Network Self-Organization in the Internet of Things

Arjun P. Athreya and Patrick Tague
Wireless Network and System Security Group
Carnegie Mellon University, USA
{arjuna, tague}@cmu.edu

***Abstract*—The Internet of Things is a paradigm that allows the interaction of ubiquitous devices through a network to achieve common goals. This paradigm like any man-made infrastructure is subject to disasters, outages and other adversarial conditions. Under these situations provisioned communications fail, rendering this paradigm with little or no use. Hence, network self-organization among these devices is needed to allow for communication resilience. This paper presents a survey of related work in the area of self-organization and discusses future research opportunities and challenges for self-organization in the Internet of Things. We begin this paper with a system perspective of the Internet of Things. We then identify and describe the key components of self-organization in the Internet of Things and discuss enabling technologies. Finally we discuss possible tailoring of prior work of other related applications to suit the needs of self-organization in the Internet of Things paradigm.**

I. Introduction

Almost every device around us today supports some form of computation and communication technology. These devices to name a few such as mobile phones, sensors, measurement devices and laptops today are part of our daily life. The immediate future of these devices is that they will interact with each other through a network such as the internet. The interaction among these devices allow them to achieve common goals [1]. Such an eco-system or a paradigm is called the *Internet of Things* (IoT), the devices being referred to as the *things*. From this definition of the IoT, we learn that the IoT is a heterogeneous system. Heterogeneity not only from the perspective of computation capabilities, but also the communication capabilities. Hence a smooth integration of these devices and their services into one networked system is still an open problem.

The IoT are expected to be part of many independently existing systems and the devices of different systems in IoT are expected to interact with each other as shown in Figure 1. Some examples of this interaction are enumerated below.

1) Temperature and humidity sensors in a home along with heart monitoring devices on a human connected to the internet and provide real-time logs to a remote cardiology specialist for remote health monitoring.
2) Energy monitoring sensors on solar panels communicate to the smart grid operator via a smart meter to maximize utilization of green energy resources.
3) Vehicular motion sensors on highways can help department of transportation inform users of possible bottlenecks to avoid long back-ups and reduce travel times.

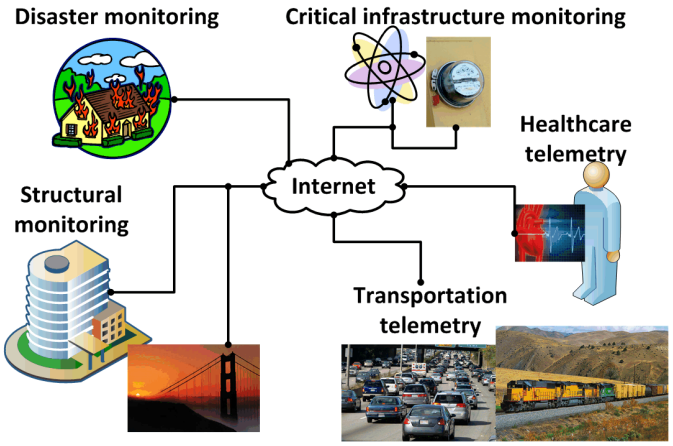

Fig. 1: This figure shows the Internet of Things eco-system. The eco-system consists of different deployment environments and their devices connecting to the internet. It is possible for devices of different environments to interact with each other.

While efforts are on to standardize the interactions of devices in the IoT, it is equally important to understand the need for data from these devices during times of disasters, outages and adversities from cyber-physical attacks. These examples of distressed times are a reality. During these times, provisioned communications and energy sources could fail and thereby do not allow to realize the full benefits and potential of the IoT. Thus even if devices survive during these conditions, lack of communication support could render data on these devices of little relevance. Hence, this motivates the need for self-organization in communication networks of the IoT. Self-organization is a process of bootstrapping communications among devices in a network after the provisioned communications have failed.

Self-organization in the IoT has several benefits, including the following,

1) Network availability to support IoT applications even during distressed times means that the common goal of interaction among devices will still continue to hold good.
2) Data from these devices during the times of distress allow for monitoring the environment's functioning and allow for command and control operations.
3) Prevent cascading effects of other environments failing if the data from current distress environments can reach in a timely manner for troubleshooting.

