Pruned Adaptive Routing in the Heterogeneous Internet of Things

Sharief M. A. Oteafy, Fadi M. Al-Turjman and Hossam S. Hassanein
School of Computing
Queen's University
Kingston, Ontario, Canada
{ oteafy | fadi | hossam }@cs.queensu.ca

Abstract— **Recent research endeavours are capitalizing on state of the art technologies to build a scalable Internet of Things (IoT). Envisioned as a technology to integrate the best of Wireless Sensor Networks and RFID systems, there is much promise for a global network of objects that are identifiable, track-able, and harmoniously informing. However, the realization of an IoT framework is hindered by many factors, the most pressing of which is attributed to the integration of these heterogeneous nodes and devices. A considerable subset of these nodes undergoes movement and dynamically enters and leaves the network backbone/topology. Routing packets and inter-nodal communication has received little attention; mainly due to the sheer reliance on the Internet as a backbone. However, spatially correlated entities in the IoT, and those which most often interact, would pose a significant overhead of communication if all intermediate packets need to be routed over distant backhauls. In remedy, we present a Pruned Adaptive IoT Routing (PAIR) protocol that selectively establishes routes of communication between IoT nodes. Since nodes in the IoT belong to different owners, we also introduce a pricing model to cater for the exchange of monetary costs by intermediate nodes to utilize their relaying resources. We also establish a cap on inter-nodal routing to dynamically utilize the Internet backbone if the source to destination distance surpasses a preset (case optimized) threshold. The PAIR routing protocol is elaborated upon, building upon the detailed system model presented in this paper. We finally present a use case to demonstrate the utility and practicality of PAIR in the heterogeneous IoT as it scales.**

Keywords- Internet of things, Dynamic routing, Pricing model, Heterogeneous communication.

I. INTRODUCTION

The Internet of Things (IoT) is growing as a framework to encompass all identifiable things, in a dynamic and interacting network. The promise of intelligent protocols and dynamic systems that could benefit from the aggregation and analysis of information over the IoT infrastructure is quite omnipresent. Researchers in communications, R&D divisions and many businesses are in the race to develop an attainable and resilient architecture to realize the IoT [1].

However, many obstacles render the IoT framework mostly a mere vision. To date, much has been presented on the promise and benefits of IoT, yet far less has covered the protocols to actually operate such a large scale and dynamic architecture [2]. The vision, however sparse, promises a resilient and dynamic framework to integrate many enabling technologies that already exceled in research and development.

Prominently, Wireless Sensor Networks (WSNs) are envisioned to play a dominant role in IoT frameworks. The resilience, autonomous and energy efficient traits of WSNs render them a vital candidate for dominating the information collection task of an IoT framework [3]. As a technology, much advancement has been seen both in research and actual deployments. However, major issues with large scale operation, dedicated and tailored designs (application specific) and stringent energy requirements (hence limited capabilities) deem WSN in need of much research to incorporate in IoT.

Equally vital, the use of RFID technologies for non-LOS and seamless identification of objects is gaining much prominence as a key player in IoT [4]. The low cost associated with deploying RFID tags (passive, semi-passive or even active) is an important motivation. Moreover, the ability to interrogate multiple tags in concurrency and utilizing multiple readers to increase the capacity of interrogation is a major reason for its envisioned adoption in the IoT. In fact, some argue that RFIDs have been a main motivator for the IoT [4].

The integration of these enabling technologies, along with Internet based and context aware services facilitate a dynamic platform for the IoT. However, much of current research has focused on developing these technologies in isolation, and optimizing performance under local constraints and goals. The bigger picture, encompassing the interplay of IoT components as a whole remains a subject of much sparseness.

One of the most important tasks to be carried out, in such a large scale and dynamic environment, is relaying information from a source to a destination, given the new metrics present in the IoT. Typical routing protocols mostly consider that all components belong to the same network, hence routing costs and link weights are directly proportional to their local characteristics (i.e. load, buffer capacity, residual energy, etc). This applies to other control protocols such as medium access control (MAC). However, in the IoT routing becomes inherently complex by multiple factors. First and foremost, most entities participating in sensing, identification and relaying belong to different networks with multiple owners. It is not in the best interest of such networks to allow their resources to be utilized for relaying data without compensation.

