8].

In this section, we identify and discuss the design features of the TCP/IP architecture that make it difficult to implement on D2D communication devices in the IoT environment.

2.1. Limitations of the TCP/IP architecture for IoT

The TCP/IP protocol stack cannot enable optimized D2D communication in the IoT because of its built-in properties and operations such as:

2.1.1. TCP/IP protocol stack is heavyweight

The TCP/IP stack requires high bandwidth, processing power, battery power and memory. It needs resources such as sockets and buffers to achieve its goal. These resources, however, consume memory and battery power [9], which are limited resources on highly constrained IoT devices [10]. Usually, a TCP/IP stack stores any packet received in a network buffer before it is accessed by the upper layer protocol. Likewise, any data to be sent is also placed in such buffers before transmission. IoT devices may not have enough

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

memory space to be utilized as network buffers to store data to be sent or data received as required by the TCP/IP stack.

2.1.2. Fragmentation and re-assembly

The TCP/IP architecture permits a sending device to fragment large chunks of data into smaller chunks and the re-assembly of the data at the receiver. Fragmentation is performed when a device tries to transmit data that is larger than the Maximum Transmission Unit (MTU) allowed by its network. Each fragment contains information in the header for forwarding to the final destination [11]. This information creates overhead and the processing needs additional processing power. The results in [12, 13] shows that fragmentation can significantly degrade the performance of devices in the IoT ecosystem. Fragmentation of data before transmission may also open the transmission to security threats. In addition, the loss of fragmented data and the need for re-transmission may degrade the reliability and integrity of the transmitted data. In general, for resource-constrained networks involving D2D communication devices, the authors in [12] recommend the need for new solutions that avoid fragmentation.

2.1.3. Addressing scheme

The TCP/IP protocol stack adds additional meta-data (i.e., headers and fields) at every layer, thus causing additional processing, which consume memory and computing power.

2.1.4. Packet acknowledgement and retransmission

The requirements for reliability through packet acknowledgement at higher layers hinder the adaptation of TCP/IP protocols on D2D communication devices in the IoT. Re-transmissions cause increased power consumption and drain the limited battery power further. Each transmitted bit uses energy and minimizing energy consumption is needed [14, 15].

2.1.5. No built-in security capability

The TCP/IP design architecture lacks an all-encompassing security mechanism because security was not considered in the original design. Security mechanisms are adapted as sub-layers, thus causing overload and extra processing.

2.1.6. Error control and detection mechanism

The need for error correction and detection slows down traffic flows within network and also consumes additional computing and memory resources at the end systems.

2.1.7. Flow control mechanism

TCP uses a window-based mechanism for flow control. The issue here is that typically; the network can transmit data faster than a typical D2D communication device can process. If a device continuously receives data without being able to process them, its receiving window size will eventually decrease to zero. A zero window size however, indicates that a device is unable to receive data and thus the transmitter should stop its transmission. The number of operations required by the TCP/IP stack will waste the limited resources (such as bandwidth memory capacity, battery and processing power) of D2D communication devices.

2.2. Constrained resources in D2D communication devices

2.2.1. Bandwidth

Devices in constrained networks typically have low achievable data rate of 20 kbps–250 kbps or less [14]. Some of these devices (e.g., light switch/passive sensor) are used for simple applications and do not need to transmit large amounts of data [16]. Bandwidth constraints of devices in the IoT limit the amount and speed of transmission at any time so they are unable to implement complex communication protocols.

2.2.2. Memory capacity

The Random Access Memory (RAM) size for constrained devices is between few kilobytes and a dozen of kilobytes [17]. The storage size limits the amount of data that can be buffered at any time. Therefore, such devices cannot store data to be sent or received before and after any transmission for upper layer processing. As such, some data may be discarded if it exceeds the allowable limit of a memory-constrained device.

2.2.3. Energy capacity

It is the amount of power available for a device to sustain itself over a period of time. A device's sustainable period includes its functional and sleeping states. The functional states are transmission, receiving, listening and overhearing states. According to [17], the power source for an energy-limited device can be recharged or replaced after some time. However, non-rechargeable devices are discarded after the power has been consumed. So, to save the battery-life of constrained devices, low bandwidth connections are desirable [18].

2.2.4. Processing capacity

Processing capacity indicates the amount of computing power a device possesses. The majority of IoT devices (e.g., RFID tags) are small, low cost devices with very low processing capacity. Thus, such devices require light-weight communication protocols to operate efficiently. They usually have 8-bit processors and clock rates of about 10 MHz. However, other devices such as consumer electronic devices, laptop computers, mobile phones, automobiles and home appliances in the IoT environment may have medium to high processing capacities. These devices constitute a minority group of devices in the IoT environment with processors ranging from 16-bit to 64-bit core and frequencies up to the gigahertz [19].

3. Interoperating D2D communication technologies in the IoT

The problem of interoperability in the IoT ecosystem arises at every layer of the protocol stack because of the heterogeneity of devices, applications and networks. Diverse use-case applications exist within the IoT. In addition, different proprietary D2D communication technologies exist. These technologies aim to provide solutions to a set of requirements for different application scenarios. So there is no and there may never be a single technology that will meet the requirements of all applications to be deployed in the IoT [20]. For example, BLE fulfils the need to run devices on a button cell battery, while ZigBee creates inexpensive D2D networks with no centralized infrastructure. As such the billions of devices in the IoT are expected to operate with different technologies to provide different services. However, an IoT application may also require simultaneous interaction between devices implementing different technologies, as in home automation, smart city and smart grid applications [1]. These applications highlight the inevitability of inter-operating and integrating D2D technologies in the IoT. Thus the problem of interoperability requires a more pragmatic and comprehensive approach. There have been several efforts towards solving the interoperability issues within the IoT, but most are focused on the application layer.

In this paper, we focus on how to achieve network layer interoperations of D2D communication technologies. A network layer solution for interoperating D2D technologies is crucial because each technology operates with unique and customized protocol stack. The IoT ecosystem will be fully realized when the data across silo systems is utilized to provide end-to-end solutions [21,22].

