Routing Issues in Internet of Things: A Survey

Amol Dhumane, Rajesh Prasad, Jayashree Prasad

***Abstract* --** "Everything that is connected to the internet is alive", is going to be the new rule for future. Future is Internet of Things (IoT), we are moving towards it with rapid pace. Often to the way humans use internet, now onwards devices will be the main users of IoT ecosystem [3]. Recent research deeds capitalizing on the state of the art technologies to build a scalable IoT [4]. However, the comprehension of IoT framework is slowed down because of some factors, out of that the most critical are integration of the devices which are heterogeneous, secure communication between them, trust management and cooperation within such devices and nodes. These devices communicate with each other for gathering, sharing and forwarding the information in multihop manner [3]. IoT generates enormous data continuously, therefore for creation of an intelligent environment, the collected information needs to be transformed into intelligence. This intelligent environment may play a vital role while routing the data in the network.

Many nodes in IoT undergo constant movement that may result into intermittent interconnectivity between the devices which may encounter frequent topology changes. Due to these frequent topological changes and limited resources available in the IoT devices, now a day's routing of the data has become a great challenge in front of the today's research community.

This survey emphasizes on routing of the data in IoT. The goal is not only to analyze, compare and consolidate the past research work but also to appreciate their findings and discuss their applicability towards the IoT.

***Index Terms*--** Context awareness, Routing, Device to Device (D2D) communication, Internet of Things (IoT).

I. INTRODUCTION

Kavin Ashton proposed the term "Internet of Things" [1]. He states that "The Internet of Things has the potential to change the world, just as the Internet did. May be even more so" [19].The IoT does not transfigure our lives or field of computing, but we can consider it as another footstep in the maturity of the Internet that we already have taken. The aim of IoT is develop an enhanced surrounding for the mankind which will automatically comprehend the requirements of human beings and will perform in view of that. From the private users point of view the most apparent effect of the introduction of IoT will be seen in both working and domestic fields.

IoT bundles several different technologies together to build its vision [2]. The integration of these enabling technologies, along with Internet based and context aware services facilitate a dynamic platform for IoT [4]. Due to the capabilities that can be offered by IoT, it has gained major attention from the industry as well as academia since the past decade [20] [21]. IoT promises to build the globe where all the objects around us will be connected to the Internet and will be communicate with each other with bare minimum human intervention [23]. Our objectives in visiting the literature are threefold: 1) to learn which routing techniques were presented in the past 2) how can we apply these techniques in solving the problems in future, and 3) to highlight the open challenges and to decide the future research direction.

The objective of this paper is to focus on the state-of-art routing algorithms and their analysis which will help to understand and identify the major challenges in the routing process of IoT. The rest of this paper is organized as follows. Section II presents an overview of IoT and the communication process. In section III, the issues related to routing in IoT are discussed. Section IV focuses on existing routing algorithms in IoT. Few observations and parameters are discussed in section V based on the study of existing protocols. Section VI puts a beam of light on the open challenges and direction for future research. Section VI concludes the paper.

II. INTERNET OF THINGS

IoT is widely used term but because of the large amount of concepts included in it but its definition is still fuzzy. Although the definition of 'Things' has changed as technology evolved, the main goal of making a computer to sense information without the help of human intervention remains the same[12]. Many researchers have attempted to define IoT. Few of the notable findings are listed below.

A. Definitions of IoT

According to [24], *"IoT stands for a worldwide network of interconnected objects uniquely addressable based on standard communication protocols"*

According to T. Lu et al. [25], *"Things have identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social environment and user contexts".*

According to cluster of European research projects [28] on IoT, *"Things are active participants in business, information and social processes where they are enabled to interact among themselves and with the environment by exchanging data and information sensed about the environment, while reacting autonomously to the real/physical world events and influencing it by running processes that trigger actions and create services with or without human intervention"*

European Commission in [26] defined IoT as, *"The semantic origin of the expression is composed of two words and concepts: Internet and Thing, where Internet can be defined as the world-wide network of interconnected computer networks, based on standard communication protocol, the Internet suite (TCP/IP), while Thing is an object not precisely identifiable. Therefore semantically, Internet of Things means the world wide network of*

Amol Dhumane and Rajesh Prasad are with the NBN Sinhgad School Engineering, Pune, Maharashtra, India (phone: +91-8793280010; email: amol.dhumane@sinhgad.edu, rajesh.prasad@sinhgad.edu). Amol Dhumane is the corresponding author.

Jayashree Prasad is with Sinhgad College of Engineering, Pune, Maharashra, India. (email: Jayashree.prasad@sinhgad.edu)

interconnected objects uniquely addressable, based on standard communication protocols."

In [18] O. Vermesan et al. defined IoT as, *"A dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols where physical and virtual 'things' have identities, physical attributes and virtual personalities and use intelligent interfaces and are seamlessly integrated into the information network".*

The widely accepted definition is suggested by P. Guillemin et al. [27] is, "*IoT allows people and things to be connected Anytime, Anyplace, Anything and Anyone ideally using any path/network and Any service*".

B. Objectives of IoT

With this preview authors rephrase the objectives as follows:

1. To build highly interconnected system where devices will be the users of the internet.
2. This system should work 'smartly' for the betterment of human beings.
3. The system should improve the relationship between the humans and the environment in which they live.

