Enabling Distributed Intelligence in the Internet of Things using the IOTA Tangle Architecture

Tariq Alsboui, Yongrui Qin and Richard Hill
School of Computing and Engineering, University of Huddersfield, U.K.

Keywords: Internet of Things, Distributed Intelligence, IOTA, Mobile Agent.

Abstract: It is estimated that there will be approximately 26 to 30 billion Internet of Things (IoT) devices connected to the Internet by 2020. This presents research challenges in areas such as data processing, infrastructure scalability, and privacy. Several studies have demonstrated the benefits of using distributed intelligence to overcome these challenges. This article reviews existing state-of-the-art distributed intelligence approaches in IoT and focuses on the motivations and challenges for distributed intelligence in IoT. We propose a potential solution based on IOTA (Tangle), a platform that enables highly scalable transaction-based data exchange amongst large quantities of smart things in a peer-to-peer manner, together with mobile agents to support distributed intelligence. Challenges and future research directions are also discussed.

1 INTRODUCTION

The Internet of Things (IoT) is a mature field of research that was brought to attention by Auto-ID centre, when they used Electronic Product Code (EBC) along with Radio Frequency Identification (RFID) to automatically identify the and track the itinerary of items in supply chain (Ashton, 2009). IoT is considered as a novel paradigm that connects physical objects to the Internet. The basic idea behind it is to connect physical objects to the virtual world and allow them to sense and modify the environment by using sensors and actuators (Atzori et al., 2010). Connecting the physical world to the Internet plays a crucial role in enhancing our lives by turning cities into smart cities (Perera et al., 2017), homes into smart homes (Doan et al., 2018), and campuses into smart campuses (Angelis et al., 2015). According to several research reports, it is estimated that there will be approximately 26 to 30 billion devices connected to the Internet in 2020 (Gartner, 2013; Research, 2013). Consequently, this in turn brings many challenges in a number of areas, such as data processing, saving resources, and scalability (Esposito et al., 2017).

One of the key technologies being explored for overcoming many of the challenges associated with the growing number of connected IoT devices is distributed intelligence (Byers and Wetterwald, 2015). Distributed intelligence is defined as a system of entities e.g., smart sensors, working together to reason, plan, and solve problems (Lynne, 2007). The main aim of such technology is to enable entities (smart objects) in an IoT system to cooperate at optimal efficiency to achieve desired goals.

In the context of IoT, according to (Van den Abeele et al., 2015), distributed intelligence is defined as *Cooperation between devices, intermediate communication infrastructures (local networks, access networks, global networks) and or cloud systems in order to optimally support IoT communication and IoT applications*. As stated in (Van den Abeele et al., 2015) in order to enable distributed intelligence, communication and computation capability should be placed at the right place.

Based on the above definition, this paper presents a new scalable, and energy efficient distributed intelligence approach for IoT. We propose the utilization of IOTA Tangle architecture (Serguei, 2017) and Mobile Agent (Leppänen et al., 2014) to enable distributed intelligence. IOTA is an emerging platform that is particularly designed for the Internet of Things to overcome the problems of scalability, transaction fees, and mining of the blockchain technology. The main component of IOTA is the Tangle, which is based on the concept of a Directed Acyclic Graph (DAG)(Serguei, 2017). The IOTA platform provides a potential and highly scalable solution to enable distributed intelligence. The mobile agent technology can provide cooperation and information sharing among different types of nodes (Leppänen et al.,

Alsboui, T., Qin, Y. and Hill, R.
Enabling Distributed Intelligence in the Internet of Things using the IOTA Tangle Architecture.
DOI: 10.5220/0007751403920398
In *Proceedings of the 4th International Conference on Internet of Things, Big Data and Security (IoTBDS 2019)*, pages 392-398
ISBN: 978-989-758-369-8

2014). A description about the architecture is presented in Section 4.

The remainder of this paper is structured as follows: Section 2 identifies the motivation and challenges behind the need for distributed intelligence in IoT. Section 3 presents an overview of the recent distributed intelligence approaches in IoT. In Section 4 a summary on future research direction is discussed. Finally, Section 5 concludes the paper.

2 MOTIVATIONS AND CHALLENGES

In this section, we present the need for distributed intelligence in the Internet of things (IoT) by enlisting some of the key factors that dictate the challenges in IoT related research. We then briefly describe how IOTA platform can be utilized to realize distributed intelligence.