Fig. 2 depicts two approaches for interoperating silo networks. Fig. 2a requires a maximum of $n(n-1)/2$ solutions, where n is the number of D2D technology and Fig. 2b requires only one solution. Since it is envisaged that the IoT will continue to grow with the

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

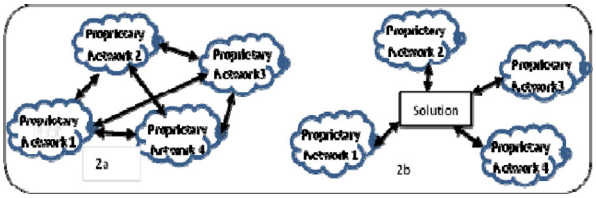

Fig. 2. Interoperating vertical D2D technology silos [23].

addition of new devices, services and technologies, the approach in Fig. 2a is expensive and is not scalable. However, for Fig. 2b, a significant challenge is identifying the universal and standardized interoperability framework at the network layer.

In this section, we discuss how the 6LoWPAN has been incorporated into some D2D technologies in the IoT. In addition, some drawbacks of the 6LoWPAN are presented.

3.1. 6LoWPAN

6LoWPAN is the scaled down version of the IPv6 standard for LoWPANs [26]. LoWPANs are D2D networks for resource constrained devices. The 6LoWPAN was developed for LoWPANs to facilitate the transmission of IPv6 packets. It modifies the TCP/IP protocol stack by introducing an adaptation layer between the link and network layers as shown in Fig. 3. It performs three key functions: Header Compression (HC), Fragmentation and Reassembly (FAR) and layer two forwarding. The HC mechanism reduces the overhead associated with the transmission of IPv6 packet. Layer two forwarding enables the delivery of IPv6 packets over multiple hops [25]. The adaptation layer also performs neighbor discovery and multicasting functions. The key functions make the header small and easy to parse [26] so as to reduce the overhead, bandwidth, processing and power consumption on resource constrained devices.

Next, we discuss typical D2D constrained network technologies such as DECT ULE, PLC, RFID, BLE and Zigbee and their limitations and how the 6LoWPAN is leveraged to enable them interoperate.

3.1.1. Digital enhanced cordless telecommunications ultra low energy (DECT ULE)

DECT ULE provides packet-mode data transmission for low-bandwidth and low-power D2D communications applications [28]. It has two parts: the Portable Part (PP), which is the constrained device and the Fixed Part (FP), which is the base station. The FPs may provide Internet connectivity for PPs [27]. Fig. 3 shows the DECT ULE protocol stack with 6LoWPAN adaptation layer. The PHY layer operates within 1880 MHz–1920 MHz with a symbol rate of 1.152 Mbits/s [27]. The MAC layer supports channel selection, and it establishes and releases connections for device discovery and pairing. It also enables broadcast beacon transmissions for PPs to identify FPs to connect with. Multiplexing and FAR are provided by the Data Link Control (DLC). The C-plane of the DLC supports signaling operations while the U-plane enables end-to-end user information transfer [28]. Channel access is accomplished through Frequency Division Multiple Access (FDMA), Time Division Multiple Access (TDMA) or Time Division Duplex (TDD). The common network topology for DECT is star topology.

IoT applications: home automation, home security, smart meters, home health monitoring.

Use case: A pendant can be used to transmit status messages to a health care provider using very little battery power. However, in case of an emergency, the pendant can set up a voice connection to an alarm service for the patient [27].

Devices: smart meters, door lock, patient monitoring devices.

Limitations: 1) Mesh topology is not supported. 2) Multicast is not supported but can be achieved by replicating unicast messages on each link, which is not energy-efficient [27].

3.1.2. IEEE 1901.2 standard

It specifies the PHY and MAC technology for narrow band D2D communication via existing alternating and direct current electric power-lines for less than 500 KHz power-line devices [29, 30]. However, devices implementing the IEEE 1901.2 standard still share the same constraints as devices using the wireless medium [31]. Fig. 3 illustrates the IEEE 1901.2 protocol stack. The PHY layer supports communication in the 10 KHz–490 KHz band using Orthogonal Frequency Division Multiple Access (OFDM) to provide robust communication over the harsh power-line medium [29]. The Adaptation (ADP) sub-layer offers an interface for the 6LoWPAN layer, compresses and decompresses datagrams for transmission via the power-line. It may also supervise the network attachment procedure for devices [29]. The MAC sub-layer is an enhancement of the IEEE802.15.4-2006 standard and allows channel access through the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism with a random back-off time. It also performs FAR, connection set-up and maintenance; and topology resolution.

IoT application: smart grid networks, home area networks, road transport communication, intelligent street lighting.

Use case: For home-to-grid applications, devices can interact directly with the electricity grid via the Internet to report utilized energy [32]. Other home appliances can also report their energy utilization for users to adjust their energy consumption.

Device: smart electric meters, home appliances, electric plugs.

Limitation: 1) As the number of devices on the Power Line Communication (PLC) network increases, a larger address space will be required to ensure end-to-end connectivity so that new applications can work in a transparent manner [32]. 2) The standard does not support efficient multicasts.

3.1.3. Radio frequency identification (RFID)

RFID technology uses radio frequency signals to identify and monitor objects or people in real-time without the need for line-of-sight connection [33]. A RFID system comprises of a tag, a reader and a host. A tag is a microchip that communicates via wireless links on radio frequencies between 125 KHz–915 MHz. Tags are usually passive read-only devices with no processing capability [34]. However, some tags are classified as active tags because they have read-write capability and built-in battery. Readers transmit information to tags by modulating a Radio Frequency (RF) signal. Passive tags within the range of a reader receive information and operating energy from the modulated RF signal. Readers receive information from tags by transmitting Continuous Wave (CW) RF signals to tags.

IoT application: asset tracking, wildlife monitoring, vehicle identification, retail logistics and healthcare monitoring.

Use case: (1) Tags can be attached to clothing or other items and an alarm is triggered if the goods leave the store before the tag is deactivated. (2) RFID tags may also be attached to animals or vehicles in order to track them through the reader.