C. Communication in IoT

According to W.Vogels et al. [13] in 2011, the number of interconnected devices on the earth overtakes the actual number of people. It is expected that interconnected devices will touch 24 billion by 2020 for crafting smart environment. Mark Wiser [5] defined smart environment as "the physical world that is richly and invisibly interwoven with sensors, actuators, displays and computational elements, embedded seamlessly in everyday objects of our lives, and connected through a continuous network". The network structure of IoT is horizontal having same priority to every node.

Various types of communication are possible in this area such as device to device, device to human and vice versa. The most important requirement of IoT is to provide connectivity between the devices to attain a seamless end-to-end D2D communication for the success of IoT. This type of communication can only be achieved if communication process supports the exchange of information between the heterogeneous devices and across the heterogeneous networks [3].

Due to the resource constraints and obvious reasons of resource conservation prevent such entities from participating in relaying data packets until and unless there is a good incentive mechanism [10]. Hence Oteafy et al. [4] suggested that intermediate nodes must be encouraged to participate in relaying messages by integrating some rewards such as monetary gain to the relaying devices.

III. ROUTING IN IoT

IoT is going to offer huge number of applications in various environments for improving the quality of our lives. These applications will generate enormous amount of data. One of the key upshots of this rising field is the creation of an unprecedented amount of data, its storage, ownership, security, expiry and it's routing to a desired destination for generating some intelligence out of it that can be further used to build a smart environment. The routing issues become more and more challenging for low-power and lossy radio-links, multi-hop mesh topologies, the battery supplied nodes and frequently changed network topologies.

One misconception related to IoT is that, a significant pool of protocols previously developed for the functionality of the Internet would migrate into IoT [4], but this is not the case. As IoT contains a set of moving as well as stationary components, multiple issues arise in the development of routing protocols where these devices will intercommunicate with each other. As various factors shown in table I are dominant in the operation of routing protocol, so it becomes difficult to devise a single protocol which will achieve all these objectives that are inherently paradoxical. Due to it routing becomes a notorious NFL (no free lunch) class of algorithm.

According to Oladayo Bello et al. [3] an intelligent routing protocol can unleash the intrinsic power of any heterogeneous, dynamic, and complex network that is characterized by multiple dynamic factors such as changing topology and flow. Thus to achieve the full functionality of IoT, intelligent protocols are needed for D2D communication in IoT. Efficient and scalable routing protocols adaptable to different scenarios and network size variations, capable to find optimal routes are required.

A.Factors affecting the Routing process

Table I enlists various factors affecting the routing process in IoT with short description.

Table I
Factors affecting communication process.

Devices	May be of similar type or dissimilar types.
Manufactures	The manufacturers of these devices may be same or different.
Network	The source and the destination may exist on the same or different networks.
Connectivity	Connectivity between any two devices may be constant or intermittent.
Resources	Insufficient resources.
Cooperation in data relaying	Non-cooperation of devices due to resource constraints.
Communication process	Changing mode of communication e.g. single hop or multihop.
Network topology	Frequently changing network topology due to mobile devices and resource constraints.
Communication range	Variety of communication ranges among devices manufactured by different vendors.
Harsh environmental conditions	Harsh environmental conditions such as heavy rain, high temperature etc. may start malfunctioning of the devices or they may be died.
Addressing mechanisms	There should be a universally acceptable and unique addressing mechanism for making the D2D communication easier.

B. Optimization techniques in routing

1. Energy efficient routing: It optimizes energy requirements while selecting a path to destination that helps to increase the network lifetime. This technique routes the data to the destination through those nodes which are having sufficient energy resources and avoids the participation of nodes having energy below a specific threshold value.
2. Data redundancy elimination: More data means more energy requirement for routing it. Most of the times there is redundancy in the data. Eliminating the redundancy will reduce the energy requirement for data routing, resulting into increased network lifetime. This generates a need to develop data fusion techniques.
3. Delay minimization: IoT contains a dense population of the devices generating enormous amount of data. Expiry is associated with the data. Due to that it is essential to send the data to the destination within fixed time span. Because of it delay minimization is necessary.

C. Classification of routing algorithms

Table II gives the classification of the algorithms based on various on parameters. The use of these algorithms should be observed according to the characteristics of the applications including their goals and QoS requirements. This classification can be further extended by adding some more parameters such as QoS. Nowadays the requirements are changing and researchers are engaged in designing more intelligent routing algorithms which will understand the environment and the exact condition of the network. Routing decisions will be taken according to the context gathered from various parts of the network. These routing algorithms are termed as ‘Context aware routing algorithms’.

D. Context Awareness in Routing

Abowd and Mynatt [22] identified five W’s (Who, What, Where, When, Why) as the bare minimum information that is needed for understanding the context. The information can be gathered from the surrounding environment may be in the form of raw data which needs to be processed for making it consistent. Before gathering the context, it is necessary to identify the features of context for exactly describing it. Context features are having some value associated with them for describing a specific attribute. Only identification and preprocessing of the context information is not sufficient, we also need to maintain the quality of the context. Quality of the context can be judged based on the some parameters such as accuracy of the context and validity of the context. The context of the environment changes time to time, so it is necessary to have more accurate, valid and unexpired context always available for taking proper routing decision. Context dissemination is the next step once the context gets ready for execution purpose. It is necessary to send the context to the neighboring nodes for further use. Mainly two different thoughts are associated with the context dissemination: first is to get and store the context in the centralized manner on the context server and other is context is stored in distributed manner and is percolated to the entire network topology as and when a specific event occurs. Both the approaches are having positive and negative aspects associated with it. But according to the majority of the researchers, second thought is more meaningful since in the first case every time the node needs to communicate with the context server for doing certain activity, which may be more energy consuming. Few Challenges associated with context aware routing are listed below.