2.1 Saving Resources

It is generally expected that IoT would produce a massive amount of data, which when sent to a central location results in larger consumption of network resources. IoT consists of nodes that has limited resources such as power consumption (battery limits), computational capability and maximum memory storage, which makes distributed intelligence a challenging task. IOTA Qubic protocol (Foundation, 2016b) saves resources by outsourcing intensive computations to an external more powerful nodes. This is can be achieved through *Qubic-enabled IOTA nodes (Q. Nodes)*. Qubics are inserted as messages in IOTA transactions. It consists of instructions, called metadata responsible for deciding how and when to process data.

2.2 Scalability

Scalability refers to the ability of the network to deal with the growing amount of work needed when the network grows. It can be divided into two parts: Horizontal scaling and Vertical scaling. In Horizontal scaling, the network is expected to grow by adding more nodes to it. On the other hand, Vertical Scaling is to equip the existing devices in the network by adding more (CPU, RAM, power) (Bondi, 2000). IoT is constantly changing and developing to fit in environmentally in order to deal constantly with enlarging demands and in accordance with the predictions provided in (Gartner, 2013; Research, 2013). Hence, potential solutions should be highly scalable to deal with billions of smart objects, which will be soon connected to the Internet.*IOTA Tangle* (Serguei, 2017) can provide a valuable solution to accommodate the fast growth of interconnected things. IOTA Tangle scales well when the number of Tangle nodes increases.

2.3 Privacy

Privacy refers to the capability of a system to keep information/data private, e.g, to make sure that if anyone has accessed the data will be unable to make sense of it. Moreover. Information leakage is generally the ultimate user concern, especially relating to sensitive data, such as location, and movement trajectory information. Potential solutions should identify in what form the data should be, and who can get access to it. Consequently, the *IOTA Masked Authenticated Messaging (MAM) protocol* (Foundation, 2016a) can be utilized for achieving privacy. An example where privacy is of concern for users is in health care applications where information about patients is sensitive.

2.4 Offline Capability

Offline Capability is also known as resiliency and is often defined as the capability of the system, to work in emergency cases, such as Internet connection not reachable. This indicates that if the internet connection goes down, the system will not function. Therefore, there is no need for a network to be connected to the Internet all the time. IOTA tasks can be done on an offline network. IOTA Tangle offers this capability, but the transactions have to be re-attached to the main tangle if further processing is needed. In such a manner, distributed intelligence and processing is desirable and well supported.

3 EXISTING DISTRIBUTED INTELLIGENCE APPROACHES IN IoT

Over the last few years, distributed intelligence has started to gain attention from many researchers in the field of IoT (Van den Abeele et al., 2015; Byers and Wetterwald, 2015; Sahni et al., 2017; Rahman and Rahmani, 2018). Most of these research efforts are to deal with problems relating to data processing, data management, scalability, and privacy. Recently, the authors in (Van den Abeele et al., 2015) introduced the concept of Sensor Function Virtualization (SFV) as a potential technique to support dis-

Table 1: Comparison Among Distributed Intelligence Approaches in IoT.

Distributed Intelligence Approaches	Saving Resources	Scalability	Privacy	Offline Capability
(Van den Abeele et al., 2015)	High	High	Low	High
(Byers and Wetterwald, 2015)	High	High	Low	Low
(Sahni et al., 2017)	High	High	Medium	Medium
(Rahman and Rahmani, 2018)	High	Low	Low	Low

tributed intelligence in IoT. The basic idea is to enable distributed processing of certain functionalities by offloading them from constrained devices to unconstrained infrastructure such as a virtualized gateway, the cloud and other in-network infrastructure. SFV focuses on the three main points including, scalability, heterogeneity of the IoT, and transparency. To achieve scalability, the approach relies on cloud infrastructure by allowing part of SFV functionalities to run on the cloud benefiting from the elasticity provided by the cloud, and tired design. this handles the increased load, when devices are joining the network. The second point is related to heterogeneity of IoT in terms of resources constraints devices, i.e., limited power, limited processing, infrastructure and it should shift the user from the low level details of the devices. The final point is related to transparency in which any virtual functions that are added to the devices must build on top of existing communication interfaces and that changes to protocols running on end devices must be minimal and preferably non-existent. The advantages of their approach are reduction in energy consumption, scalability, flexibility, and transparency. However, security and privacy issues are briefly acknowledged in their approach. Moreover, implementation and evaluation of the proposed approach is not provided in which they outline as part of their future work.