Device: RFID tags.

Limitations: (1) Requires a large addressing space to manage different identification codes for tags. (2) As tags move around, their network prefix changes thus, keeping track of tags becomes challenging [35]. (3) Data security and user privacy is a challenge as tags are prone to unauthorized access, traffic analysis and denial of service attacks [36].

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

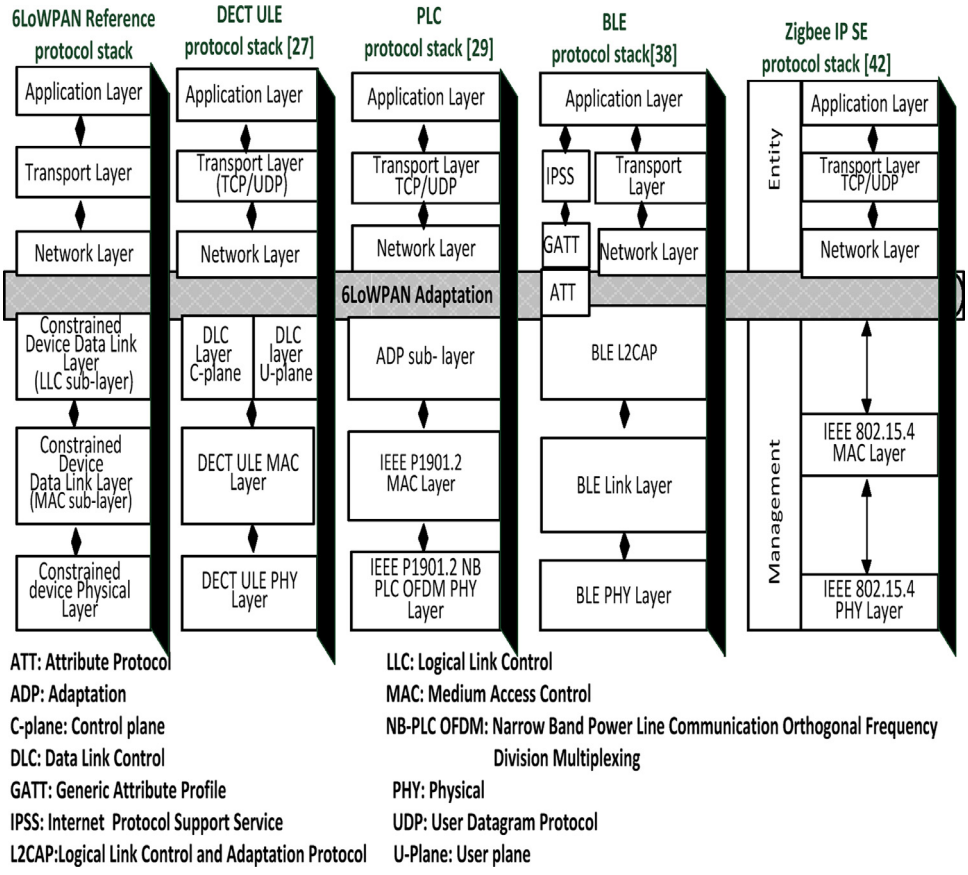

Fig. 3. 6LoWPAN on vertical D2D technology silos.

3.1.4. Bluetooth low energy (BLE)

BLE enhances the classic Bluetooth standard by allowing wireless connectivity for low cost devices that operate with ultra-low power [37]. It is useful for devices transferring small quantity of data at low data rate within relatively short ranges.

The BLE PHY layer depicted in Fig. 3 defines two PHY channels, which are the piconet and advertising channels. Devices can use only one of these channels at a time. Piconet channels are used for communication between connected devices and are associated with specific piconets. Advertising channels are used to broadcast information to disconnected devices or to set up connections between devices.

The BLE link layer performs acknowledgement and repeat request [38]. The BLE Logical Link Control and Adaptation Layer Protocol (L2CAP) support connection-oriented channels, multiplexing and error control. It uses a credit-based scheme to multiplex data sent over multiple channels [39]. It also performs FAR to allow efficient transfer of large data. Internet Protocol Support Services (IPSS) enables the discovery of other IP-enabled devices and sets up link-layer connection for transmitting data. The set-up allows 6LoWPAN to operate. The Attribute Protocol (ATT) enables a device (server) to expose its set of attributes and associated parameters to a peer device (client) while the Generic Attribute Profile (GATT) uses the ATT to define the procedure, format and characteristics of a service. The BLE protocol stack in Fig. 3 supports address autoconfiguration [40] and neighbor discovery.

IoT application: health and fitness, proximity applications, body sensors, in-car communication and home automation.

Use case: (1) To enable presence detection, such that light is either turned off or on, or a door is shut or opened when authorized person's presence is detected. A BLE-enabled car key can detect its owner's proximity to the car and automatically open the car. (2) A BLE-enabled body thermometer can send its readings to a smartphone so that a care-giver can monitor a sick person's temperature [41].

Device: body patch, watches, thermometers, smartphones.

Limitations: (1) Very low operating power limits high data transfer rates. (2) The number of connected devices allowed on the BLE network makes it difficult to scale [25]. (c) In addition, the Star topology that BLE uses creates basic security concerns [41].

3.1.5. Zigbee IP

Zigbee provides low-cost, two-way wireless communications at very low-power consumption. It was revised to Zigbee IP, which specifies requirements for developing devices for D2D communications in the IoT environment. Devices can join networks, pair with other devices to operate and interact without a centralized control [24]. A device can function as a Zigbee Coordinator (ZC), Zigbee Router (ZR) or a Zigbee End Device (ZED) [42]. ZC initiates the network formation and controls the network. ZRs relay traffic for ZEDs and may be used to extend the network if required. ZEDs are other devices connected to the Zigbee network and are managed by ZCs and ZRs.

The PHY and MAC layers conform to the specifications of the IEEE 802.15.4-2006 standard. Basically, the link layer allows the discovery of Zigbee networks within some range. The management entity enables a Zigbee device to perform power management, authentication, network access control and security key distribution [42].