While the benefits of self-organization are huge and en-

978-1-4673-3122-7/13/$31.00 ©2013 IEEE

couraging, challenges in self-organization are bigger making this an exciting research problem. The aim of this paper is to survey prior work on self-organization in other relevant research areas and discuss future research opportunities for network self-organization by describing key components of self-organization and their challenges in the IoT. We start the discussion of challenges by first treating the IoT as one system. Our perspective of IoT as one large and distributed system stems from the fact that there exists heterogeneity in IoT and comprises multiple interconnected networks. This perspective is important because self-organization designs need to be cognizant of the operational constraints and protocols of devices across the various interconnected networks in the IoT. We then discuss key components of self-organization in the context of network disruptions and their challenges. We also describe possible solution framework to those challenges or improvements to existing scientific results that will benefit self-organization in the IoT paradigm.

We illustrate and describe the key components of self-organization in the IoT. *Neighbor discovery* is the process of discovering available peer devices to support and initiate communications during self-organization. *Medium access control* deals with minimizing collisions in medium access as this directly impacts network performance and the overall system's performance. *Local connectivity and path establishment* discusses the ways in which establishing peer connectivity can lead to end-to-end path establishment allowing for connectivity in the self-organized network. *Service recovery management* is the process of recovering from local failures of devices and avoiding network service disruptions in the self-organized network. Finally, *energy management* is the mechanism of load-balancing data forwarding responsibilities in the self-organized network and also the processes involved in reducing energy consumption in the battery operated devices.

We discuss future research opportunities in network self-organization in the IoT. With a system perspective of the IoT , we envision that a cross-layer approach towards self-organization could lead to the design efficient and robust algorithms. A self-organized network comprising heterogeneous devices could support heterogeneity in network service models too, thereby needing real-time network intelligence to make decisions on boundaries of different network services. Radio functionality such as cognitive radios on devices in the IoT could directly impact the self-organization process. Hence the extent and deployment strategies for such expensive radio enabled devices needs to be explored. In times of self-organization, on-board energy conservation will be a concern. Hence, low-power algorithm and architecture design is vital to longevity and scalability in the self-organized networks. Finally, with self-organized networks being restricted in scale either due to energy or information capacity limits, end-to-end connectivity cannot always be guaranteed. Hence, such discretely formed self-organized networks could serve as a platform for delay tolerant network aided by unmanned aerial vehicles. Thus localization techniques to find all self-organized networks for data collection needs to be explored.

The remainder of this paper is organized as follows. In Section II we introduce our system perspective of the IoT. We illustrate and describe the components of self-organization and their challenges in Section III. Research opportunities and open questions for self-organization design in the IoT are discussed in Section IV. We survey related work relavant to self-organization in the IoT in Section V and finally conclude our paper in Section VI.

II. Self-Organization from a System Perspective

We look at the IoT from a system perspective. All the things (devices) envisioned in the IoT paradigm are part of a heterogeneous network. It is heterogeneous not only from a device's computation capability perspective, but also from the perspective of network and communication technologies used to interconnect these devices and the services being offered by various devices in the IoT. Thus we treat the computation and the communication operations of these devices towards the common goal in IoT as one system.

We envision that the system perspective of the IoT is critical to not only plan and understand the normal operations or true potentials of this becoming a full-scale reality, but also the behavior of the system during adversarial or distressed conditions. For these situations, we discuss the need for a common framework which is considerate of constraints and challenges of various computing and networking components coming together. In essence, the *common goal* for the IoT during adverserial or distress times is *self-organization*. Towards this common goal, we will discuss the various networking challenges which have been addressed in different research communities but play a role in the paradigm of IoT. In this paper, we bring together those challenges and propose to address them together as one system.

Before we address the challenges and components of self-organization, we discuss the key properties we envision that are critical to efficient self-organization in the IoT.