a) Context acquisition and distribution: For smart routing it is necessary to collect the context from the environment. The network topology has to gather the raw information from various parts and then it needs to convert it into context after preprocessing and validating it.

b) Context quality: A survey on context quality [14] has defined quality of context (QoC) based on three parameters: context data validity, context accuracy, and up-to-dateness of context data. The survey states that QoC depends on quality of the physical sensor, quality of the context data and that of the delivery process. Context quality also depends on the way of conversion of primary context into its secondary context form.

c) Context storage: It is always painful to store the context on the resource constrained devices due to shortage of memory. There should be some mechanisms that will store the context on such devices in the compressed form or another approach can be to store the context of the entire network on the centrally situated context server.
Advantages of context aware routing: Intelligent routing, network load balancing, network lifetime maximization, and reduction in communication delay

IV. EXISTING ROUTING ALGORITHMS IN IoT

This section discusses some of the recent routing protocols in IoT. Authors have analyzed these protocols based on some parameters.

A. Ad-hoc on demand Multipath Distance Vector routing protocol for IoT (AOMDV-IoT)

This protocol creates the connection between regular nodes (not connected to internet) and the internet nodes [15]. Every node maintains two tables known as internet connecting table (ICT) and the routing table on it. This adds an extra overhead on the available memory of the nodes. Initially, the source node does not know with which internet connected node it is going to communicate as there can be few (or many) nodes connected to internet. When the node attempts to create a link to the internet, it puts the destination IP address as Internet Linking Address (ILA). Then it search into the ICT and tries to find if ICT have appropriate nodes connected to internet. If ICT contains such nodes, then the ILA address is replaced by the destination node’s IP address. Otherwise the source node broadcasts the route request (RREQ) message for refreshing the content of routing table and the ICT tables. This is a reactive protocol which discovers the path on demand. The protocol uses following four types of messages in the communication process:
RREQ: For searching the route to the destination.
RREP: Destination sends RREP to source in response to RREQ message (like ACK message).
RERR: Used by unreachable node’s neighbors for notifying other nodes that the previously reachable node is now unreachable.

Table II
Classification of routing algorithms

Parameter	Types	Description
Network Structure	Hierarchical or vertical	The network topology is broken down into several layers of hierarchy; the intention may be downsizing the routing table. The main idea here is the network is divided into clusters and cluster head is selected from every cluster based on its energy level. Lower energy nodes are used to sense in the proximity and higher energy nodes are used for processing data for understanding the context. Cluster head functionality is not permanently assigned to a single node. Rather this functionality is offered to all the node of the cluster time to time depending on their energy level. Data fusion techniques can be applied at cluster head for reducing the redundancy in the data. Hierarchical algorithms are further divided into two subtypes [3]: 1. Tree based algorithms: A tree of multiple hops is dynamically constructed for routing messages and data by creating traffic pattern of many to one. 2. Cluster based algorithms: It classify devices into clusters. Devices play different roles according to their level in the hierarchy. The main shortcoming of this type of algorithm is, they require extra time for cluster formation which is unsuitable for many IoT applications.
	Flat or Horizontal	These protocols are used in the network having flat or horizontal structure. In contrast to hierarchical network structure, every node in this network has equal importance and is treated at the same level. No special efforts are taken to organize the network and its traffic. Generally efforts are taken to discover the route hop by hop to a destination by any path. Flat-based approaches represent a suitable solution for many homogeneous IoT solutions due to their low operational complexity and high efficiency.
	Location based	Location of nodes is taken into consideration. Signal strength is used to address the location of the node when the nodes are in proximity. The nodes which are separated by enough distance, relative coordinates of nodes can be extracted through the information exchanged between the neighboring nodes. In case of location based routing protocols, a node decides the transmission route according to the localization of the destination and positions of some other nodes in the network.
Protocol operation	Multipath routing protocol	The main objectives of multipath routing protocols are to provide reliable communication and to ensure load balancing as well as to improve quality of service (QoS). As a fault tolerance mechanism, these protocols construct many paths and based on the energy requirement a single path is selected from this set of paths. For keeping alive the sparse paths, periodic messages are sent on them. The goals are to improve delay, provide reliability, reduce overhead, maximize network life and support hybrid routing.
	Query based	These protocols are also considered as reactive protocols. The route discovery process has two phases: request phase and reply phase. When node requires a route to destination, it starts a route query phase. This query source generates a query packet and sends it to its neighbors. When the query destination receives the query, it responds it with reply.
	Negotiation based	In this type of protocols, source and destination communicates with each other for eliminating the redundant data. Depending on the availability of the resources with each participating node the negotiation decisions are done.
	Energy aware	The aim of these protocols is to select those routes that are expected to maximize the network lifetime. To do so, the preferred routes are made up of nodes with high energy resources or having energy resources with the value which is above the specified threshold.
	Context aware	Context is the information that can be used to characterize the situation of an entity [11]. The context can be the residual energy of the device, memory, processing power, its location and its speed of mobility. Context aware routing systems makes use context in the routing process.
	Swarm intelligence	These are based on the laws and dynamics that govern biological systems. Examples are ant colony optimization (ACO) algorithms. They can also be based on other biological systems such as human immune system and epidemic spreading [7] [13] [16].