IoT application: smart energy, home/building automation, industrial remote controls, health care and retail services.

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

Use case: (1) Patients with Zigbee medical sensors can monitor their heart rate, blood pressure or glucose level to note any anomalies. The data collected is securely transmitted to the data collection unit for the care provider to access [43].

Device: sensors, light switches, thermostats.

Limitations: (1) Inflexible address allocation and naming of automated remote devices that may be communicating [44]. (2) Power efficiency is critical because Zigbee devices are often not connected to power. (3) Zigbee does not allow inter-operability with other non-Zigbee devices over the Internet.

Table 1 Summarizes the open issues related to 6LoWPAN, the effects of these issues on D2D communication in the IoT and some recommended solutions.

List of acronyms in table 1

IPHC	Internet Header Compression
DECT ULE	Digital Enhanced Cordless Telecommunications Ultra Low Energy
BLE	Bluetooth Low Energy
PLC	Power Line Communication
MTU	Maximum Transmission Unit
DLC	Data Link Control
L2CAP	Logical Link Control and Adaptation Protocol

4. Network layer challenges and solutions for D2D communication in the IoT environment

The network layer provides services that enable seamless connectivity between devices. Inter-operation issues and limitations of D2D technologies are associated with network layer services such as addressing, routing, resource optimization, security, QoS and mobility support. However, for D2D communication in the IoT, how to ensure these services remains a challenge for existing network layer protocols. In this section, we present the protocol requirements that should be satisfied to ensure efficient, robust, reliable and scalable IoT services.

4.1. Addressing

Due to the heterogeneity of devices, efficient device identification is necessary for scalable and seamless ubiquitous connectivity in the IoT. However, as the number of devices increases, will it be feasible to have permanent or unique identification for each device? To alleviate the challenge of device identification, addressing scheme for the IoT must support:

4.1.1. Flexible allocation of addresses to devices in the network at any time

Devices should be able to choose an address for communication in any application scenario. Customized addresses do not provide the flexibility required for different application scenarios where devices may be deployed.

4.1.2. Network address duplication detection for multi-interface devices

The uniqueness of network address during communication is paramount in a heterogeneous network environment such as the IoT. Specifically, for D2D communications the ability to flexibly select addresses and detect any address duplication on its interfaces is necessary in some IoT applications [50]. Address duplication detection will allow devices to know if its interfaces have been assigned the same address. Multicast, broadcast and anycast communication addresses should be assigned without causing collision on multi-interface devices. For instance, if a dual-interface device is simultaneously involved in smart grid and home automation, an address duplication detection procedure will be necessary because it will be connected to both of these heterogeneous networks, and will be identified as a single device on each network.

4.1.3. Address recycling

Some identifiable devices (e.g., tags, medicines, books) may require network connectivity for a brief period and eventually leave the network, while other devices may be connected throughout their lifetime.

4.1.4. Automatic self-configuration of network addresses

Some devices may be deployed in remote locations not within human reach. Thus, it is desirable that such devices are capable of performing address self-configuration to eliminate the need for manual configuration [44]. In addition, the auto-configuration capability of network address reduces the time taken for configuring and managing addresses. New devices should be able to obtain addresses quickly as soon as they join the network so that they can start communications promptly.

4.2. Routing

Direct data transmission between devices is challenging in the IoT ecosystem because of its large scale, dynamic and heterogeneous network environment [45]. By exploiting D2D communication, devices may not communicate over the core network but can route data for each other [51]. For this, D2D communication requires new routing strategies that can make use of efficient optimization techniques to tailor the use of network resources as required by different applications in the IoT. The success of IoT depends on the efficient and intelligent use of network resources [52]. Most traditional routing techniques provide strict and unintelligent routing that can waste both network and device resources. The following factors should be considered by routing protocols that operate in the IoT environment.

4.2.1. Multi-copy (MC) routing

Where multiple copies of a data is present within the network at any time. Copies are generated by the custodian and routed independently to different destinations. It is useful for device discovery and route searches. MC routing may also be used for communication. For example, lighting systems may route information to turn a group of light bulbs on or off simultaneously. It is also useful in mobile social networks for minimizing message delivery delay [53].

4.2.2. Uni-directional (UD) routing

Benefits networks where asymmetric connectivity exists. Asymmetric connectivity occurs when the transmission power level or interference level around devices vary. A device may be able to transmit to its neighbor but the neighbor may not be able to transmit back or its transmission may not be received. Asymmetric links are common in D2D communication (e.g., PLC), where transmission ranges and interference levels vary. Thus, UD routing is useful for one-way critical or high-volume transmissions that do not require acknowledgements [54].

4.2.3. Device and network constraints metrics

Constrained resources (e.g., memory, residual energy, sleep intervals, throughput threshold, Received Signal Strength (RSS), Bit Error Rate (BER), and Interference) should be taken into consideration by routing protocols [55]. In particular, as the number of devices increases, the contention for spectrum will increase, so devices need to be able to avoid interference-prone links. Thus, routing protocols must possess cognition for good spectrum conditions to enable reliable connectivity.

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

Table 1
6LoWPAN open issues in relation to D2D communication in the IoT.