1) *Cooperative communication model* is a key property in self-organization in the IoT. The IoT being a heterogeneous network, there are multiple interconnected networks involved to support end-to-end communications. Hence there could be multiple distinct networking protocols needed to support communications across each layer. All these distinct protocols should support the network operations so that no device is left behind during self-organization. Thus the cooperation among networks also extends to cooperation for resource access, fair and appropriate resource usage (bandwidth) and consideration of energy constraints of other devices in the network.
2) *Situational awareness* is key to effective self-organization in the IoT. Devices should not only be cognizant of the operations in their neighborhood, but also their adjacent neighborhoods. This will not only help in initiating self-organization, but also help to recover from local faults. Thus this plays a vital role in improving availability in the network.

3) *Automated load-balancing* is a desired property for self-organization in the IoT. While self-organization leads to devices forwarding data towards a data sink, devices towards the sink are spending more energy to keep the network services alive. This could lead to energy exhaustion on these devices if they are battery powered and hence lead to single points of failure. Instead, we need to have automated load-balancing to the maximum possible extent. Load-balancing could also allow for devices to recalibrate their transmission rates or prioritize data for transmission so that energy consumption towards the sink is maintained under limits, thereby improving the overall longevity of the self-organized network.

III. Key Components of Self-Organization in the Internet of Things

We envision five components that are key to self-organization in the IoT. These components perform specific functions but allow for the smooth operation of the self-organized network in the IoT. We will also see the inter-dependencies of various components of self-organization, which makes algorithm design all the more challenging. This section will show that a system perspective of the IoT lends well into designing self-organization algorithms for the IoT.

A. Neighbor Discovery

The networks deployed for the IoT applications are generally hierarchical [1]. It is a recursive chain of a group of slave devices communicating with a master device, and a set of these master devices communicating with the next tier master device. This is similar to a sensor network set up within a home or a building, where sensors report data to a nearby sink node and these sink nodes could further report the home's sensor network gateway. Such networks are planned to ensure that the sink nodes can detect the presence and collect data from downstream devices and forward them to the upstream devices. However, it is not always possible that the networks are designed to allow for devices to know the presence and operational status of their peers. This is important because, the failure of devices or the occurrence of an event that triggers self-organization must be known to peer devices which can cooperate with the distressed device to support its communications. This means that devices in the IoT paradigm should monitor the operational status of their peers. Thus when a device's connectivity fails, the device would know who is operational and seek connectivity. Hence we believe that this should be the first step in self-organization in the IoT.

In our earlier work, we proposed the use of status codes for smart meters which are broadcast and processed by their peers and the uplink receiver [2]. Certain types of status codes allowed for the self-organization to begin and thus created local awareness of the need to self-organize. Similar to status codes are periodic beacons in sensor networking applications to detect failure of nodes in a data collection tree. However, a challenge to implement this in the paradigm of IoT is the need for all devices in a heterogeneous network to be able to interpret the codes in the same way, thus leading to actions on those codes towards a common goal.

B. Medium Access Control

Medium access control is responsible for ensuring that when a network node accesses a channel, no other node interferes with it. Robust medium access control is critical for effective self-organization and network performance in the IoT paradigm. The reasons for this being multi-fold, 1) every device in the network will have data to send, hence every device needs exclusive access to the medium, 2) devices forwarding traffic from other devices will have more data to send, thus there will be asymmetric needs for medium access, 3) changes in network topology could result in medium access schedules also needing changes, and 4) services needing guaranteed access needs network-wide and end-to-end medium access scheduling.

There are two possible ways of managing medium access for self-organization in IoT. First is to provision medium access by polling devices for their needs for medium access and then allowing the devices to access the medium using a deterministic schedule. Second is to allow for random access to the medium. Devices sense the medium and use the medium if there is no other device using it, else they wait and use access the medium when it becomes free. We will discuss the scenarios under which each could be applicable and their deployment challenges.

