ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

A Detailed Study of Routing in Internet of Things

Tausifa Jan Saleem

Abstract*— The convergence of the Internet, sensor networks, and Radio Frequency Identification (RFID) systems has ushered to the concept of Internet of Things (IoT) which is capable of connecting daily things, making them smart through sensing, reasoning, and cooperating with other things. Internet of Things (IoT) has emerged as a potential future scenario of the applicability and impact of technology in human life. Internet of Things extends the concept of Internet from a network of rather homogeneous devices such as computers to network of heterogeneous devices such as home appliances, consumer electronics etc. IoT has the potential for a wide range of applications related to healthcare, environment, transportation etc. In order to turn this IoT vision into reality, routing protocols are needed to aid the communication between these things in a decentralized, self-organized and changing infrastructure. Many routing, power management, and data dissemination protocols have been specifically designed for IoT. In this paper I present various challenges for routing in IoT followed by a survey of the state-of-the-art routing techniques in IoT.

Index Terms— **Internet of Things (IoT), Routing techniques, Wireless sensor network (WSN).**

I. INTRODUCTION

The Internet of Things, as given syntactically by its name, is composed of two terms: "Internet" and "Things". The first term describes a networking-oriented aspect of the IoT where the Internet serves as the central building block interconnecting every possible computing device in the world. This aspect is explicitly reflected in the definition for IoT as "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols"[1].Recent fast advancements in various technological fields including hardware miniaturization, embedded computing, wireless networking, and sensing and actuating allow for augmenting real-world things with an unique identification (ID) and the capabilities to process information, to sense and respond to the environment, thus making them smart, and for smart things to be able to wirelessly communicate with other smart things by connecting smart things to the Internet such that they can publish their ID and status (i.e., the real-world states perceived by their embedded sensors) on the Web, an Internet of Things (IoT) is formed. By mashing up smart things with the services and data available on the Web, novel and valuable IoT applications for human users will be created. Although a final definition of the IoT is still subjected to debate , there is a consensus on the vision of the IoT, which is three-fold:

(i) To give the inanimate things of the physical world the ability to gather, process, and act on information, therefore making them "smart".

(ii) To unite the cyber world of computers and information with the physical world we live in by connecting all smart things to the current Internet.
(iii) To enable the intuitive interaction between humans and technology, such that human users are unobtrusively assisted by technology in performing everyday activities.

In the last two decades, embedded computing and hardware miniaturization technologies advanced to a stage where it became possible to pack processing, wireless communication, sensing, and power supply capabilities into a volume size of a cubic centimeter or even a few cubic millimeters [2], creating a miniaturized computing device. Due to their tiny size, these computing devices could be attached to objects (e.g., people, desks, food items), embedded into places (e.g., homes, offices), and dispersed in large quantities into the environment (e.g., forests, farm fields), forming wireless networks of embedded computing devices that can be used as tools for tracking, observing, and influencing the real world. RFID systems and wireless sensor & actuator networks are typical examples of these tools, where objects that are equipped with an RFID tag can be tracked and aspects of the real world can be observed via sensors and controlled via actuators. Routing is an essential service in the IoT, since it enables the exchange of information between Things, by efficiently directing and reliably delivering data on the

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

network from their sources to their destinations. Routing, in general, answers the question of "how an entity is brought from an origin to a destination". In the context of the IoT, the entity is a data packet, and the origin and destination of the data packet are two computing devices and are called the source and the destination, respectively. A computing device can either be an IoT device (such as an RFID tag, a sensor node, or a Smartphone) or an Internet device (such as a PC or a server computer). We call a computing device a routing node. Due to the fact that there is not always a direct physical connection between the source and the destination of a data packet, the packet must be relayed from one intermediate routing node to another before arriving at the destination. This approach is known as multi-hop routing. The series of hops i.e, intermediate routing nodes that are involved in relaying the data packet, is called a routing path or a routing route.

II. VARIOUS ROUTING CHALLENGES

There are many challenges that can affect routing in the IoT. The challenges can come from the routing layer itself, and/or from the layers underneath it such as physical and medium access control (MAC) layers.

A. Limited Resource

One of the main challenges to the IoT, is the limitation of resources, including energy supply, processing power, memory capacities, wireless communication range, and wireless communication bandwidth. This limitation affects routing in many ways. The short wireless communication range dictates that routing must be done in a multihop fashion, i.e., the data packets must be forwarded by multiple relay nodes in order to reach to their destination. The low processing power and program memory require that the routing process running on the IoT devices must be highly optimized and light-weight. The small storage memory and scarce communication bandwidth may limit the size of the packets to be forwarded. The scarce energy source (either battery-supplied or harvested) makes it difficult to decide which nodes should forward the data packets, since wireless communication dominates the energy consumption of the IoT devices.