6LoWPAN function	The way the function is achieved in D2D silo technology				6LoWPAN open research issues and recommendations
	DECT ULE	BLE	PLC	Zigbee	
Stateless Address Auto-Configuration (SLAAC) **Applicability**: To allow devices to join the network by obtaining addresses by themselves.	64 bit Interface Identifier (IID) is derived from the 48 bit MAC address or DECT device addresses.	64 bit IID is formed using the 48 bit BLE device address (IEEE 802-2001) or a randomly generated Interface Identifier IID.	IID is from 16 bits and 64 bits MAC addressing scheme based on IEEE 802.15.4-2006.	IID is derived from 64 bit and 16 bit MAC level addressing modes.	***Issue:*** Insufficient entropy compared to link lifetime in IID generation. ***Effect:*** Devices are vulnerable to address scanning and exposed to security threats e.g., location tracking, activity correlation analysis, device-identification [45]. ***Recommendation:*** (a) Generation of IID with collision-free cryptographic hashing (b) Randomized IID for transient communication.
Header Compression(HC) **Applicability**: To reduce the overhead associated with the transmission of IPv6 packet.	6LoWPAN HC required, uses LoWPAN IPHC∗ encoding format.	6LoWPAN HC required.	6LoWPAN HC may be required.	6LoWPAN HC required.	***Issue***: Not all header types are supported for compression. ***Effect:*** New encoding specification for every new header to be compressed [46]. ***Recommendation:*** Efficient header compression requires further research [46].
Fragmentation and Reassembly (FAR) **Applicability**: To accommodate the MTU requirements of LoWPANs.	6LoWPAN FAR not required since the DLC procedures supports FAR.	6LoWPAN FAR not required, FAR is provided by BLE L2CAP.	6LoWPAN FAR not recommended.	6LoWPAN FAR is required.	***Issue***: a) lost fragments and duplicate fragments delay processing and occupy memory space thereby blocking new incoming data. b) no way to authenticate received fragments. ***Effect:*** a) Packet delivery probability is reduced. b) Fake and legitimate fragments cannot be distinguished [15],[47]. ***Recommendation***: Fragmentation should be avoided [15] or a fragmentation indicator should be introduced [48].
Multicast address mapping **Applicability**: Allows devices to participate in a wider range of communication with other devices.	No multicast.	Not supported.	Multicast is a set of point-to-point transmissions.	Supports multi-cast.	***Issue***: Maps multicast onto broadcast messages. ***Effect***: Results in broadcast storms, inefficient service discovery and network management, consumes energy and bandwidth. ***Recommendation:*** mapping with multicast destination filtering at link layer is needed.
Neighbor Discovery Optimization (NDO). **Applicability**: Easy reachability of devices over the Internet.	6LoWPAN NDO for Star topology required.	6LoWPAN NDO for Star topology required.	Uses the mechanism described in IEEE Std. 802.15.4-2006.	6LoWPAN NDO is required.	**Issue:** a) Does not consider devices' energy saving modes; it assumes devices are always on or reachable. b) Insecure Neighbor Discovery protocol. **Effect:** a) Poor routing due to sleeping devices. b) Insecure D2D communication. **Recommendation**: sleep-aware/energy-aware schemes. b) Trust-levels as a security metric for connectivity can be used [49].

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

4.2.4. Information/data-pulling by devices

This routing action allows devices to request specific data they require from other devices within the network. If a device needs a certain data, it broadcasts a query message to devices in the region where the data resides and waits for these devices to respond with the data. Properties of the data requested are specified using attribute-based naming and devices have knowledge of the areas where the specific data requested resides [56].

4.3. Mobility

In the IoT environment, mobility of devices is common. Consequently, mobility introduces the challenge of locating mobile devices so as to maintain seamless connectivity with them. Mobility protocols must enable easy reachability of devices within the IoT ecosystem. For D2D devices with multiple network interfaces, support for multi-homing within the IoT is necessary so that such devices can have ubiquitous network access through any network technology within their coverage range [57,58]. Multi-homing can enable load sharing, load balancing and network preference setting for D2D communication devices.

4.4. Security

Encryption for stored and transmitted data is required to ensure privacy and confidentiality of data within the IoT environment. The computational requirement for today's encryption mechanisms poses a significant challenge for resource-constrained devices. In particular, the processing power and battery life limitations of most IoT devices will have a huge impact on their ability to run existing high-end security algorithms [59]. Most of these algorithms use complex security key management and credential exchange schemes. Therefore, lightweight security protocols have to be devised for D2D communication within the IoT [60] environment. Cognitive security protocols are also needed to prevent security breaches and distributed denial of service attacks. Such protocols can authenticate and confirm the integrity of devices and software applications [61].

4.5. Quality of service (QoS)

D2D communication in the IoT will be for different purposes and thus will generate different types of data traffic. IoT traffic may be bursty or continuous in nature (e.g., video or voice). Such traffic may have varying delay, data loss or throughput requirements. Typically, D2D communication for real-time and mission-critical applications (e.g., obtaining a patient's real-time health data) requires QoS guarantees [13, 62]. QoS protocols must facilitate reliable end-to-end connection for such mission critical traffic traversing the IoT environment. In addition, two recommendations that should be considered by QoS protocols for the IoT include:

4.5.1. Multi-dimensional QoS provisioning

Multi-dimensional QoS refers to multiple and varying QoS requested concurrently by multiple entities operating in different domains but within the same system. In a single-service network, individual applications generate traffic, which requires a set of QoS constraints to be satisfied in order to deliver a service efficiently. However, the IoT environment is a multi-service and multi-application network in which diverse applications may have to cooperate to provide a service [63,64]. Each application has its own QoS requirements. Thus, QoS must be supported across multiple dimensions, which means guaranteeing multiple QoS required by multiple applications operating towards a common service simultaneously. Therefore, the process of guaranteeing QoS for some services in the IoT is complex due to the availability of limited network resources [65, 66]. For example, in a health monitoring service, different applications may be integrated to simultaneously provide data as input for detecting a patient's fall. Such aggregated data may be from the heart rate monitor, accelerometer, floor pressure sensor, video cameras and alarm systems and these applications may have dissimilar set of QoS requirements.

4.5.2. Tradeoff between traffic prioritization and fairness

In addition to the huge volume of traffic generated by the IoT environment, such traffic will also exhibit different characteristics [67]. For example, smart meter traffic will be bursty and intermittent while video streaming will generate continuous traffic. Thus QoS protocols need to ensure that traffic from applications that consume a lot of network resources does not dominate traffic with low network resource requirements. It is worth pointing out that traffic from public safety, home medical and health monitoring, and video streaming from real-time surveillance cameras will need to be handled with high priority. However, prioritizing such traffic, should not cause starvation for applications such as smart meter and web browsing [68].