Our contribution in this paper is two-fold. First, presenting a routing protocol tailored for the diverse IoT components, with heterogeneous components and limitations. This is only possible with our second contribution, a pricing model which caters for the diverse requirements and conditions of nodes

978-1-4673-0921-9/12/$31.00 ©2012 IEEE

willing to relay IoT packets without using the Internet backbone. The utility function presented here incorporates measures of load balancing, buffer space and link maintenance. An overview of the routing problem and the dynamic constituents of the envisioned IoT is depicted in Fig 1.

We present our model in this paper as follows. Section II will cover the background on routing IoT, and its basis in the underlying enabling technologies. This is followed by a rigorous definition of our proposed network model, manifesting the interactions of components in the IoT, and their governing constraints. Built on those, we formally present the routing protocols in Section IV and elaborate on the algorithms and message exchange. Our proposed model is verified in Section V and presented with the aid of a use case. We conclude in Section VI.

II. Background and Motivation

The race for realizing a feasible framework for the IoT is gaining momentum. In fact, isolated improvements and performance gains in the enabling technologies of the IoT (especially WSNs and RFIDs) are generating a significant drive for further investigations into their integration and large scale adoption. To present a perspective on the enabling technologies, and the major domains of difference in properties, Table I contrasts the properties of three main paradigms to the IoT.

In this section, we highlight two major drives. First, the lack of a distinctive routing protocol that caters for dynamic IoT components, and the implications of utilizing heritage routing schemes. The second drive lies in the tradeoff costs of routing over multiple entities, belonging to different networks.

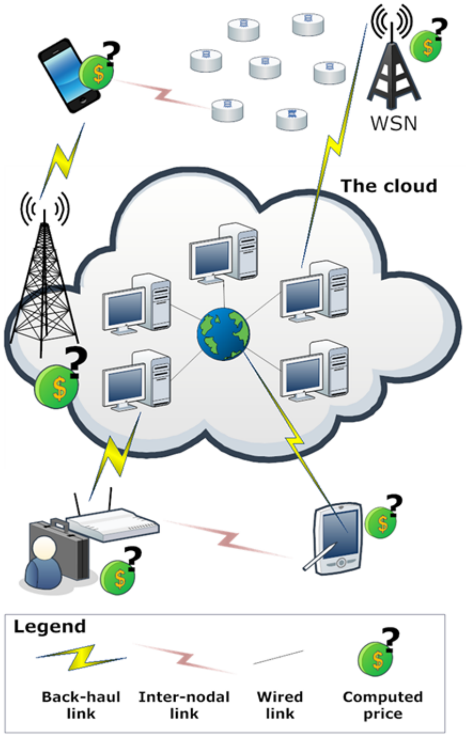

Figure 1. An overview of cross-network routing in the IoT and the pricing requirement imposed by heterogeneous nodes

A. Routing in the Internet of Things

A major misconception was imposed by an inherent property of the IoT; namely being a descendent of the Internet. That is, as research on the IoT developed, it was expected that a significant pool of protocols previously developed for Internet services would migrate into the IoT. However, as the IoT is set to encompass many stationary (access points, backhauls, static WSNs, RFID readers, etc) and dynamic (laptops, PDAs, cell phones, etc) components, we are challenged with multiple issues [5]. Most prominently, assuming that all components will inter-communicate via backhaul access (i.e. via the Internet) is insufficient and often degrading to performance.

A major hindrance would stem from the mounting number of messages that overload a network already handling millions of hosts. This is a significant problem as recent endeavours are targeting higher levels of dynamic interaction between the IoT and its users, as in the Human Computer Interaction (HCI) work presented by Kranz *et al* in [6]. As such, if a WSN needs to identify an object, with the aid of an RFID reader, direct communication between a sensing node (SN) and the reader would leverage bottlenecks of communication and swarming the backhaul over the Internet with numerous data packets. This is an eminent architecture, one that is strongly pushed for as a truly integrating IoT [7].