The work by (Byers and Wetterwald, 2015) presents fog computing architecture as a solution to enable distributed intelligence in IoT. The proposed approach described fog nodes in terms of hardware architecture as well as software architecture. From a hardware point of view, fog nodes can be implemented as ancillary functions on traditional network elements such as gateways, edge devices, and appliances or as stand-alone fog boxes. From a software point of view, fog nodes are highly virtualized machines with multiple VMs running under a highly capable hypervisor. The benefits of using fog nodes are to enhance reliability, bandwidth, and security. However, fog computing still has issues regarding security, privacy (Esposito et al., 2017; Yi et al., 2015; Gillam et al., 2018). In addition to that, implementation and evaluation of the proposed approach is not provided.

More recently, a new computing paradigm, called Edge Mesh that aims to enable distributed intelligence in IoT is proposed in (Sahni et al., 2017). The proposed paradigm distributes the decision-making tasks among edge devices within the network rather than transferring all the data to a centralized server for further processing. In Edge Mesh, all the computation tasks and data are shared using a mesh network of edge devices and routers. Edge Mesh architecture consists of four main types of devices. First, end devices are mainly used for sensing and actuating. Second, edge devices are used for processing and connecting with end devices. Third, routers are used for transferring data among edge devices. Finally, cloud is used to perform big data analytics on historical data. The advantages of edge mesh are, distributed processing, low latency, fault tolerance, better scalability, better security, and privacy. However, they have component for achieving security and privacy, but how privacy can be achieved is not considered. Furthermore, implementation and evaluation is not provided.

Different from the above, the work presented in (Rahman and Rahmani, 2018) proposed an AI based distributed intelligence assisted approach named as Future Internet of Things Controller (FITC). The proposed approach uses both edge and cloud based to distribute intelligence. In particular, edge controller is used to provide low-level intelligence and cloud based controller to provide high-level intelligence, which they refer to as distributed intelligence. The benefits of their work are to reduce response time and loosen the requirements for rules. However, the approach lack of a mechanisms that enables privacy, and offline capability.

Table 1 provides a comparison of the reviewed distributed intelligence approaches according to the challenges provided in Section 2. Overall there are many pieces of solutions to enable distributed intelligence in IoT. We compare the approaches and ranked as *High, Medium, and Low* based on potentiality of tackling the identified technical challenges. A field in the table is given a rank of *High* if the approach satisfies the challenge corresponding to that column. The approach is ranked with *Medium* if it supports the challenge, but not providing a way of how to achieve it. *Low* is given to the approach if it does not address

the challenge at all.

3.1 Limitations of Prior Work

From the above we can see that most of the existing approaches to enabling distributed intelligence in IoT suffer from inherent problems. Firstly, they rely on centralized architecture for processing data (Gillam et al., 2018), which introduces a high cost and delay that is not acceptable for distributed applications. Such examples include health monitoring, emergency response, autonomous driving, and so on. In addition to that, it would consume much network bandwidth (Perera et al., 2017). Besides, solutions based on fog computing still have issues regarding security and privacy (Esposito et al., 2017). Moreover, there is a need for a standardized way for describing the data generated by IoT, such as the one promised by IOTA Identity of Things (IDoT) (Foundation, 2016a), which will also help secure the network. Another problem is the lack of a mechanism to describe in what form the data should be, and who can get access to it (multi-party authentication scenarios), all of which are related to privacy. Finally, only a few of the approaches facilitate an implementation and evaluation of their proposed approach.

4 A NOVEL ENABLING APPROACH FOR DISTRIBUTED INTELLIGENCE IN IoT

The problems and limitations presented above lead to future research opportunities. Possible solutions for enabling distributed intelligence in IoT can be achieved through the use of the IOTA platform (Serguei, 2017) and mobile agent technology (Leppänen et al., 2014).