4.6. Resource optimization

Resource optimization is needed for successful IoT deployments. As the number of IoT devices deployed increases and with limited human intervention to fall back on, inefficient and defective devices can waste network resources [51]. A problem that may be caused by such devices is network congestion due to excessive signaling traffic, which can lead to service degradation or outage. The effect of this problem can cascade to other devices thereby affecting the QoS provided by the IoT system. Therefore, resource optimization protocols must apply cognitive intelligent algorithms to learn about devices' conditions and consider such as parameters to be used to adjust network resource allocations accordingly. A benefit of cognitive algorithms is that they are not deterministic and they can evolve overtime to suit any network and device conditions [62].

5. Conclusion and future work

With the rapid increase in the number of Internet-enabled devices, the IoT paradigm is now a reality. Therefore, integrating and inter-operating silo-based D2D networking technologies has become vital. The TCP/IP protocol stack that underpins most networks has a rigid one-size-fits-all structure, which limits its implementation for D2D communication within the IoT. Since devices play a huge role in realizing the IoT, their capabilities are important factors that must be considered in interoperating the D2D network silos. Thus, a practical interoperability framework should be device-centric (i.e., decentralized, gateway-free) rather than network-centric (centralized) because the network is only utilized as a communication pipe [21]. Several gateway-based solutions have been proposed in the past, but the major drawback is that they have to be updated when a new technology or device is developed [24]. For D2D communication in the IoT, a gateway-free interoperability framework will be suitable to enable scalability. For instance, for a home automation scenario, where the number of light bulbs and sensors operating with diverse technologies can increase continuously, a scalable framework will enable a consistent robust D2D communication [25]. In addition, such a framework will allow auto-configuration of new devices. Finally, the interoperability framework must be lightweight, adaptable and cognitive so that emerging paradigms and concepts such as Information Centric Networking (ICN), Software Defined Networking (SDN) and Network Function Virtualization (NFV) can be seamless inte-

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

grated to enable future D2D communication within the IoT ecosystem.

We will use the results of the comprehensive analysis presented in this paper in future experimentation and simulation works to obtain quantitative results on the issues outlined and recommendations proposed in this work.

Acknowledgments

We thank the anonymous reviewers for their valuable feedback and comments which helped us improve the quality and presentation of this paper.