B. Dynamic Routing Topology

The cause of the dynamicity of the routing topology is many folds. Firstly, due to energy constraint, IoT devices are usually scheduled to be idle or working (e.g., by turning the wireless radio on/off) to minimize energy consumption, making the routing topology dynamic. Secondly, since users deploy or remove their IoT devices at will, routing nodes will be connected to and disconnected from the IoT at unknown rate, which adds the unpredictability to the dynamicity of the routing topology. Thirdly, node failures are common in the IoT. The causes of a failure include hardware malfunctioning (e.g., antenna damage), exhausted energy supply (e.g., depleted batteries), and environmental impact. Fourthly, node mobility causes the wireless links between the mobile nodes and other nodes in their proximity to be reconfigured. Finally, the low-power wireless links in networks of IoT devices (e.g, WPAN, WSN) are unreliable and transitional, which also contributes to the dynamicity of the topology. The routing protocols hence must be flexible enough to deal with such dynamicity of the IoT's topology.

C. Scalability

The IoT will be large in scale, both in terms of number of nodes and geographically. As routing means to decide over which routing path the data packet should be sent, the more candidate relay nodes to be evaluated for inclusion in a routing path, the more complex routing is. This complexity is many fold, including what cost function to be used, how to decide which of the neighbors of a node is the relay node, what is the cost to setup and maintain a routing path, how to setup a new routing path when another one is broken, etc. Such complexity will quickly grow unmanageable if the routing protocol was not carefully designed with scalability challenge being taken into account.

D. Partitions and Voids

Another major challenge to routing in the IoT is the presence of network partitions and voids in the network. A partition is a disconnected part of the network, such that nodes inside a partition cannot communicate with nodes in the other parts of the network, because there is no routing path to exchange data packets. A void is an area that is not covered by the network. Since there is no node located inside the void that is connected to node(s) outside it, data packets can only be forwarded around the void to reach to their destination. For example, a WSN has been

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

deployed by randomly scattering a large number of sensor nodes over a geographical area. Due to the structure of the area, there may be lakes that cause voids, or rivers that cause partitions in the WSN.

III. ROUTING APPROACHES

A. Distributed vs. Centralized

These two approaches refer to where the routing decision is made, i.e., deciding which path to send the data packet along. There are two choices: centralized and distributed. In a centralized approach, there is a super node that is assumed to have abundant resources and knowledge about the state of the entire network. This super node has control over all other nodes, computes the optimal routing path for every data packet, identifies bottlenecks and underutilized nodes, and adapts the routing paths accordingly. The advantage of centralized routing is a complete control over all aspects of the network, therefore optimal routing paths could be computed. The disadvantages are, however, costly maintenance of the super node, the super node could potentially be the central point of failure, high control overhead as instructions need to be communicated between the super node and other nodes, and last but not least, the computed optimal routing paths may become obsolete quickly due to the dynamicity of the network, especially in the context of the IoT.

In a distributed approach, an individual node or a set of nodes that are in proximity of each other make the routing decision. These nodes do not have knowledge about the state of the entire network, but only about their local state (and possibly the state of their neighbors). The routing decision, therefore, is made only according to this limited knowledge. The advantages of distributed routing are flexibility as decision making is distributed and performed by each node, and responsiveness because nodes in proximity can quickly react to any dynamicity-related issue that occurs locally. The disadvantages are possibly suboptimal routing paths and potentially unbalanced load distribution, since only local information is used. Almost every routing protocol designed for the IoT is distributed to ensure scalability.

B. Flat vs. Hierarchical

Once one decides to follow the distributed approach, one could further decide to follow either the flat or the hierarchical approaches. These two approaches refer to where the routing algorithm is placed and run in the network. In a flat approach, a relatively simple routing algorithm is implemented on every individual routing node of the network. A node makes routing decisions based solely on its own state and the state of a number of other nodes in its proximity. As the design is relatively simple, typical IoT devices such as sensor nodes or active RFID tags can afford to run the routing algorithm. There is no super node that controls the routing of the network in this case. The routing paths computed are the emergent results of many nodes executing the same routing algorithm.
In a hierarchical approach, the routing nodes are divided into several hierarchical levels. Nodes that belong to the same level are assumed to have similar resource budgets, while nodes belonging to different levels have significantly different resource budgets. The routing algorithm is also divided into components with different degrees of complexity. More complex components are implemented on nodes that belong to the higher hierarchy level. Usually, a node manages inferior-level nodes, reports to superior-level nodes, and only collaborates with nodes at the same level. With such a distribution of roles and complexity, network resources could be efficiently utilized for calculating routing paths.