B. Routing tradeoffs

There is a need for establishing a cooperative scheme for routing in the IoT; one which includes all nodes with capabilities of relaying data. This includes those with only one access medium (e.g. WiFi routers) and others with multiple mediums (e.g. cell phones). However, due to obvious reasons of resource conservation, such entities would not participate in relaying data packets unless there is an incentive [8]. It is important to note that some components only generate data, such as RFID tags.

Different incentives take part in the pricing model that dictates the choice of a group of candidates for relaying. Recent results in incentive based routing have been well studied. Zhong *et al* present an elaborate study on routing and forwarding in Mobile Ad hoc Networks (MANets), by emphasizing a scheme that ensures optimal gain for the individual nodes [9].

Other schemes have been presented to incorporate dynamic game theory models, for non-cooperative scenarios where local utility functions dictate the participation of nodes in relaying [10]. It is important to note as well that many of such factors are non-trivial to compute, and many nodes in the IoT would not possess the computational capacity to compute and execute local utility functions. Thus, it is intuitive to pursue a game theoretic approach for the IoT only if it caters for offloading the task of computing local utility functions to nearby high-end nodes.

Other problems stem from scalability issues in IoT, being an architecture that is envisioned to span continents and the globe [11]. The major issue is being able to maintain end-to-end links, and keeping track of nodes that are dynamically entering and exiting from the network. Remedies have been

TABLE I. IoT ENABLERS AND THEIR PROPERTIES IN CONTRAST

Property	***Wireless Networks***			
	IoT	***MANets***	***WSNs***	***RFIDs***
Computational power per node	Varies	High	Low	Low to none [a]
Typical density	Very high	Small to medium	Medium to high	Medium to high
Topology	Dynamic	Dynamic [b]	Mostly static	Application dependent
Communication range	Varies	High	Medium (varies)	Reader dependent
Buffer size	Varies	High	Low	None
Medium contention	High	High	Medium	Low with singulation
Mobility	Frequent	Varies [b]	Limited	Frequent
Inter-node communication	Heterogen-eous	Homogeneous		

[a] disregarding active-tags, as they equate many features of sensing nodes

[b] since Manets typically encompass VANets as well

proposed by increasing the density of backhaul connections and multiple readers to enhance connectivity and capacity, respectively. However, recent studies highlighted the degrading effect of inter-reader and relay collisions. Ali *et al* introduced a redundant reader elimination scheme to optimize tag coverage yet limit reader-to-reader contention; in addition to reducing the costs of deployment [12]. Many other factors take part in the pricing scheme, but we only focus on the factors highlighted in Section III.

III. IoT System Model

Many factors are intrinsically dominant in the operation of a routing protocol. More factors are further augmented as we devise a routing protocol for the IoT with dynamic topologies in place. Thus, it is the scope of this section to detail and elaborate upon the factors that are considered in this protocol. No single protocol would achieve all objectives, as many objectives are inherently contradictory, thus routing belongs to the notorious NFL (no free lunch) class of algorithms.

Our system is presented in the remainder of this section and elaborated upon in four components. First we present the IoT network as a whole, elaborating on the description of heterogeneous nodes in this model. Each of the resources pertaining to these nodes, and affecting the relaying scheme, are discussed in the following subsection. The discussion is completed with a derivation for the utility functions that would govern the choice of nodes, and finally the types of messages exchanged in the routing scheme to optimize upon the resources and residual energy in these nodes.

A. IoT network Model – a heterogenous approach

We assume a network of heterogeneous devices, those belonging to WSNs, MANets, RFIDs and stationary and mobile devices. Each communicating entity of these devices (i.e. wired/wirelessly enabled device) is considered as an active node in this design; hereon referred to as a node. Thus, given a set $\boldsymbol{N}$ covering all these devices, we represent each node as $\boldsymbol{n_i} \in \boldsymbol{N}$ where $\boldsymbol{i} = \{1,2,\cdots,|\boldsymbol{N}|\}$. Thus the set N includes both nodes that are sole relays (access points, routers, WSN sinks, etc) and other devices with relaying capabilities (communication and processing).