References

[1] IEEE Standards Association "Internet of Things Ecosystem Study" Available: http://standards.ieee.org/innovate/iot/study.html.
[2] J. Apcar, The Internet of Things, powered by IPv6, in: iDA IPv6 Conference[Online], 2014 https://www.ida.gov.sg/~/media/Images/Infocomm%20Landscape/Technology/IPv6/download/JeffApcar.pdf.
[3] S. Sorrell, IoT-Internet of Transformation, in: Juniper Research [Online], 2015 http://www.juniperresearch.com/document-library.
[4] M. Andersson, Short-range Low Power Wireless Devices and Internet of Things (IoT), in: *Wireless Congress* 2013: *Systems & Applications*, Munich, Germany, 2013.
[5] O. Bello, S. Zeadally, Communication issues in the Internet of Things, Next Generation Wireless Technologies: 4 G and Beyond, Springer, London, 2013, pp. 189–219.
[6] , Vision and Challenges for Realising the Internet of Things, in: H. Sundmaeker, P. Guillemin, P. Friess, S. Woelfflé (Eds.), Vision and Challenges for Realising the Internet of Things, Cluster of the European Research Projects on the Internet of Things, 2010 ISBN 9789279150883.
[7] G. Reiter, Wireless connectivity for the Internet of Things, One Size Does Not Fit All, Texas Instruments [Online], 2014 Available: http://www.ti.com/lit/wp/swry010.
[8] J. Chase, The Evolution of the Internet of Things, Texas Instruments. [Online], 2013 Available: http://www.ti.com/lit/ml/swrb028.
[9] S. Zeadally, S. Khan, N. Chilamkurti, Energy-efficient networking: past, present, and future, J. Supercomput. 62 (3) (2012).
[10] M.R Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L.A. Grieco, G. Boggia, M. Dohler, Standardized protocol stack for the Internet of (Important) Things, *Commun. Surv. Tut. IEEE*, Third Quart. 15 (3) (2013) 1389–1406.
[11] Á.L.V. Caraguay, A.B. Peral, L.I.B. López, L.J.G. Villalba, SDN: evolution and opportunities in the development IoT applications, Int. J. Distrib. Sensor Netw. [online] 2014 (2014) Article ID 735142.
[12] C. Legare, Reworking the TCP/IP stack for use on embedded IoT devices, in: Presented at Embedded Systems Conference [Online], 2014 http://www.eetindia.co.in.
[13] O. Mazhelis, M. Waldburger, G.S. Machado, B. Stiller, P. Tyrväinen, in: Extending Monitoring and Accounting Infrastructure Towards Constrained Devices in Internet-of-Things Applications, University of Zurich, 2013 [online] Technical Report, Available: https://www.merlin.uzh.ch/contributionDocument/download/5076.
[14] P. Francesca, B. Donato, B. Lorenzo, B. Andrea, T.M. Santina, M.N. Blefari, On the IP support in IEEE 802.15.4 LR-WPANs: self-configuring solutions for real application scenarios, in: *Proc. 9th IFIP Annual Med-Hoc-Net*, France, June 23–25, 2010, pp. 1–10.
[15] J. Pope, R. Simon, The impact of packet fragmentation and reassembly in resource constrained wireless networks, *J. Comput. Inf. Technol.* [Online], CIT 21 (2) (2013) 97–107 Available: http://cit.srce.unizg.hr/index.php/CIT/article/view/2195.
[16] N. Kang, J. Park, H. Kwon, S. Jung,). ESSE: efficient secure session establishment for internet-integrated wireless sensor networks, *Int. J. Distrib. Sensor Netw.* [Online] (2015).
[17] C. Bormann, M. Ersue, A. Keranen, Terminology for Constrained-Node Networks RFC7228, ISSN 2070–1721, 2014.
[18] Wireless Medium Access Control (MAC) and Physical Layer (PHY), Specifications for Low-Rate Wireless Personal Area Networks (LR-WPANs) IEEE 802.15.4-2006, 2006.
[19] E. Kim, D. Kaspar, J.P. Vasseur, Design and Application Spaces for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs) RFC6568, ISSN: 2070–1721, 2012.
[20] N. Venkatesh, Ensuring coexistence of IoT wireless protocol: using a convergence module to avoid contention, Accelerating the Internet of Things, 12th ed., Embedded Innovator, 2015, pp. 32–35. Available: intel.com/embedded-innovator.
[21] R. Cepeda, "The IoT Generation will need 5G"Available: www.interdigital.com/post/5g-and-iot–two-sides-of-the-same-coin .
[22] M. Serrano, P. Barnaghi, F. Carrez, P. Cousin, O. Vermesan, P. Friess, Internet of Things: IoT Semantic Interoperability:Research Challenges, Best Practices, Recommendations and Next Steps, European Research Cluster on The Internet of Things, 2015.
[23] M. Jung, J. Weidinger, C. Reinisch, W. Kastner, C. Crettaz, Y. Bocchi, O. Crettol, A transparent IPv6 multi-protocol gateway to integrate building automation systems in the Internet of Things, in: Proc. of the IEEE International Conference on Internet of Things, Besancon, France, 2012.
[24] S. Ashton, Zigbee's new IP specification for IPv6 6LoPAN wireless network designs, Silicon Labs [Online], 2013 Available: http://www.embedded.com/print/4419558.
[25] Silicon labs, "Bringing the IoT to Life," Available: www.silabs.com/pages/Silabs-Search.aspx? q=bringing the IoT to life.
[26] J.W. Hui, D.E. Culler, IPv6 in low-power wireless networks, in: Proc of the IEEE, 98, 2010, pp. 1865–1878.
[27] P. Mariager, J. Petersen, Z. Shelby, M. van de Logt, D. Barthel, Transmission of IPv6 Packets over DECT Ultra Low Energy, IETF Internet Draft (2015) (Status: Informational), draft-ietf-6lo-dect-ule-03.txt.
[28] ETSI EN 300 175-5, Digital Enhanced Cordless Telecommunications (DECT); Common Interface (CI); Part 5: Network (NWK) layer, 2015 Version 2.6.1 Available: https://portal.etsi.org.
[29] P1901.2a/D0.3, in: IEEE Approved Draft Standard for Low-Frequency (less than 500 kHz) Narrowband Power Line Communications for Smart Grid Applications - Amendment 1, 2015.
[30] Breaking Down Silos, in: The Value Of A Standards-Based Approach To Smart Metering And Smart Grid, 2013 Available: www.cisco.com or www.itron.com.
[31] D. Popa, J. Hui, 6LoPLC: Transmission of IPv6 Packets over IEEE 1901.2 Narrowband Powerline Communication Networks, IETF Internet Draft (2014) (Status: Informational), draft-popa-6lo-6loplc-ipv6-over-ieee19012-networks-00.txt..
[32] P. Pereira, "Building an Interoperable Grid with Industry Standard IPv6 Architecture, in: CIGRE Colloquium, India, 2013.
[33] Q. Sheng, S. Zeadally, Z. Luo, J. Chung, Z. Maamar, Ubiquitous RFID: where are we? Int. J. Inf. Syst. Front. 12 (5) (2010).
[34] Q. Sheng, X. Li, S. Zeadally, Enabling next-generation RFID applications: solutions and challenges, IEEE Computer 41 (9) (2008).
[35] Y. Wu, Q. Sheng, H. Shen, S. Zeadally, Modeling object flows from distributed and federated rfid data streams for efficient tracking and tracing, IEEE Trans. Parallel Distrib. Syst. 24 (10) (2013).
[36] L.F. Rahman, M.B.I. Reaz, M.A.A. Ali, M. Marufuzzaman, M.R. Alam, Beyond the WiFi: introducing RFID system using IPv6, in: Proc. Kaleidoscope: Beyond the Internet? Innovations for Future Networks and Services, ITU-T, Pune, 2010, pp. 1–4.
[37] Bluetooth Specification Version 4.1, Vol 0, 03 December 2013.
[38] T. Savolainen, Bluetooth 4.0 update to 4.1 and what it means for IPv6 over bluetooth low-energy, in: Presentation at IETF 6lo WG meeting at IETF, 89, 2014 draft-ietf-6lo-btle-00.
[39] J. Nieminen, T. Savolainen, M. Isomaki, B. Patil, Z. Shelby, C. Gomez, Transmission of IPv6 Packets over BLUETOOTH(R) Low Energy, IETF Internet Draft (2014) (Status: Informational), draft-ietf-6lo-btle-02.
[40] N. Thomas, S. Thomson, T. Jinmei, IPv6 Stateless Address Auto Configuration RFC 4862, 2007.
[41] Bluetooth® Low Energy, Litepoint [Online], Available: www.litepoint.com/whitepaper/Bluetooth%20Low%20Energy_WhitePaper.pdf.
[42] Zigbee IP specification, 12-0572-10, ZigBee Alliance Available:, 2013 www.zigbee.org/Specifications/ZigBeeIP/Download.aspx.
[43] , ZigBee Wireless Sensor Applications for Health, Wellness and Fitness, Zigbee Alliance, 2009 Available: www.zigbee.org.
[44] L.H. Yen, W.T. Tsai, Flexible address configurations for tree-based ZigBee/IEEE 802.15.4 wireless networks, in: Proc. 22nd International Conference on Advanced Information Networking and Applications, Okinawa, Japan, 2008, pp. 395–402.
[45] D. Thaler, 6LoWPAN Privacy Considerations, IEFT Internet-Draft (2015) (Status: Informational), draft-thaler-6lo-privacy-considerations-00.txt.
[46] C. Bormann, 6LoWPAN Generic Compression of Headers and Header–like Payloads, IETF Internet-Draft (2014) (Status: Standards Track), draft-i-etf-6lo-ghc-01.txt.
[47] R. Hummen, J. Hiller, H. Wirtz, M. Henze, H. Shafagh, K. Wehrle, 6LoWPAN Fragmentation Attacks and Mitigation Mechanisms, in: Proc. of the sixth ACM conference on Security and privacy in wireless and mobile networks, New York, NY, USA, 2013, pp. 55–66.
[48] C. Bormann, Adaptation Layer Fragmentation Indication, IEFT Internet-Draft (2013) (Status: Standards Track), draft-bormann-intarea-alfi-04. txt.
[49] S.K Das, K. Kant, N. Zhang, Handbook on Securing Cyber-Physical Critical Infrastructure, Elsevier, 2012.
[50] O. Bello and S. Zeadally, "Intelligent Device-to-Device communication in the Internet of Things (IoT)", to appear in IEEE Systems Journal, 2016.
[51] S.M.A Oteafy, F.M. Al-Turjman, H.S. Hassanein, Pruned adaptive routing in the heterogeneous Internet of Things, in: Proc IEEE GLOBECOM, 2012, pp. 214–219.
[52] GSM Association, IoT Device Connection Efficiency Common Test Cases CLP.09, Version 2.0, 01, 2015.
[53] J. Wu, M. Xiao, L. Huang, Homing spread: community home-based multi-copy routing in mobile social networks, in: Proc. IEEE INFOCOM, 2013, pp. 2319–2327.
[54] D. Minoli, Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications, Wiley publications, 2013.
[55] Cisco IOS Software Configuration Guide, Release 12.2SX, Cisco Systems.
[56] O. Younis, S. Fahmy, Constraint-Based Routing in the internet: basic principles and recent research, IEEE Commun. Surv. Tut. 5 (3) (2003) 2–13.