4.1 Fundamental Tools and Techniques

IOTA (a.k.a. distributed ledger (Serguei, 2017)) is an emerging platform that is particularly designed for the internet of things to overcome the problems of scalability, transaction fees, and mining, which is considered as a resource extensive task that other cryptocurrency lacks by utilizing the blockchain technology (Nakamoto et al., 2008). The main component of IOTA is the *Tangle*, which is based on the concept of a Directed Acyclic Graph (DAG) (Serguei, 2017).

Tangle is the protocol, or the data structure used in IOTA in order to store the transactions, which has collection of nodes (also called as Sites or Vertices) and arrows (also called as Edges). All the vertices or sites which hold data (transactions) are connected to one another using edges, and these edges are used to validate the transaction and to check whether it is valid transaction, in order to achieve approval or confirmation of the transaction eventually. Edges can range from a minimum of two to a maximum of many and are called as Parent. If there is a site with less than two edges, it represents that the actions are unconfirmed, and these are called as Tips of the tangle. Genesis is the unique site or the very first site which do not have any previous site or parents (Serguei, 2017). The Tangle architecture through several nodes *QubicNodes, Full Nodes, Light Node, and Masked Authentication Messaging*. As discussed in Section 2 will be utilized to achieve distributed intelligence in IoT.

Table 2: Node Types in IOTA Network.

Node Type	Storage	Validation
Full Node	Full Tangle last Snapshot	Yes
Light Node	None	No
PermaNode	Full Tangle Permanently	Yes

Table 2 Describes the features of the participant's nodes of IOTA network. the following paragraphs describes each participants node in the network

The concept of IOTA Full Node (Foundation, 2016a), which can be defined as node within the tangle architecture that is capable of finding neighbours and communicate with them, attaching data to the tangle, bundling and signing, tip selection, validation, PoW, and attaching data to the tangle. IOTA full nodes have high computational capacity and are responsible for doing the PoW on behalf of the end nodes taking into consideration that end nodes have limited resources.

The concept of Light Node (Foundation, 2016a) that participates in the network and can be defined as a node within the tangle architecture that relies on the full node to interact with the Tangle; it distinguishes itself from other nodes in the sense that it does not store a copy of the tangle, and does not either validate transactions or communicate with neighbors. It has been specifically designed as a lightweight node for resource constrained nodes.

The concept of Qubic protocol (Foundation, 2016b), which is under development and is defined as a protocol that describes IOTA's solution for quorum-based computations. Qubic focuses on three types of computations including: oracle machines, outsource computations, and smart contracts. We are mainly concerned with the outsourcing part to save resources of IoT devices. Qubic is optimized for IoT and makes it possible to offload computations function-

alities from nodes with battery-limits to an external more powerful nodes, which in turns reduces energy consumption. Qubic are inserted as messages in IOTA transactions. It consists of instructions, called metadata responsible for deciding how and when to process them.

The concept of Permanodes (Foundation, 2016a), which is under development and is defined as node within the IOTA tangle architecture that has features including: finding a neighbouring nodes and communicate with them, attaching data to the tangle, tip selection, and do the Proof-of-Work (PoW). The PoW is a short computational operation compared to mining in blockchain. Furthermore, these nodes are distinguishable from other nodes by having the capability of storing the whole tangle data permanently. This is beneficial for some of the IoT applications in which access to the full data history is required.

In order to ensure privacy, IOTA developed a protocol called Masked Authenticating Messaging (MAM) (Handy, 2017). In the tangle, each transaction carries a message, which allows these messages to be exchanged between the nodes. This indicates that anyone can view the messages in the network. MAM utilizes the Merkle tree based signature scheme and enables privacy by encrypting data. Encryption occurs through three techniques including: private mode, public mode, restricted mode, thereby enabling privacy.

The mobile agent (MA) technology can provide cooperation and information sharing among different types of nodes (Leppänen et al., 2014). Mobile agent is defined as a piece of software that performs data processing autonomously while moving from node to node in the network (Alsboui et al., 2017). The agent can collect local data and perform any necessary data aggregation. Mobile agents can make decision autonomously without user input. They provide flexibility in terms of decision making, and reliability in terms of node failure. (Lange and Oshima, 1999) listed seven good reasons for using MA such as, reducing network load, they adapt dynamically, and They execute asynchronously and autonomously.

4.2 A New Enabling Approach

Based on the above tools and techniques, we propose an approach that enables distributed intelligence in IoT while taken into consideration the challenges identified in Section 2.