We assume each $\boldsymbol{n_i}$ is connected to the network, as disconnected nodes would not take part in this scheme. i.e. if there's no link from a node $\boldsymbol{n_j}$ to some other node $\boldsymbol{n_i} \in \boldsymbol{N}$ then $\boldsymbol{n_j} \notin \boldsymbol{N}$. It is important to note that the size of N varies over time as nodes enter, leave, run out of energy and are re-introduced to the network.

Connectivity between nodes is assumed to take one of two modes. If nodes are in close proximity, then we advocate for direct communication between the nodes without re-routing through the Internet (via a backhaul). However, to sustain the important large scale aspect of the envisioned IoT, we dictate that packets travelling over a threshold of hops $\boldsymbol{\delta}$, would be routed through a backhaul as an intermediate stage, and then re-routed to the final destination from the closest backhaul to that destination. It is thus an important factor to cater for both short and long range communication between nodes, both directly or via the Internet backbone.

We iterate the importance of adhering to a scheme that utilizes the Internet backbone only when necessary, and re-route spatially correlated data packets between neighboring nodes without loading the backbone.

B. Node representation

Each node $\boldsymbol{n_i} \in \boldsymbol{N}$ takes part in relaying, as well as other tasks. Accordingly, each $\boldsymbol{n_i}$ encompasses a group of resources, with a minimum of communication and processing units. Moreover, in the case of cell phones, PDAs, WSN sinks and RFID readers, they would all encompass a larger pool of resources, not necessarily geared towards the routing task.

Thus, it is important to consider how the load of performing these tasks could affect/hinder the relaying capabilities of such nodes. We note their existence but in this scope we account for their effect on residual energy and buffer capacity. Fig 2 depicts the main components considered in the utility function of a node $\boldsymbol{n_i}$.

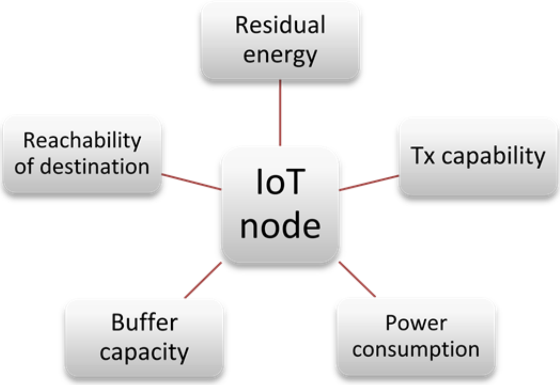

Figure 2. The resources incorporated in the pricing model for computing a utility function. i.e. the nodes involved in relaying data packets in the heterogeneous IoT

A quintuple $\mathbf{\Psi_i}$ is computed for each $\boldsymbol{n_i} \in \boldsymbol{N}$ aggregating the following parameters, for both their direct and implied effect on the routing scheme:

1) Residual energy and power consumption

Each node operating on battery power would possess an energy reservoir, denoted by $\boldsymbol{e_i}$ where $0 \leq e_i \leq E_i$. Here we denote $\boldsymbol{E_i}$ as the maximum charge for n_i, since this varies across the different types of nodes.

To normalize this representation across the heterogeneous nodes in this protocol, we define

$$\acute{e}_\iota = \frac{e_i}{E_i} \tag{1}$$

Knowing the size of data packet $\mathbf{D_k}$ to be forwarded, its distance to its next hop and the current load (u_i), each node would compute a value for the power consumption to be incurred by processing a given packet. The power consumption would be represented as $\boldsymbol{\pi_i}$.

However, since this is a crude number dependent on the available resources at node n_i and their strength (of transceiver), this value is normalized by dividing by its maximal attainable load and transmission distance. This would favor high end nodes with longer transmission capabilities and more buffers. The normalized value is represented as $\boldsymbol{\acute{\pi}_\iota}$.