Maintaining routing information	Proactive	Proactive protocols always maintain route information in tabular format at any time. Proactive protocols are used in static networks where topology is fixed most of the times. As the routing is always based on routing table, these protocols are also referred as “table driven protocols”.
	Reactive	Reactive protocols do not maintain the information of route, the routes are formed as and when they are required. Reactive protocols are used in dynamic networks where there is occurrence of frequent topological changes. As IoT supports dynamic topologies most of times so from the researcher’s point of view reactive protocols are having special importance in it.
	Hybrid	Hybrid protocol uses the functionality of both the proactive and reactive protocols together.
Network conditions	Stochastic or probabilistic Algorithm	They are designed to formulate routing probabilities which optimizes the set of network resources. The resources are selected based on the conditions within the network and are defined as the criteria for optimality. It uses two methods for optimization: real time and priory optimization.

HELLO: Used at periodic intervals for the maintenance of routing tables.

Shortcomings in AOMDV-IoT:

i. There is no security mechanism in the data routing.
ii. This protocol does not understand the context. It does not optimize its routing paths based on the residual energy of the nodes.
iii. The problem associated with distance vector routing algorithms is that it routes the data based on minimal hop count but which may not be necessarily energy efficient solution.
iv. This type of algorithms stores information of only one possible route towards the specified destination which may result into increase in the delay and failure rate of data delivery in case of link failure.

B. *Secure Multihop Routing Protocol (SMRP):*

It focuses on increasing the security of the data by preventing the malicious attacks [9]. In this protocol owners of every IoT network have to register their own applications, network address and data link address to a legitimate Service Provider (SP). Based on the registers information, before the network formation, it’s a duty of the SP to generate an Encrypted File (EF) and install it on every individual device.

Similar to all other routing protocols, the IoT devices emits HELLO messages after every equal interval of time. When device (device_1) comes into the vicinity of other device (device_2), the header of HELLO messages received from device_2 are verified against the headers of HELLO messages of device_2. If there is a match, the devices will communicate, otherwise not.

If device_x wants to connect to an IoT network, it will request to device_y. Then device_y checks the network address, data link address of device_x in the EF file against the list of permitted devices. If device_x is permitted to join the IoT and the application(s) running on it matches the application(s) running on device_y, a signal is sent to unique code generator. It generates unique code which is further embedded into the ‘reserved’ bits of the HELLO packets. Once the timer which is synchronized among all the IoT devices reaches to pre-assigned value, it triggers the scrambler module to change the sequence of the ‘reserved’ bits for enhancing the security in timely manner.

Virtue in SMRP:

i. It is a multihop protocol
ii. It provides a good level security to the data from the malicious attacks. The security is enhanced by scrambling the sequence of the ‘reserved’ bits in the HELLO message.

Shortcomings in SMRP:

i. This is not context aware protocol. Does not conserve the energy of the nodes while routing. It may result into less network lifetime.
ii. The memory requirement is higher as there is a need to store EF file on every devices which may further create a hurdle in the network scalability issue. In short, if devices are less on the IoT network, small is the size of EF file otherwise the EF file size increases which may result into high memory requirements in the devices.
iii. Also the number of devices in any IoT network belongs to the specific owner are need to be specified before the actual network formulation.

C. *Energy aware Ant Routing Algorithm (EARA)*

The main objective of this protocol is to adapt routing process for maximizing the network lifetime [6]. This is a swarm intelligence or bio-inspired algorithm. It not only considers the pheromone values but also the residual energy level of the nodes. As the residual energy in the IoT devices changes over time, the authors had introduced the mechanism to update energy information.

As compared to Ant Routing Algorithm (ARA), ant agents of EARA keep the information of two additional fields: a) Average energy of the nodes ξavgon the basis of number of hops a packet travelled b) It also stores a lowest residual energy value ξminwhich an ant agent encounters in the path.

EARA uses periodic energy ant agents (PEANTs) for updating the energy values in the nodes routing table. The broadcasted PEANTs at the destination collect the energy information on that path. Flooding PEANTs can be a costly operation in terms of consumed energy, so the algorithm sends these control packets occasionally. The destination nodes in EARA achieve this by keeping track of the residual energy of their own battery. If the residual energy is changed by a configurable threshold, EARA floods the network with new PEANT. The time interval of broadcasting the PEANT mainly depends on two parameters i.e. maximum battery capacity and the threshold value of energy which is configured.

Virtue in EARA:

i. It is multihop and context aware routing protocol.

Shortcomings in EARA:

i. Security of data is not considered.
ii. The threshold value of change in energy may affect the performance of it.

D. *Routing protocol over low power and lossy networks (RPL):*

Routing is very challenging for 6LoWPAN networks due to the low power and lossy radio links, the battery supplied nodes, multihop mesh topologies and frequent topology changes due to mobility.