[57] E. Baccelli, C. Mehlis, O. Hahm, Information centric networking in the IoT: experiments with NDN in the wild, in: Proc. 1st Int. Conf. on ICN, New York, USA, 2014, pp. 77–86.
[58] L. Bokor, A. Huszak, G. Jeney, Novel results on SCTP multihoming performance in native IPv6 UMTS and WLAN environments, Int. J. Commun. Netw. Distrib. Syst. 5 (1/2) (2010) 25–45.
[59] F. Siddiqui, S. Zeadally, SCTP multihoming support for handoffs across heterogeneous networks, in: Proc. 4th Annual Communication Networks and Services Research Conference, 2006, pp. 8–16.
[60] A.J. Jara, L. Ladid, A. Skarmeta, The Internet of Everything through IPv6: an analysis of challenges, solutions and opportunities, J. Wireless Mob. Netw. Ubiquit. Comput. Dependable Appl. 4 (3) (2013) 97–118.
[61] T. Heer, O. Garcia-Morchon, R. Hummen, S.L. Keoh, S.S. Kumar, K. Wehrle, Security challenges in the IP-based Internet of Things, J. Wireless Personal Comm. 61 (3) (2011) 527–542.
[62] R. Muraleedharan, L.A. Osadciw, Increasing QoS and security in 4G networks using cognitive intelligence, in: Proc. IEEE Globecom Workshops, 2007, pp. 1–6.
[63] J. Gubbi, R. Buyya, S. Marusic, M. Palaniswami, Internet of Things (IoT): a vision, architectural elements, and future directions, Future Gener. Comput. Syst. 29 (7) (2013) 1645–1660.
[64] M.-A. Nef, L. Perlepes, S. Karagiorgou, G.I. Stamoulis, P.K. Kikiras, Enabling QoS in the Internet of Things, in: Proc. Fifth International Conference on Communication Theory, Reliability, and Quality of Service, Chamonix/Mont Blanc, France, 2012, pp. 33–38.
[65] N.X. Liu, J.S. Baras, Modelling multi-dimensional QoS: some fundamental constraints, Int. J. Commun. Syst. 17 (3) (2004) 193–215.
[66] L. Li, M. Rong, G. Zhang, "An Internet of things QoS estimate approach based on multi-dimension QoS, in: Proc. *9th International Conference on Computer Science & Education (ICCSE)*, Vancouver, BC, 2014, pp. 998–1002.
[67] N. Sanadi, “Understanding W2CM: How an FPGA-based blade answers the call for next-generation user-plane testing”. [Online]. Available: http://www.exfo.com/solutions/bu1-simulation-load-testing/policy-charging-control.
[68] J. Algar, “Cisco: Video, Internet-of-Things, mobile are prime drivers of Internet use”. [Online]. Available: http://www.techtimes.com/articles/8271/20140611/cisco-video-mobile-big-internet-use.htm.

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010

Oladayo Bello holds a B.Sc in Electronics and Electrical Engineering. She received a B.Sc (Hons) in Industrial and Systems Engineering from the University of Pretoria, M.Sc in Electrical Engineering and a PhD in Electrical Engineering from the University of Cape Town, South Africa. Her research interests include communication in the Internet of Things, interworking multi-hop wireless networks, and resource allocation in wireless networks She has authored several peer-reviewed international journals, conference papers, and newsletter articles. Oladayo actively serves as a reviewer for international journals and technical program committee member for international conferences.

Sherali Zeadally received the bachelor's degree in computer science from the University of Cambridge, U.K., and the doctoral degree in computer science from the University of Buckingham, U.K. He is an Associate Professor with the College of Communication and Information, University of Kentucky, Lexington, KY, USA. He is a fellow of the British Computer Society and the Institution of Engineering Technology, U.K.

Mohammad Badra is an Associate Professor at Zayed University, Abu Dhabi, UAE. He received a PhD degree in networks and computer science from TLECOM Paris TECH. His research interests include key exchange, wireless network security, public key infrastructures, smart cards, and wireless sensors networks. He is the author of several international standards on security exchange and the co-author of many international conference and journal papers.

Please cite this article as: O. Bello et al., Network layer inter-operation of Device-to-Device communication technologies in Internet of Things (IoT), Ad Hoc Networks (2016), http://dx.doi.org/10.1016/j.adhoc.2016.06.010