2) Current load and buffer space

Since an intermediate node might be taking part in multiple tasks, each node will represent its available capacity to compute and relay a message as a utilization factor $\boldsymbol{u_i}$, which will be normalized by contrasting it to its maximal capacity, thus yielding a normalized $\boldsymbol{\acute{u}_\iota}$. This is directly derived from memory and processing operations, and the yield of the node's MCU in handling different traffic paths.

3) Distance to neighbor

It would not suffice to consider only the number of hops as a measure of energy spent in transmission. That is, transmission power is directly proportional to the distance required for transmission, and as it increases the power required increases in multiple folds. A simple model to represent such transmission expenditure ($\boldsymbol{E_{Tx}}$ for transmitting and $\boldsymbol{E_{Rx}}$ for receiving) over distance $\boldsymbol{d}$ meters is presented by the Friss-free space model (adopted from [13]) as:

$$E_{Tx}(k, d) = k * \left(E_{elec} + d^{\theta} * E_{amp}\right) \tag{2}$$

$$E_{Rx}(k) = k * \; E_{elec} \tag{3}$$

where $\boldsymbol{k}$ is the number of bits in the transmitted packet, with a path loss exponent of θ usually in the [2,4] range.

C. Utility functions (pricing)

All the previous factors are pertaining to nodal resources and their operation levels, in contrast to the remaining energy each node could support. However, an important aspect to cater for, and possibly arbitrate upon, is the price the nodes are going to charge for relaying a given data packet. That is, since the heterogeneous nodes in the IoT system do not belong to the same network nor the same owner, it is imperative that a monetary cost would be associated with the forwarding action.

This is an important aspect for integrating multiple heterogeneous nodes in the architecture and enhancing global scalability. The argument for utilizing current resources with a given cost is more dominant than claims of deploying enough resources to cater for all connectivity and coverage tasks of the envisioned IoT. We adopt and build upon this argument.

We hereby introduce a pricing factor for each node, denoted by $\boldsymbol{\gamma_i}$. This is a factor that could be set as a flat rate per number of bytes transmitted, or computed based on the state of the current resources at node $\boldsymbol{n_i}$ represented by $\mathbf{\Psi_i}$. In this work we adopt the latter, as a proof of concept to the monetary exchange for forwarding in the IoT under varying conditions. Thus, we denote the price charged by each node $\boldsymbol{n_i}$ as $\boldsymbol{p_i}$:

$$p_i = \gamma_i * \left[\frac{E_{Tx}\left(D_k, n_j\right) + E_{Rx}(D_k)}{e_i} + \boldsymbol{\acute{\pi}_i} + \boldsymbol{\acute{u}_i}\right] \tag{4}$$

It is intuitive to note that owners of nodes in the vicinity of such a network, may choose to adaptively contribute or withdraw from the topology by varying the value assigned to γ_i. i.e. setting it to a relatively high value would diminish the chances of it being selected for relaying.

IV. PAIR ROUTING APPROACH

The integrated architecture imposed by the heterogeneity of the IoT demands a scalable and inclusive routing protocol. The latter property refers to exploiting different relaying resources able to forward a data packet towards the destination. This section presents our Pruned Adaptive Routing in the heterogeneous Internet of things (PAIR) protocol. The IoT topology is assumed to connect a large number of nodes.

PAIR is divided into two stages: forward and backward. The forward stage starts at the source node by broadcasting setup messages to its neighbors. A setup message includes the cost seen from the source to the current (intermediate/destination) node. A node that receives a setup message will forward it in the same manner to its neighbors after updating the cost based on the values computed in $\mathbf{\Psi_i}$. All setup messages are assumed to contain a route record that includes all node's IDs used in establishing the path fragment from the source node to the current intermediate node. The destination collects arriving setup messages within a Route-Select (RS) period, which is a predefined user parameter.

The backward stage starts when an Acknowledgment (Ack) message is sent backward to the source along the best selected path (called **active** path) in terms of the parameters passed in $\mathbf{\Psi_i}$. If a link on the selected path breaks (due to node movement or bad channel quality), the Ack at an intermediate node *i* is changed to setup message (called i_setup) and forwarded to neighbors of *i* which has discovered the error. Once the source receives i_setup, the active path between S and D is established. When no breaks are discovered, the source receives an Ack and it knows that the path has been established, and it starts transmission.