This protocol is developed by International Engineering Task Force (IETF) for low power and lossy networks and it is considered as a de facto routing standard for Internet of Things having the aim to optimize the routing scheme for convergecast traffic pattern. RPL is a distance vector protocol. Starting from a border router, RPL constructs a Destination-Oriented Directed Acyclic Graph (DODAG) using one or several metrics. The DODAG is generated by considering the link costs, node attributes and an objective function. Rank generation for every node on the DODAG is done by the objective function. It supports various types of traffic such as multipoint to point, point to multipoint and point to point. For having loop-free topology, the rank must strictly monotonically increase from the root towards the leaves of the DODAG.

In complex scenarios lossy link network is divided into many partitions depending on the applications context. So in situations it may form multiple uncoordinated DODAG's with independent roots. Multiple instances of RPL can run concurrently on the network devices. RPLInstanceID is used for the unique identification of the instance.

The formation and maintenance of the network topologies is done by DODAG Information Option (DIO) messages which are multicasted periodically and link locally by each node for establishing path towards the root node. DIO messages contain the information such as the DODAG identifier, the objective function, the rank of the node, or the metrics used for the path calculation.

After receiving the DIO message, the neighboring node can set its own rank based on its neighbor's rank. Thus the DODAG construction is done in widening wave fashion. Destination Advertisement Object (DAO) messages are used to back propagate the routing information from leaf nodes to the roots.

Virtue in RPL:

i. This is end to end IP based solution which does not require translation gateways for accessing the nodes within the network from outside world.
ii. It dynamically adapts the sending rate of the routing control messages which will be generated frequently only if the network is in unstable condition.
iii. It allows optimization of network for different application scenarios and deployment.

Shortcomings:

i. Does not support multipath routing.
ii. Energy balancing and load balancing are not taken into consideration.

E. *Multiparent routing in RPL:*

Lifetime of the network is considered as the time period before the death of the first node of the network due to run out of the energy. The purpose behind designing this routing protocol is to maximize the overall lifetime of the network by taking care of most energy constrained nodes i.e. bottlenecks. Oana Iova et al. proposed the Expected Lifetime (ELT) metric for denoting the residual time of the node [17].They constructed a DODAG based on ELT metric for accurately estimating the lifetime of all the routes towards the border router and designed a mechanism for detecting bottlenecks for spreading the traffic load to several parents. A node exploits all its parents, assigning a weight of traffic to each of them and distributes fairly the energy consumption among all the paths towards the border router. As only a part of its traffic will finally arrive at a specific bottleneck, energy consumption is well balanced.

Virtue:

i. Supports multipath routing to improve the fault-tolerance, congestion avoidance and QoS.
ii. It also increases the network lifetime by balancing the traffic load amongst multiple parents.

F. *PAIR (Pruned Adaptive IoT Routing):*

According to Sharief M. A et al. [4], since IoT network belongs to different owners, this protocol introduce a pricing model which helps the intermediate nodes to get some monetary benefits as they utilize their resources for relaying. The pricing model of PAIR protocol is based on following parameters of each relaying node.

Residual energy and power consumption

Current load and buffer space.

Distance to neighbor

PAIR works in two stages: forward and backward. In forward stage, setup messages are broadcasted by the source to its neighbors which contain the cost seen from the source to the current node. Once the intermediate nodes receive these messages, they forward them to their neighbors by updating the cost based on above listed set of parameters. The destination node sends the acknowledgement (ack) on the best selected path based on the collected values of cost parameters from the setup message.

If the acknowledgement message experiences a break in the path of it at a current node i, then it is converted into setup message (called as i_setup) and is forwarded to the neighbors of i for the purpose of route discovery. After getting the i_setup message, the active path gets established between the source and destination and the data transmission may get started.

During data transmission if it comes across a link break then either the transmission of the data is done on the alternate path or by buffering the received data, i_setup messages are generated for discovering a new path towards the destination.

Virtue in PAIR:

i. It is multihop and context aware routing protocol.
ii. It helps to solve the issue of cooperation between the nodes of heterogeneous networks by trying to give some incentive to the relaying nodes as these nodes are spending their energy for relaying that data which does not give any benefit to them.

Shortcomings in PAIR:

i. Security of data is not considered.

ii. Memory requirement may be high as it has to buffer the data on the current relaying node for finding the alternate path when the link break is observed.

G. REL (Routing protocol based on Energy and Link Quality):

It uses the link quality of wireless links as well as the residual energy during the route selection process to increase systems reliability and provides QoS to the various IoT applications. The use of low-power radios and sensitivity to noise, interference as well as multipath distortions makes the wireless links unreliable.

When analyzing a single link, REL relies on Link Quality Indicator (LQI). This metric is provided by physical layer of IEEE 802.15.4 standard. REL stores n possible routes towards the destination and selects the one based on i) quality of wireless links based on weak links metric ii) residual energy and iii) hop count to avoid long and inefficient paths.

The path selection process depends on two threshold: hop count threshold $\mathrm{HCdiff\ max-allow}$ and energy threshold Eth. Energy threshold is used in the route selection and load balancing mechanism. In case of load balancing optimization, the Eth corresponds to the monitoring of energy levels in each node individually. It calculates the difference between current $\mathrm{E(t)}$ and previously recorded $\mathrm{E(t-1)}$ energy level. It the difference between them is greater than Eth, route advisor message gives the information about the new value of residual energy to neighboring nodes where the neighboring nodes re-assess the use of that node in their routes. Low values of Eth shows uniform energy consumption while the high values of it denotes large differences in the energy consumption in the nodes.