C. Location-based vs. State-based

These two approaches refer to the type of information used by the routing protocol to forward data packets. In a location-based routing protocol, information about the location of the routing nodes are used for addressing nodes and forwarding data packets. The node's locations can be obtained via dedicated hardware (e.g., GPS sensors) or software (e.g, location discovery algorithms). The forwarding decision is usually made based on a Distance metric (e.g, Euclidean distance). Sometimes, information about network resources are also combined with the distance metric if one or more routing properties are to be integrated into the design. The advantages of location-based routing are low control overhead, scalability, and robustness against network dynamicity, since the processes of route discovery and maintenance (i.e, finding the destination and maintaining an established path to it) are spared, and information about network topology is not required. The disadvantage is the dependence on means for location discovery, which can be costly in terms of money (e.g., buying GPS receiver hardware) or network resources (e.g., distributed algorithm for location discovery).

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

In a state-based routing protocol, a data packet is forwarded based on the information about the current state of the network. The network state can be (i) stored at nodes and/or (ii) included in the data packet. In the case (i), each node has a view on the current topology of the network in terms of which nodes are connected to which other nodes, or the distances from the node to all other nodes (distance is a measure of the cost to reach a certain node, that usually is a cost function of hop count and/or a set of resources such as the node's residual energy). These two approaches are known as link state and distance vector routing, respectively. Representative routing protocols that follow these approaches are for link state routing, and for distance vector routing, and their variants. In the case (ii), a routing path that the data packet should traverse to its destination is stored in its header and is specified by the source. A relay node uses this information to make routing decisions. The main disadvantage of state-based routing is poor scalability, since the storage required to store the network state at each node and the amount of information required to be exchanged across the network to update topology changes do not scale with the number of nodes. Additionally, network state may get obsolete quickly if topology changes are not updated fast enough leading to inefficiently computed routing paths.

D. Data-centric vs. Address-centric

The design choice to follow one of these two approaches depends on the type of the application running on the network. In traditional networks such as the Internet or networks of wireless computer devices (e.g., laptops, smart phones), data packets usually are routed based on the addresses of their destination nodes. For example, in a video conferencing application, multimedia data packets are destined only to the addresses of the participants in the video conference (i.e., their laptops or smart phones). An address is unique to a network node, which could be the node's MAC address, IP address, or any other type of unique identification (e.g., RFID). This approach is known as address-centric routing. Many IoT-enabled applications require that data generated by all or a large percentage of nodes are reported to a sink node for further processing. For example, an RFID reader scans all RFID tags within its communication range, or sensor nodes in a WSN periodically send their sensed data about a certain event to the WSN's base station. In such applications, it is important that nodes with certain types of data (e.g., temperature readings, free parking lots) rather than with specific addresses (or identifications) send data packets to the sink.
Due to multiple nodes sampling the same type of data or observing the same event, there are data redundancies which can be eliminated by performing data fusion at relay nodes as the data packets travel to the sink. Data fusion at a relay node means to integrate similar information contained in multiple data packets into a consistent, accurate, and useful piece of information that is to be forwarded by the relay node towards the sink. This type of forwarding is known as data-centric or query-based routing. The data-centric routing is usually a consequence of the sink dispersing a query into the network with the help of a routing protocol (e.g., a location-based routing protocol to deliver the query to multiple geographical regions).

IV. VARIOUS ROUTING TECHNIQUES

A. Flooding

In flooding [4], the source node floods all events to every node in the network. Whenever a sensor receives a data message, it keeps a copy of the message and forwards the message to every one of its neighboring sensors and the cycle repeats. It is an easy-to-implement routing scheme, and it is suitable for various network types, node distributions and environments. The main advantage of flooding is the increased reliability. Since the message will be sent at least once to every host it is almost guaranteed to reach its destination. But the unlimited broadcasting packets in the flooding scheme will cause the broadcast storm.