If during the communication session (i.e., after selecting the active path) a break is detected, the intermediate node detecting the break will send data on an alternative route (if any) or it will buffer data and send an i_setup message to the destination to look for an alternative path.

In general, nodes track their neighbors and update the Routing Table (RT) either by receiving a broadcasted setup message and accordingly update its neighborhood table, or by broadcasting a "*hello*" message periodically, if no messages have been exchanged. This hello message is sent only to the neighborhood of the node. A new neighbor introduced, or failing to receive from a node for two consecutive hello periods, is an indication that local connectivity has changed.

A pseudo code description of the source node algorithm is shown below. Lines 1-2 represents the beginning of the forward stage, where a request to establish an active path is initiated. Such that, if S has new packets to send and no route is known to targeted destination D, then a setup message is forwarded to all available neighbors of S. Lines 3-4 indicate that the path has been found.

Hence, active path between S and D is updated and source begins transmitting the new data packets. Lines 5-6 describe the case where a Route Discovery (RD) period is expired. Therefore, the source restarts the route discovery process by sending a new setup message. Finally, lines 7-8 indicate that S has not exchanged messages with neighbors for more than *hello_interval* time units. Thus a hello message is sent and RT is updated accordingly.

Algorithm 1: For Source node S.

```
1. If S has a new data msg & no route to D
2. Then forward a setup msg.
3. If S receives D_Ack or i_setup msg,
4. Then check local $p_i$ and send the new data msg's if
   satisfied.
5. If S doesn't receive a response for a RD period,
6. Then go to line 2.
7. If no pkts are exchanged for hello_interval time units,
8. Then send a hello msg and update RT and $p_i$.
```

Algorithm 2: For intermediate node *i*.

```
1. If i receives setup msg,
2. Then check thresholds and update/forward setup msg if
   satisfied. Also, the forwarded setup msg records visited
   nodes while traveling to D.
3. If i receives D_ Ack
4. Then, If a backward_neighbor is reachable,
5. Then forward the D_Ack
6. If backward_neighbor is not reachable,
7. Then send i_setup msg & update RT and local $p_i$.
8. If i receives i_setup msg
9. Then check thresholds and update/forward i_setup msg
   if satisfied. Also, the forwarded i_setup msg records
   visited nodes while traveling to destination.
10. If i receives data msg
11.   If next hop is still reachable
12. Then send data
13. If a new active path was established
14. Then check the price, update RT and send data if
    satisfied.
15. Else buffer data and send i_setup
```

A pseudo code description of the intermediate node algorithm is shown in Alg. 2. Lines 1-2 handle the forward stage, such that if an intermediate node *i* receives a setup message, it forwards this message to all its unvisited neighbors and records every visited node to establish a backward path. Contrarily, lines 3-7 handle the backward stage of the algorithm. If node *i* receives Ack from destination (called D_Ack), then it checks whether the neighbor towards S on the backward path is reachable or not (i.e. has a broken link). If reachable, it passes the D_Ack to this neighbor and records the necessary information to establish the active path. Otherwise, it initiates a new setup process between *i* and S, by sending i_setup message to *i*'s neighbors. Lines 8-9 keep forwarding this i_setup message until it reaches S to establish an active path between *i* and S instead of the broken one.

Similarly, lines 10-12 check for the availability of the next hop on the active path while data packets are transmitted through *i* towards the destination D. If next hop is not available, the intermediate node *i* checks for an alternative path. If a new path has been established, lines 13-14 detour the Data packets between S and D along this new partial route and update the active path. If no alternative path is found, line 15 buffers the data packets and initiate a new setup process. We remark that lines 2 and 9 will kill any setup message, if $\boldsymbol{n_i}$ is not willing to participate in routing.