1) Provisioned medium access: Time Division Multiple Access (TDMA) is a type of provisioned medium access scheme and is widely implemented for variety of wireless communication applications [3]. TDMA allows for devices to access channel in dedicated time slots in a TDMA frame. Slot allocation for the network nodes is decided based on the network topology and slot needs of nodes at the beginning of each frame. Slot allocation could be centralized or distributed based on the nature of the application or service being supported [4]. In either of the implementation of TDMA, hidden and exposed terminal problems are avoided to a large extent thereby providing higher guarantees for medium access [5]. Thus, this makes TDMA more suitable for time-sensitive applications where timely data delivery is critical. Applications such as disaster monitoring in neighborhoods, outage monitoring in smart grids, health monitoring for personal health systems are examples of such time-critical IoT applications. However, this comes at a cost of complexity in the implementations of TDMA which also need network-wide time synchronization.
2) Random medium access: Carrier Sense Multiple Access (CSMA) is a lightweight random medium access scheme. CSMA with Collision Avoidance (CSMA/CA) is the contention based medium access scheme used in wireless standards such as the IEEE 802.11 and 802.15.4 [6]. As the name indicates, network nodes sense the channel before accessing the channel. If busy, they wait until the channel is free and then attempt to access the channel.

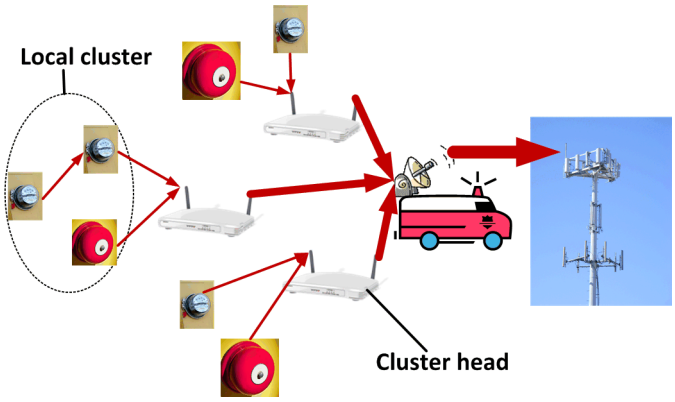

Fig. 2: This figure illustrates self-organization of devices to connect to a cellular tower to connect to the internet. The multiple layers of networks formed show the traffic aggregation at each layer through the thickness of the arrows.

As CSMA/CA is a best effort service, over multiple hops CSMA/CA can deteriorate network performance steeply [7]. Hence, CSMA/CA is suitable for applications or services not needing timely data delivery guarantees. For example, sensor readings from renewable sources of energy in smart homes is still valuable to the grid's monitoring center during outages. This gives a notion of how much the grid can self-support itself during an outage, but it is not critical for managing the grid's outage. Hence, timely delivery guarantee of such data is not needed.

C. Local Connectivity and Path Establishment

Neighbor discovery allows devices to know their nearest available peers who can coordinate and cooperate for self-organization. However, peer connectivity alone may not always result in connecting distressed devices to the internet. In-fact, in most applications envisioned for the IoT, multi-hop communication might be needed to reach the internet or provisioned network service. This need for multi-hop communication arises from communication, medium access contention and radio propagation distance limitations. Hence, we need the self-organization to create a hierarchical network which can mirror the hierarchy that was designed for normal operations. This however makes an implicit assumption that devices towards the functioning internet in the self-organized network have capability to haul more traffic than their downstream networked devices as shown in Figure 2. In order to recreate the network hierarchy, nodes could first self-organize into local groups called clusters and inter-cluster communications are facilitated by cluster-heads to eventually reach the data sink. The end-to-end path is created via a layer of network comprising the cluster heads. This layer operates above the locally formed clusters.

Clustering allows for scaling in the self-organization process. Each cluster is designed to have a cluster head that can communicate with other members of the cluster either via one-hop or multi-hop communications. Thus if cluster heads can further interconnect forming a mesh network to connect clusters to data collectors, scalability can be improved. This is because the average path length from a device to the functioning internet gateway will not be in the order of $O(N)$, N being size of the network, but closer to the order of $O(log(N))$.

D. Service Recovery Management

It is possible that during times of disasters or outages or even during normal operations for devices in the IoT to fail. When device failure occurs, the connections and services it was earlier supporting also dies. Hence it is important for the self-organization algorithms to be cognizant of device failures and allow for service recovery post the failures. Effectiveness of service failure recovery largely depends on structure of the network and the relative positions of devices in the network. We discuss the advantages and constraints for clustering techniques in self-organization which will help recover from service disruptions.