As the number of the Internet of Things nodes are expected to reach 30 billion devices in 2020, any proposed solution should be highly scalable, and energy efficient to deal with billions of smart objects that will be connected to the internet. Aiming at this, two important points are to be noted. Firstly, by offloading functionality using IOTA Qubic from resource constraints nodes i.e., battery limit to a more powerful unconstrained infrastructure, we expect our solution to take advantage of the mechanisms provided by these environments to save resources i.e., power consumption, and storage. Secondly, towards a scalable approach, IOTA scales well when the number of nodes are added. This requires only the verification of two previous transactions by signing nodes with a private keys, apply tip selection using Random Walk Montecarlo Algorithm (RWMC), and Proof-of-Work (PoW) to solve the cryptographic puzzle. If the PoW is heavy on nodes with limited processing, the PoW can be directed to the IOTA full node.

Another final impotent point is to ensure privacy by employing Masked Authenticated Messaging (MAM). MAM is offered by IOTA as an extension module, which acts as a second layer data communication protocol to encrypt or mask data. This means that IoT edge nodes running the MAM client are able of transmitting encrypted sensor data by using this communication protocol. This fulfills a crucial need in IoT applications, i.e., health care in which access and privacy meet.

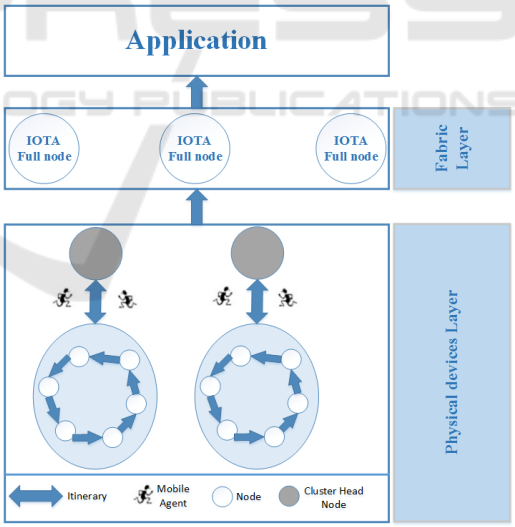

Figure 1: A New Distributed Intelligence Approach for IoT.

Having in mind the requirements of the previous paragraphs, our proposed approach is presented in Figure 1. Our approach consists of three layers. In the first layer, which comprises end nodes running an IOTA light client and will act as an end points to the IOTA network. Since there will be no interactions among nodes in the network running IOTA light clients, we employ MA to facilitate cooperation among nodes in

the network and by cooperation we mean data sharing. To do so, MA will carry transactions that contains the data and aggregate the data. Furthermore, by dispatching MA, we reduce the amount of sensory data by eliminating redundancy. For example, nodes that are placed in proximity of each other are likely to generate redundant data. Ultimately, data aggregation is required to reduce the data traffic in the network.

Second Layer, comprise of a less unconstrained devices running the IOTA full Node. Finally, the application layer utilize from the proposed approach in terms of energy efficiency, scalability, and privacy. To this end, a number of questions should be tackled in the future: How is data offloaded? What kind of primitive mode will be used? How is the PoW outsourced to IOTA full Node? How MA will be routed between nodes in an energy efficient manner?

5 CONCLUSIONS

IOTA Tangle architecture has the potential of enabling distributed intelligence in IoT, which will be beneficial for a wide-range of applications, such as smart cities, and healthcare. IOTA Tangle allows for distributed computation, making it suitable for enabling distributed intelligence in IoT. In this article, we have discussed the need for distributed intelligence in IoT as well as how the IOTA platform can be utilized to enable it. We have presented a review of the recent state of the art distributed intelligence approaches in IoT. Also, we have discovered that there is a need for a a lightweight solution for enabling distributed intelligence based on the identified limitations of existing approaches. We have discussed the challenges as well as future research directions in developing a new distributed intelligence approach and we believe that the integration of IOTA and mobile agent would solve the problems. Finally, we outline pathways to solutions to the problems identified and envision that an IOTA Tangle architecture will facilitate distributed intelligence in IoT.

In the authors opinion, MA migrates between nodes in the network and facilitates cooperation between them. This leads to several advantages, such as reduction in the network load by moving MA carrying data instead of sending data to a central location for further processing, and overcomes network latency.