Finally, a pseudo-code describing the actions at destination node D is shown in Alg. 3. Lines 1-10 handle the case when a setup process has been initiated by an intermediate node *i*. This also indicates link breakage at node *i* in active path between S and D. If there exist alternative path(s) passing through the node detecting link breakage (i.e., node *i*) or passing through the source S, lines 3-4 select the best-cost path and notify *i*. Otherwise, lines 5-10 initiate a new setup process and act as a source node in looking for a new path to S. Therefore, it sends to all D's neighbors and waits for an Ack from the source S (called S_Ack). Meanwhile, lines 11-14 represent the backward stage in response to the forward stage that has been initiated at S. The destination D keep receiving setup messages with the corresponding found paths between S and D for a Route Select (RS) interval. After RS time units, D acknowledges the source S that the active path has been established by sending a D_Ack message to it through the best-cost selected path.

Algorithm 3: For Destination node D.

```
1. If D receives i_setup
2. Then remove paths containing broken links.
3. If there exist path(s) passing through i or S
4. Then select best-cost path and notify i.
5. If no paths found
6. Then send a setup msg
7. If D receives S_Ack or i_setup
8. Then select path indicated by received msg.
9. If D doesn't receive a response for a RD period,
10. Then go to line 5.
11. If D receives setup msg RS not expired
12. Then store the candidate path and cost.
13. If RS expired
14. Then select best-cost path and send D_Ack on it.
```

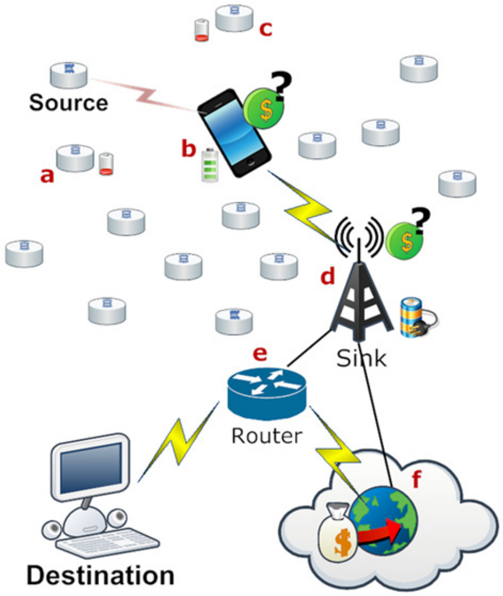

Figure 3. Use case: Routing paths taken by intermediate nodes from the source (SN node) to destination (remote computer)

V. Use Case

To demonstrate the utility of the PAIR protocol, we hereby adopt a use case that utilizes heterogeneous nodes in a sample IoT environment. The remainder of this use case will refer to Fig 3. A sensing node (the source) has obtained information to be sent to a destination computer. However, no direct link connects both devices, and intermediate devices belong to different networks. We assume that nodes ***a*, *b*, *c*, *d*, *e* & *f*** are willing to relay, yet ***a* & *c*** are already depleted in energy. The sink, node ***d***, is electrically powered and acts as an intermediate node between the resourceful cell phone ***b*** and the router ***e***.

PAIR will initiate a setup message sent to ***a*, *b*, *c***, its current neighbors. Since ***a* & *c*** have depleted batteries, they will terminate the flow of the setup request towards the destination. Since the cell phone ***b*** is in range of communication to the source, it will forward the message to its neighbors (not highlighted here as the pattern is clear). Eventually the shortest path to the destination is established. The destination will receive two streams $\{S \rightarrow b \rightarrow d \rightarrow e \rightarrow D\}$ and $\{S \rightarrow b \rightarrow d \rightarrow f \rightarrow e \rightarrow D\}$. Since both f and e are resourceful entities, the arbitration of number of hops would manifest a preference for the former route, which will carry an Ack message back to the source node. It is important to note that an Internet link (both forward and backward), which would also incur a cost, takes part in the route options, as the setup message would also parse through it when it is beyond the preset threshold of hops dictated by the application and source request.