Virtue in REL:

i. It considers the link quality while selecting the link for routing.

ii. Better the link quality, more chances of successful packet delivery, which saves more energy by reducing the number of packet retransmissions, resulting into maximization of network lifetime.

iii. Load balancing mechanism avoids the excess use of single path or single node which may further help in reducing the hot spots or energy holes in the network. The energy utilization will be uniform in the network.

V.OBSERVATIONS

This section enlists the node level specific, point to point communication based and end to end communication based factors as shown in figure 1, which may create an impact on the routing mechanism.

i. Node specific: The residual energy of the node, the processing power of the node and the internal memory of the node can affect the routing at node level. The residual energy is directly related to the network lifetime, processing power is the ability of the node to process the data. Higher processing power can make the routing process faster. Also more the internal memory, more data can be buffered, which reduces the chances of packet loss resulting into less number of packet retransmissions but it may introduce queuing delay in the packet transmission. Less memory results into high packet loss but it reduces the queuing delay. As the queue size affects the routing process badly, it is necessary to choose it carefully.

ii. Point to point communication based: trust level, energy requirement for data transmission on this link and cooperation of the communicating nodes. Here trust level is considered as a ratio of number of packets received by the destination to the number of packets sent by the source in point to point communication. More is the $trust\ level$ better is the link quality. Also the required energy for transmission also plays a significant role as it is directly concerned with the network lifetime. The link with less required transmission energy and a very good trust level can be considered a healthy link for the communication process. Healthy links can also become the causes of hotspots or energy holes, as the traffic flow is more on these links compared to the other ones.

As IoT network is a network of heterogeneous networks having different owners and different applicability, so the cooperation of the nodes from such different network may become a reason of headache. As the networks are resource constrained, it becomes tedious to allow other networks to use the resources of our network for relaying their data without any additional (monetary) advantage to us.

iii. End to end communication based: Path length in terms of number of hops or the overall energy requirement, incentive based cooperation between the relaying devices of the other networks, security in the communication process and identification of the alternate path in case of the regular path failure can affect the routing process.

Generally protocols searches the shortest path length based on the minimum number of hops on that path. But such path length may or may not serve the purpose. For that it is essential to search the path towards the destination based on the energy requirement. The less is the energy requirement for the transmission of the data the better is the path for the routing of data even though the path contains more number of hops than the other one which consumes more energy for the data transmission.

As the routing mechanism involves multiple networks of different owners, the security of data is always one of the crucial factors. Proper trust management between the different networks must be done.

VI. OPEN CHALLENGES FOR FUTURE RESEARCH

Routing data over a network made up from heterogeneous devices and diverse networking standards is a real challenge. The success of routing depends on various parameters. As the routing in IoT is at its preliminary stage, various obstacles yet to be faced by the researchers though the basic classification exists. Few of them are discussed in this section:

i. Context awareness: In IoT the devices are the actors. For smart routing it is essential to collect the context from the environment and analyze it for generating knowledge. This knowledge can be used for taking the routing decisions. Existing protocols are mainly using residual energy of the nodes as a parameter for context awareness but along with it memory of the node, its processing power and link quality can also be considered as the important parameters.

ii. Heterogeneity: IoT is an umbrella for bringing together various technologies. As there are various technologies, the heterogeneity can be in terms of devices and their networking standards. This heterogeneity adds additional complexity in the routing process. The existing protocols are having rigid boundaries. So it is essential to build a routing protocol that will incorporate all the types of heterogeneity in it.

iii. Death of nodes: Network may contain many energy constrained nodes. Unnecessary and over use of energy may result into its death. It is not possible to replace the batteries of dead nodes or physically replace these nodes due to their high density. Energy holes may get created due to the dead nodes which may create hurdles in the routing process as the relaying devices have short ranges.

iv. Topology changes: There are various reasons of topology changes such as constant mobility of the nodes, complete energy exhaustion of the nodes and environmental factors. The remedy over this problem can be to develop a reactive or hybrid routing protocol that will handle frequent topology changes in the network.

v. Scalability: Most of the technologies involved in IoT are wireless. The devices using these technologies may be stationary or mobile. The mobile devices may enter or leave the network, which may increase or reduce the size of the network. So the network scalability can affect the routing.

vi. Latency: The data generated in IoT may get expired due to that it is necessary to deliver the data to the destination within desired amount of time. So it is essential to handle the latency by the routing protocols for maintaining the service quality.

vii. Incentive based routing: In any type of communication there is a need of cooperation between two entities. As IoT contains heterogeneous devices, it is essential that these devices must cooperate with one another for making the routing successful. But the obvious question can be why should the resource constrained devices from other networks relay the data even though they do not have any direct benefit? Some researchers tried to find out the remedy on this problem by making the routing incentive based.

viii. Congestion control: Congestion is a problem in all types of networks. Due to the exponential increase of network traffic it became a complex phenomenon. Congestion occurs when the amount of traffic increases beyond the capacity of the network. Packet loss and unwanted delays are the results of congestion. For preventing congestion at a specific node it is necessary that routing protocol should do load balancing when the traffic increases at a specific node. Due to congestion, the nodes can become hotspots and if congestion persists for long time rapid depletion of node's energy may takes place which may result into reduction in network lifetime. So it is essential that the routing protocol should notify and try to overcome the congestion immediately and must take some precautionary steps for congestion avoidance also.