B. Sensor Protocols for Information via Negotiation (SPIN)

SPIN [5,6] disseminates all the information at each node to every node in the network assuming that all nodes in the network are potential base-stations. This enables a user to query any node and get the required information immediately. These protocols make use of the property that nodes in close proximity have similar data, and hence there is a need to only distribute the data that other nodes do not posses. The SPIN family of protocols uses data negotiation and resource-adaptive algorithms. Nodes running SPIN assign a high-level name to completely describe their collected data (called meta-data) and perform meta-data negotiations before any data is transmitted. This assures that there is no redundant data sent throughout the network. The semantics of of the meta-data format is application-specific and is not specified in SPIN. For example, sensors might use their unique IDs to report meta-data if they cover a certain known region.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

C. Ad-hoc On-demand Distance Vector (AODV)

AODV [7] is the simplest and widely used algorithm either for wired or wireless network. It is one of the most efficient routing protocols in terms of establishing the shortest path and lowest power consumption. It is mainly used for ad-hoc networks and also in wireless sensor networks. It uses the concepts of path discovery and maintenance. However, AODV builds routes between nodes on-demand i.e. only as needed. So, AODVs' primary objectives are:

1. To broadcast discovery packets only when necessary.
2. To distinguish between local connectivity management (neighborhood detection) and general topology maintenance.
3. To disseminate information about changes in local connectivity to those neighboring mobiles nodes that are likely to need the information.

D. Directed Diffusion

Directed diffusion [8] is a data-centric (DC) and application aware paradigm in the sense that all data generated by sensor nodes is named by attribute-value pairs. The main idea of the DC paradigm is to combine the data coming from different sources (in-network aggregation) by eliminating redundancy, minimizing the number of transmissions; thus saving network energy and prolonging its lifetime. Unlike traditional end-to-end routing, DC routing finds routes from multiple sources to a single destination that allows in-network consolidation of redundant data.

E. Active Query Forwarding In Sensor Networks (ACQUIRE)

ACQUIRE [9] views the network as a distributed database where complex queries can be further divided into several sub queries. The operation of ACQUIRE can be described as follows. The BS node sends a query, which is then forwarded by each node receiving the query. During this, each node tries to respond to the query partially by using its pre-cached information and then forward it to another sensor node. If the pre-cached information is not up-to-date, the nodes gather information from their neighbors within a look-ahead of d hops. Once the query is being resolved completely, it is sent back through either the reverse or shortest-path to the BS. Hence, ACQUIRE can deal with complex queries by allowing many nodes to send responses. Note that directed diffusion may not be used for complex queries due to energy considerations as directed diffusion also uses flooding-based query mechanism for continuous and aggregate queries. On the other hand, ACQUIRE can provide efficient querying by adjusting the value of the look-ahead parameter.

F. Energy Aware Routing (EAR)

The objective of energy-aware routing protocol [10], a destination initiated reactive protocol, is to increase the network lifetime. Although this protocol is similar to directed diffusion, it differs in the sense that it maintains a set of paths instead of maintaining or enforcing one optimal path at higher rates. These paths are maintained and chosen by means of a certain probability. The value of this probability depends on how low the energy consumption of each path can be achieved. By having paths chosen at different times, the energy of any single path will not deplete quickly. This can achieve longer network lifetime as energy is dissipated more equally among all nodes.

G. Low Energy Adaptive clustering Hierarchy (LEACH)

LEACH [11] is a cluster-based protocol, which includes distributed cluster formation. LEACH randomly selects a few sensor nodes as cluster heads (CHs) and rotates this role to evenly distribute the energy load among the sensors in the network. In LEACH, the cluster head (CH) nodes compress data arriving from nodes that belong to the respective cluster, and send an aggregated packet to the base station in order to reduce the amount of information that must be transmitted to the base station. LEACH uses a TDMA/CDMA MAC to reduce inter-cluster and intra-cluster collisions. However, data collection is centralized and is performed periodically. Therefore, this protocol is most appropriate when there is a need for constant monitoring by the sensor network. A user may not need all the data immediately. Hence, periodic data transmissions are unnecessary which may drain the limited energy of the sensor nodes.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

H. Power-Efficient Gathering in Sensor Information Systems (PEGASIS)

The protocol, called Power-Efficient Gathering in Sensor Information Systems (PEGASIS) [12], is a near optimal chain-based protocol. The basic idea of the protocol is that in order to extend network lifetime, nodes need only to communicate with their closest neighbors and they take turns in communicating with the base-station. When the round of all nodes communicating with the base-station ends, a new round will start and so on. This reduces the power required to transmit data per round as the power draining is spread uniformly over all nodes. Hence, PEGASIS has two main objectives. First, increase the lifetime of each node by using collaborative techniques and as a result the network lifetime will be increased. Second, allow only local coordination between nodes that are close together so that the bandwidth consumed in communication is reduced. Unlike LEACH, PEGASIS avoids cluster formation and uses only one node in a chain to transmit to the BS instead of using multiple nodes.