We believe that clustering in initial stages of self-organization has more advantages than just grouping devices for scalability purposes. First, nodes need not have a global knowledge of the network, hence reducing the need for on-board memory and minimizing network control updates. Second, clusters can locally repair routes due to node failures to an extent that it does not induce impact on the entire network's operations. This way even devices within a cluster need not be aware of routing changes happening outside of its clusters, as long as the data makes it to the destination which is a data collector. Third, cluster heads perform statistical operations on data from cluster's devices, average value of the data will not vary much with local failures. This is true provided that the event being sensed or monitored does not drastically change in a short interval of time. Thus clustering can save bandwidth by not relaying all the data packets received from nodes in the cluster and also be resilient to local failures.

In the design for clustering during self-organization, it is desired to minimize the number of clusters [8]. This has many advantages. It reduces the number of inter-cluster hops needed to reach a data collector. Second, if multi-channel communications are used with spatial reuse, then number of channels needed is also minimized to some extent. Third, smaller number of clusters allows for lesser number of updates needed by cluster heads to update connectivity information between clusters. Finally, since cluster heads are spending more energy than other nodes in the network, smaller number of clusters in the network means smaller number of cluster heads in the network and therefore allows for better performance in network longevity.

A hierarchical clustering scheme was proposed that considers overlapping of clusters to allow for inter-cluster connectivity and also considering the cluster sizes for management purposes [9]. This scheme allows for asymmetry in cluster sizes, but does not have a mechanism to dynamically compute and bootstrap a mesh of mesh hierarchy. Since the work