REFERENCES

Alsboui, T., Alrifaee, M., Etaywi, R., and Jawad, M. A. (2017). Mobile agent itinerary planning approaches in wireless sensor networks- state of the art and current challenges. In Maglaras, L. A., Janicke, H., and Jones, K., editors, *Industrial Networks and Intelligent Systems*, pages 143–153, Cham. Springer International Publishing.

Angelis, E. D., Ciribini, A., Tagliabue, L., and Paneroni, M. (2015). The brescia smart campus demonstrator. renovation toward a zero energy classroom building. *Procedia Engineering*, 118:735–743.

Ashton, K. (2009). That 'Internet of Things' Thing. *RFID Journal*.

Atzori, L., Iera, A., and Morabito, G. (2010). The internet of things: A survey. *Computer Networks*, 54(15):2787–2805.

Bondi, A. B. (2000). Characteristics of scalability and their impact on performance. In *Workshop on Software and Performance*, pages 195–203.

Byers, C. C. and Wetterwald, P. (2015). Fog computing distributing data and intelligence for resiliency and scale necessary for iot: The internet of things (ubiquity symposium). *Ubiquity*, 2015(November):4:1–4:12.

Doan, T. T., Safavi-Naini, R., Li, S., Avizheh, S., K., M. V., and Fong, P. W. L. (2018). Towards a resilient smart home. In *Proceedings of the 2018 Workshop on IoT Security and Privacy*, IoT S&P '18, pages 15–21, New York, NY, USA. ACM.

Esposito, C., Castiglione, A., Pop, F., and Choo, K. R. (2017). Challenges of connecting edge and cloud computing: A security and forensic perspective. *IEEE Cloud Computing*, 4(2):13–17.

Foundation, I. (2016a). Iota development roadmap. (1). (visited on 2-01-2019).

Foundation, I. (2016b). The qubic protocol. (1). (visited on 2-1-2019).

Gartner (2013). Gartner says the internet of things installed base will grow to 26 billion units by 2020. (1).

Gillam, L., Katsaros, K., Dianati, M., and Mouzakitis, A. (2018). Exploring edges for connected and autonomous driving. In *IEEE INFOCOM 2018 - IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pages 148–153.

Handy, P. (2017). Introducing masked authenticated messaging. (1). (visited on 6-01-2019).

Lange, D. B. and Oshima, M. (1999). Seven good reasons for mobile agents. *Commun. ACM*, 42(3):88–89.

Leppänen, T., Riekki, J., Liu, M., Harjula, E., and Ojala, T. (2014). *Mobile Agents-Based Smart Objects for the Internet of Things*, pages 29–48. Springer International Publishing, Cham.

Lynne, P. (2007). Distributed intelligence: Overview of the field and its application in multi-robot systems. In *The AAAI Fall Symposium Series*. AAAI Digital Library.

Nakamoto, S. et al. (2008). Bitcoin: A peer-to-peer electronic cash system.

Perera, C., Qin, Y., Estrella, J. C., Reiff-Marganiec, S., and Vasilakos, A. V. (2017). Fog computing for sustainable smart cities: A survey. *ACM Comput. Surv.*, 50(3):32:1–32:43.

Rahman, H. and Rahmani, R. (2018). Enabling distributed intelligence assisted future internet of things con-

troller (fitc). *Applied Computing and Informatics*, 14(1):73 – 87.

Research, A. (2013). More than 30 billion devices will wirelessly connect to the internet of everything in 2020. (1).

Sahni, Y., Cao, J., Zhang, S., and Yang, L. (2017). Edge mesh: A new paradigm to enable distributed intelligence in internet of things. *IEEE Access*, 5:16441–16458.

Serguei, P. (2017). The tangle. (1).

Van den Abeele, F., Hoebeke, J., Teklemariam, G. K., Moerman, I., and Demeester, P. (2015). Sensor function virtualization to support distributed intelligence in the internet of things. *WIRELESS PERSONAL COMMUNICATIONS*, 81(4):1415–1436.

Yi, S., Li, C., and Li, Q. (2015). A survey of fog computing: Concepts, applications and issues. In *Proceedings of the 2015 Workshop on Mobile Big Data*, Mobidata 15, pages 37–42, New York, NY, USA. ACM.