I. Routing Protocol Based on Energy and Link Quality (REL)

REL combines a reliable scheme for route discovery and load balance mechanism, which provides high reliability, QoS-awareness and energy-efficiency. Moreover, it proposes an end-to-end route selection scheme based on cross-layer information with a minimal overhead. Nodes become energy efficient by sending the residual energy to their neighboring nodes with the aid of a piggyback and on-demand scheme. Additionally, REL also uses an event-driven mechanism to provide load balancing as a way to improve the system performance and avoid the energy hole problem. We summarize recent research results on data routing in IoT in the Table (Table 1).

Table 1: Classification and comparison of routing protocols

	Classification	Mobility	Scalability
A. Flooding	Flat	Limited	Limited
B. SPIN	Flat	Possible	Limited
C. AODV	Flat	Possible	Limited
D. Directed Diffusion	Flat	Limited	Limited
E. ACQUIRE	Flat	Limited	Limited
F. EAR	Flat	Limited	Limited
G. LEACH	Hierarchical	Limited	Good
H. PEGASIS	Hierarchical	Fixed BS	Good
I. REL	Flat	Limited	Good

V. CONCLUSION

Routing in internet of things is a new area of research, with a limited, but rapidly growing set of research results. In this paper, I presented a comprehensive survey of routing techniques in internet of things. They have the common objective of trying to extend the lifetime of the sensor network, while not compromising data delivery. Although many of these routing techniques look promising, there are still many challenges that need to be solved in the Internet of Things.

REFERENCES

[1] INFSO D.4 Networked Enterprise & RFID INFSO G.2 Micro & Nanosystems. Internet of Things in 2020, Roadmap for the Future, Version 1.1. In: Co-operation with the Working Group RFID of the ETP EPOSS, 27 May 2008.

[2] B. A. Warneke, M. D. Scott, B. S. Leibowitz, L. Zhou, C. L. Bellew, J. A. Chediak, J. M.Kahn, B. E. Boser, and K. S J. Pister, “An Autonomous 16 Cubic mm Solar-Powered Node for Distributed Wireless Sensor Networks”, In IEEE International Conference on Sensors 2002, pages 1510–1515, Orlando, USA, June 2002.

[3] Jamal N. Al-karaki and Ahmed E. Kamal, “Routing Techniques in Wireless Sensor Networks A Survey”, IEEE Wireless Communications, 11:6–28, 2004.

ISSN: 2319-5967
ISO 9001:2008 Certified
International Journal of Engineering Science and Innovative Technology (IJESIT)
Volume 5, Issue 3, May 2016

[4] Wei Yen, Ching-Wei Chen and Cheng-hsiang Yang, "Single Gossiping with Directional Flooding Routing Protocol in Wireless Sensor Networks", in Proceedings IEEE, 2008.

[5] W. Heinzelman, J. Kulik, and H. Balakrishnan, "Adaptive Protocols for Information Dissemination in Wireless Sensor Networks", Proc. 5th ACM/IEEE Mobicom Conference (MobiCom '99), Seattle, WA, August, 1999. pp. 174-85.

[6] J. Kulik, W. R. Heinzelman, and H. Balakrishnan, "Negotiation-based protocols for disseminating information in wireless sensor networks", Wireless Networks, Volume: 8, pp. 169-185, 2002.

[7] Elizabeth M. Royer, Charles E.Perkins, "An Implementation of the AODV Routing Protocols".

[8] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", Proceedings of ACM MobiCom '00, Boston, MA, 2000, pp. 56-67.

[9] N. Sadagopan et al.,"The ACQUIRE mechanism for efficient querying in sensor networks", in the Proceedings of the First International Workshop on Sensor Network Protocol and Applications, Anchorage, Alaska, May 2003.

[10] R. C. Shah and J. Rabaey, "Energy Aware Routing for Low Energy Ad Hoc Sensor Networks", IEEE Wireless Communications and Networking Conference (WCNC), March 17-21, 2002, Orlando, FL.

[11] W. Heinzelman, A. Chandrakasan and H. Balakrishnan, "Energy-Efficient Communication Protocol for Wireless Microsensor Networks", Proceedings of the 33rd Hawaii International Conference on System Sciences (HICSS '00), January 2000.

[12] S. Lindsey, C. Raghavendra, "PEGASIS: Power-Efficient Gathering in Sensor Information Systems", IEEE Aerospace Conference Proceedings, 2002, Vol. 3, 9-16 pp. 1125-1130.

[13] Suciu, G., Vulpe, A., Todoran, G., Cropotova, J. and Suciu, V. (2011) Cloud Computing and Internet of Things for Smart City. 1409-1416.