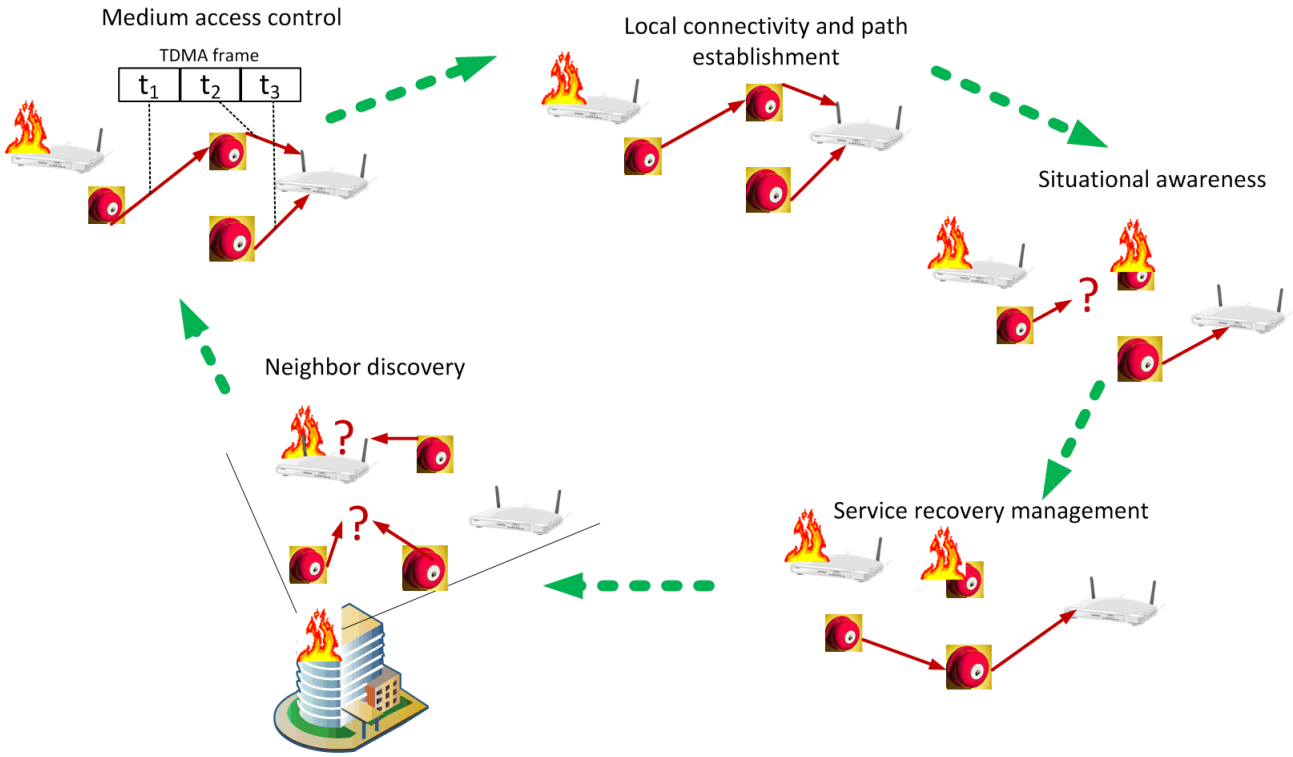

Fig. 3: This figure illustrates self-organization eco-system in the Internet of Things. As devices constantly monitor their environment, an adversarial event triggers the self-organization process. Devices then connect to their neighbors, cooperate for medium access, establish paths, monitor their environment for faults, recover from local faults and restore services and continue to monitor their environment. Thus we see that self-organization is a cycle until the operating environment is fully restored for normal operations.

involves recursive building of trees at each level, breakage of link in any of the trees formed might need the entire network to initiate the clustering process again. More-ever, this work does not build the hierarchy based on application demand needs which considers the medium access constraints. These constraints are addressed in the self-organization of a mesh hierarchy for smart meter infrastructures in the smart grid in our earlier work [10].

E. Energy Management

Under normal operations, energy is not a constraint as all these sensing devices are powered by energy lines. However, when energy supply fails and the self-organized network is dependent on battery powered communications, energy management is a concern. If the self-organized network is hierarchical, and if there is no in-network processing of the sensor data, the data aggregates towards the data sink. This means that more energy might be needed to support communications towards the data sink. Hence, devices might start to fail because of lack in energy to support communications. Energy management has been well studied in the sensor networking community with aim of optimizing energy consumption for various constraints [11]. Additionally, lightweight operating systems have been designed and deployed for sensor networks to support real-time applications [12]. Energy management is also dependent on cluster head election schemes as cluster-heads will have higher energy consumption profiles, which could also lead to multiple points of failures in a network. Hence we see that energy management is not only a function of how much data is being sent, but also various other factors such as efficiency in operating system, clustering, medium access control and environment monitoring techniques.

F. Integration of IoT's Self-Organization's Components

Summarizing the role of the key components, we can see that the self-organization in the IoT works as one eco-system. To our best knowledge, the self-organization will be a continuous and closed cycle process as shown in Figure 3. An event triggers self-organization, devices look to their neighbors for connectivity as part of *neighbor discovery*, devices cooperate with each other for medium access as part of *medium access control*, end-to-end connectivity is established, situation in this self-organized network is monitored for failures, neighborhood awareness leads to service recovery and restoration and the self-organization cycle continues going back to monitoring the environment for events. With the environments recovering from failures to normal operations, self-organization can be ceased to make way for provisioned communications to be functional.

IV. Open Research Problems

We have so far illustrated and described the challenges of various components in self-organization in the IoT paradigm.

We now discuss some of the open research problems for designing efficient self-organization algorithms for the IoT.

A. Cross-Layer Design for Self-Organization

Each of the challenges discussed in Section III have so far been addressed as individual research problems in the past. However, when viewed from a system's perspective a cross-layered approach is needed to address all these problems as one system by understanding the constraints of each challenge we discussed laid on each other performance of the others [13]. A simple example of this is, if neighborhood awareness is not properly executed, then an unaware medium access control protocol will perform poorly due to large contentions and then leads to degradation in network performance which directly affects the service supported by the IoT application. Hence, we need a holistic approach to designing the self-organizing algorithms which are aware of such constraints. An example of a cross-layer based self-organization was shown for collecting smart meter data during outages [10]. The constraints of application demand and the medium access scheme was factored into designing the self-organization of smart meters during outages. However, a deeper understanding of resource needs (number of channels) and the information capacity limits are yet to be explored for such dynamically created hierarchical networks. Additionally, it is still not clear as to how much of cross-layer design is needed to achieve desired properties in self-organization. Metrics needed to quantify the performance of cross-layer design for self-organization need to be understood. Is it studied in terms of communication performance metrics such as throughput, delay or graph theoretic metrics such as betweeness, average degree, connectivity is still an open question. In our experience, a combination of both are needed to understand the dynamics of self-organization, but the right combination of such metrics will have to be explored.