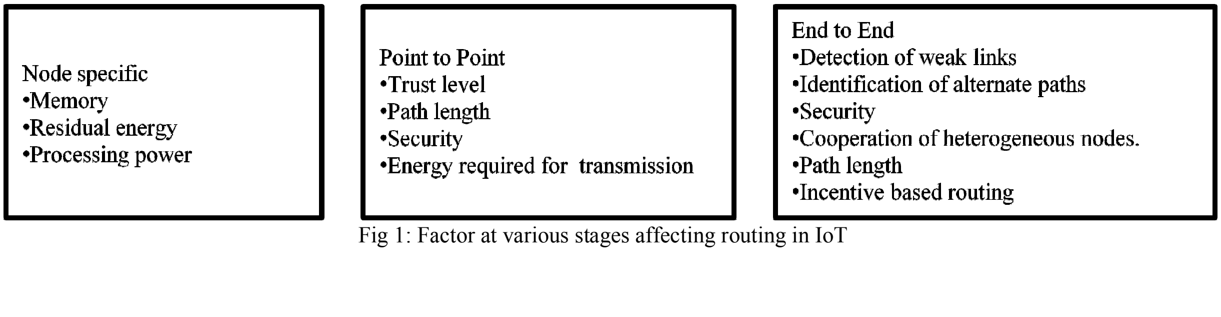
ix. Data security: As the data is routed through various networks having different owners, it is necessary to provide the security to the data for keeping the data intact. As most of the communication is wireless it makes snooping very easy. Authentication is important before making the connection between two devices for preventing data theft.

x. Elimination of data redundancies: IoT networks will generate tremendous amount of data and will send it to destination for further processing. So instead of handling and forwarding similar data repeatedly and wasting of network energy, it is essential to do data fusion for eliminating the data redundancies.

xi. Multipath routing: It is necessary for balancing the load and increasing the lifetime of the network. It will stop the exhaustive use of specific parent nodes and their fast energy depletion but it is also necessary to keep the topology reconfigurations in control. Less topology reconfigurations means less control packets and less control packet means less energy consumptions which ultimately results into increase in network lifetime. Along with load balancing, this technique may help to increase the fault tolerance, reliability and QoS improvement.

Table III
Parameter based comparison between IoT protocols

Protocol	**Context aware**	**Secure**	**Multihop routing**	**Supports dynamic topology**	**Incentive based**	**Considers Link quality**
AOMDV-IoT	No	No	Yes		No	No
SMRP	No	Yes	Yes		No	No
EARA	Yes	No	Yes		No	No
RPL	Yes	Yes	Yes	Yes	No	No
Multiparent routing in RPL	Yes	No	Yes	Yes	No	No
PAIR	Yes	No	Yes	Yes	Yes	No
REL	Yes	No	Yes		No	Yes



Node specific
•Memory
•Residual energy
•Processing power

Point to Point
•Trust level
•Path length
•Security
•Energy required for transmission

End to End
•Detection of weak links
•Identification of alternate paths
•Security
•Cooperation of heterogeneous nodes.
•Path length
•Incentive based routing

Fig 1: Factor at various stages affecting routing in IoT

VII. CONCLUSION

The internet has changed drastically over last few years. Due to the advancement in sensor hardware technology and availability of cheap hardware, now a days it become easy to attach sensors to all the objects around us so that these devices will communicate with each other without human interference. Understanding routing of sensor data as one of the main challenges that IoT would face, we have surveyed the most important aspects of routing in IoT with stress on what is being done and what are the issues that need to be addressed in the future research.

We discussed currently existing routing protocols based on various parameters; we tried to classify these protocols based on their network structure, protocol operation, maintaining routing information and network conditions. We also analyzed the importance of context-awareness and incentive based relaying mechanism in the routing process. We also discussed the factors affecting the routing process at various stages such as node specific, point to point and end to end.

At the end, we have stated the possible open challenges for future research which may be helpful to the researchers in forthcoming time.

We believe that, given the interest shown by the industries in the routing process of IoT, in the next few years addressing such issues will be a commanding driving force for research in routing in both industrial as well as academic laboratories.

REFERENCES

[1] Maria Rita Palattella, Nicola Accettura, Xavier Vilajosana, Thomas Watteyne, Alfredo Grieco, Gennaro Boggia, Mischa Dohler, “Standardized Protocol Stack for the Internet of (Important) Things”, IEEE Communications Surveys and Tutorials, IEEE, PP(99):1 –18, 2012. ISSN 1553-877X.

[2] Charith parera, Arkady Zaslavsky, Peter Christen, Dimitrios Georgakopoulos,"Context Aware Computing for The Internet of Things: A Survey", IEEE Communications Surveys and Tutorials, vol. 16, no. 1, pp. 414-454, First Quarter 2014

[3] Oladayo Bello, Sherali Zeadally, "Intelligent Device-to-Device Communication in the Internet of Things," Systems Journal, IEEE, Issue.99, pp.1-11, 2014. ISSN 1932-8184.

[4] Sharief M. A. Oteafy, Fadi M. Al-Turjman and Hossam S. Hassanein, “Pruned Adaptive Routing in the Heterogeneous Internet of Things”, Global Communications Conference (GLOBECOM), 2012 IEEE, pp. 214 – 219, ISSN 1930-529X.