VI. Conclusions

The envisioned IoT is to form an umbrella of multiple technologies, all to harmoniously integrate and operate efficiently. Many factors have hindered the realization of the IoT, most prominently the voids existing in the integration of its enabling technologies. Both WSNs and RFID systems are deemed critical enablers and players in the development and realization of a feasible, scalable and truly dynamic IoT. However, these systems are inherently application specific, and their current state of the art fails to integrate on a global scale.

One of the prominent issues is the ability to route information across the heterogeneous nodes of the IoT, especially with multiple owners. Hence, we presented an adaptive routing protocol –PAIR– that prunes request messages propagating across the nodes in the IoT, to allow the source-destination pair to utilize the most beneficial route based on tunable cost metrics. Accordingly, intermediate nodes are also encouraged to participate in relaying messages by integrating a monetary gain, dictated by a utility function tailored to each node's resources. Our model establishes contributions both as a heterogeneous routing protocol for the IoT, which capitalizes on incentives and cost functions to capitalize on the abundance of relaying resources in the IoT.

Acknowledgment

This research is funded by a grant from the Ontario Ministry of Economic Development and Innovation under the Ontario Research Fund-Research Excellence (ORF-RE) program.

References

[1] Al-Turjman, F.; Alfagih, A. & Hassanein, H. "A Novel Cost-Effective Architecture and Deployment Strategy for Integrated RFID and WSN Systems", *In Proc. of the IEEE Int. Conf. on Computing, Networking and Communications (ICNC),* Maui, Hawaii, 2012, pp. 835-839.

[2] Atzori, L., Iera, A. and Morabito, G. "The internet of things: A survey Computer Networks", *Computer Networks*, *Elsevier,* vol. 54, 2010.

[3] Zhu, Q.; Wang, R.; Chen, Q.; Liu, Y. & Qin, W. "IOT Gateway: Bridging Wireless Sensor Networks into Internet of Things", *In Proc. of the IEEE/IFIP Int. Conf. on Embedded and Ubiquitous Computing (EUC*), Hong Kong, China, 2010, pp.347-352.

[4] Welbourne, E.; Battle, L.; Cole, G.; Gould, K.; Rector, K.; Raymer, S.; Balazinska, M. & Borriello, G. "Building the Internet of Things Using RFID: The RFID Ecosystem Experience", *Internet Computing, IEEE*, vol. 13, pp. 48 -55, 2009.

[5] Vermesan, O.; Friess, P.; Guillemin, P.; Gusmeroli, S.; Sundmaeker, H.; Bassi, A.; Jubert, I.; Mazura, M.; Harrison, M.; Eisenhauer M,, "Internet of things strategic research roadmap" *Internet of Things: Global Technological and Societal Trends*, 2009.

[6] Kranz, M.; Holleis, P. & Schmidt, A. "Embedded interaction: Interacting with the internet of things" *Internet Computing*, *IEEE,* vol.. 14, 2010.

[7] Sarma, A. and GirÃo, J. "Identities in the Future Internet of Things" *Wireless Personal Communications*, *Springer Netherlands*, vol. 49, pp 353-363, 2009.

[8] 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.

[9] Zhong, S.; Li, L.; Liu, Y. & Yang, Y. "On designing incentive-compatible routing and forwarding protocols in wireless ad-hoc networks", *Wireless networks*, vol. 13, no. 9, pp. 799-816, 2007.

[10] Saad, W.; Han, Z.; Debbah, M.; Hjorungnes, A. & Basar, T. "Coalitional game theory for communication networks", *Signal Processing Magazine, IEEE*, vol 26, pp.77-97, 2009.

[11] Sundmaeker, H.; Guillemin, P.; Friess, P. & Woelfflé, S. "Vision and challenges for realising the Internet of Things", *CERP-IoT, European Commission*, Luxembourg, 2010.

[12] Ali, K..; Hassanein, H. & Alsalih, W. "Using neighbor and tag estimations for redundant reader eliminations in RFID networks", *In IEEE Wireless Comm.& Net. Conf. (WCNC)*, 2011, pp. 832-837.

[13] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "Energy-efficient communication protocols for wireless microsensor networks," *In Proc. of Hawaiian Int. Conf. on Systems Sci*, 2000, pp. 2-10.