[5] M. Weiser, R. Gold, “The Origins of Ubiquitous Computing Research at PARC in the late 1980s”, IBM Systems Journal (1999).

[6] Michael Frey, Friedrich Grose, Mesut Gunes, “Energy-aware Ant Routing in Wireless Multi-hop Networks”, IEEE International Conference on Communications (ICC), pp. 190-196, 2014.

[7] I. Carreras, D. Miorandi, G. S. Canright, and K. Engo-Monsen, “Understanding The Spread of Epidemics In Highly Mobile Networks,” in Proc. 1st IEEE/ACM Int. Conf. Bio-Inspired Models Netw., Inf. Comput. Syst.,Cavalese, Italy, pp. 1–8, 2006.

[8] E. De Poorter, I. Moerman, and P. Demeester, “Enabling Direct Connectivity Between Heterogeneous Objects In The Internet of Things Through a Network-service-oriented Architecture”, EURASIP J. Wireless Commun. Netw., vol. 2011, no. 61, pp. 1–14, Aug. 2011.

[9] Paul Loh Ruen Chze, Kan Siew Leong ,“A Secure Multi-Hop Routing for IoT Communication”, IEEE World Forum on Internet of Things (WF-IoT), 2014, pp. 428 – 432.

[10] Afergan, M. “Using Repeated Games to Design Incentive-based Routing Systems” In Proc. of the IEEE Int. Conf. on Computer Communication,(INFOCOM), Barcelona, Spain, 2006, pp. 1-13.

[11] G. Abowd, A. Dey, P. Brown, N. Davies, M. Smith, and P. Steggles, “Towards a Better Understanding of Context and Context-Awareness,” in Proc. Handheld Ubiquitous Comput., 1999, pp. 304–307.

[12] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic, Marimuthu Palaniswami, “Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions”, Future Generation Computer Systems 29 (2013), pp. 1645–1660

[13] W. Vogels, R. van Renesse, and K. Briman, “The Power of Epidemics: Robust Communication for Large-scale Distributed Systems,” ACM-SIGCOMM Computer Communication, vol. 33, no. 1, pp. 131–135, Jan. 2003.

[14] P. Bellavista, A. Corradi, M. Fanelli, and L. Foschini, “A survey of context data distribution for mobile ubiquitous systems,” ACM Computing Surveys, vol. xx, no. xx, p. 49, 2013.

[15] Yicong Tian, Rui HOU,“An Improved AOMDV Routing Protocol for Internet of Things”, International Conference on Computational Intelligence and Software Engineering (CiSE), 2010, pp. 1-4.

[16] T. Tsuchiya and T. Kikuno, “An Adaptive Mechanism for Epidemic Communication,” in Proc. 1st Int. Workshop Biologically Inspired Approaches Adv. Inf. Technol., Lausanne, Switzerland, 2004, pp. 306–316.

[17] Oana Iova, Fabrice Theoleyre, Thomas Noel, “Using Multiparent Routing in RPL to Increase The Stability and The Lifetime of The Network”, Ad Hoc Networks, Elsevier 2015, pp. 45-62.

[18] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, et al., “Internet of Things Strategic Research Agenda”,Chapter 2 in Internet of Things—Global Technological and Societal Trends, River Publishers, 2011, ISBN 978-87-92329-67-7

[19] K. Ashton, “That, ‘Internet of Things’ Thing In The Real World, Things Matter More Than Ideas”, RFID Journal, June 2009, http://www.rfidjournal.com/article/print/4986

[20] Carnot Institutes “Smart Networked Objects and Internet of Things”, Carnot Institutes’ Information Communication Technologies and Micro Nano Technologies alliance, White Paper, January 2011.

[21] L. Azori, A. Iera and G.Morabito, “The internet of Things: A Survey”, Computer Network, vol.54, no.15, pp. 2787-2805, Oct 2010.

[22] G. D. Abowd and E. D. Mynatt, “Charting past, present, and future research in ubiquitous computing,” ACM Trans. Comput.-Hum. Interact., vol. 7, pp. 29–58, March 2000.

[23] D. Le-Phuoc, A. Polleres, M. Hauswirth, G. Tummarello and C.Morbidoni, “Rapid Prototyping of Semantic Mash-ups Through Semantic Web Pipes”, in proc. 18th international conference on World wide web, ser. WWW 2009. ACM, 2009, pp. 581-590.

[24] INFSO D.4 Networked Enterprise RFID INFSO G.2 Micro Nanosystems in Co-operation with the Working Group RFID of the ETP EPOSS, “Internet of Things in 2020, Roadmap for future, Version 1.1”, European Commission, Information Society and Media, Tech. Rep., May 2008.

[25] T. Lu and W. Neng, “Future Internet: The internet of things”, in 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), vol. 5, August 2010, pp. V5-376-V5-380.

[26] European Commission, “Internet of Things in 2020 Road Map for The Future”, Working Group RFID of the ETP EPOSS, Tech. Rep., May2008,

[27] P. Guillemin and P. Friess, “Internet of Things Strategic Research Roadmap”, The Cluster of European Research Projects, Tech. Rep., September 2009.

[28] H.Sundmaeker, P. Guillemin, P. Friess, S.Woelffle, “Vision and Challenges for Realizing The Internet of Things”, The Cluster of European Research Projects on the Internet of Things-CERP IoT, 2010.