Challenge: A self-adaptive cross-layer model for self-organization in the IoT, which is aware of scale, energy and communication resource constraints.

B. Heterogeneity in Self-Organization

We have so far discussed the heterogeneity in computation and communication capabilities of things in the IoT. Another dimension of heterogeneity that is an interesting problem is the heterogeneity in services being offered from self-organization. What we mean by heterogeneity in services is, bottom most layers of the self-organized network could function with a best-effort service model. For example, by using CSMA/CA for devices not frequently wanting to send data. But higher layer devices which are connecting these lower network layers could function with high availability and reliability network operation models. Thus data which reaches these *reliable* network layers offers lesser latency in getting the data to reach functioning or provisioned networks as shown in Figure 4. The problem to be addressed here is, network intelligence models for when the best-effort service model be stopped during self-organization and reliable service models begin. Such a self-organizing design seems more practical as it allows for the low layer network devices to be simple, have simpler hardware with minimal computation and communication capabilities and higher layer devices to be more capable to support efficient self-organization.

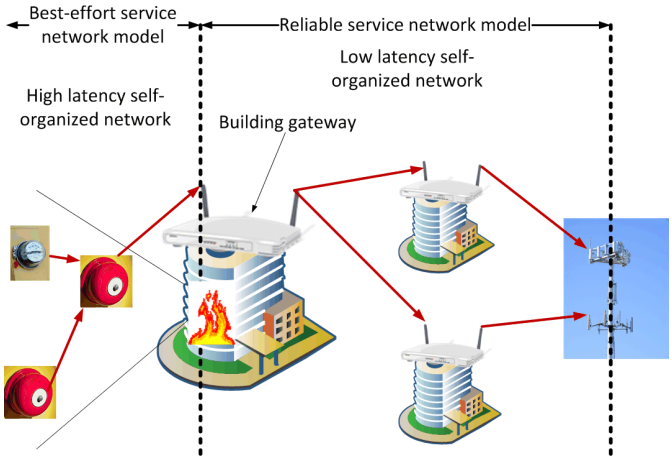

Fig. 4: This figure shows an example of heterogeneity in services offered in a self-organized network. Sensors in buildings under adversarial conditions use a best-effort service model to reach the building's gateway. The gateways of buildings use reliable service network models to reach a functioning gateway to the internet, which could be a cellular tower.

Challenge: Network intelligence to derive barriers between types of services supported in self-organized network of the IoT.

C. Multi-Radio Multi-Channel Communications

For communications during self-organization to be supported continuously and still allow for network scalability, data has to be sent and received at the same time at the devices. This is not possible on a single channel-single radio interface [2]. We need the devices in IoT to support multi-channel multi-radio communications. This will allow for the device to receive data traffic from downstream devices on one set of radios and forward them to the next set of upstream devices on another set of radios. However, multi-radio and multi-channel communications impose complex channel assignment mechanisms. For each layer of the network the channel assignment is a coloring problem [14]. Hence, multi-radio multi-channel communication could create layers of coloring problems so that no consecutive layers of networks and their adjacent networks get assigned the same channel for communications. This will create a larger contention size for medium access beyond what can be supported and thereby allowing for inconsistencies in network performance. However, part of this could be overcome by the diversity in radio technologies being supported on the devices as shown in Figure 5. Additionally, the use of cognitive radios that scan the spectrum for available channels to support communications during emergencies help improve to sustain communications if licensed or provisioned channels are busy [15]. Multi-radio cognition devices also allow for additional

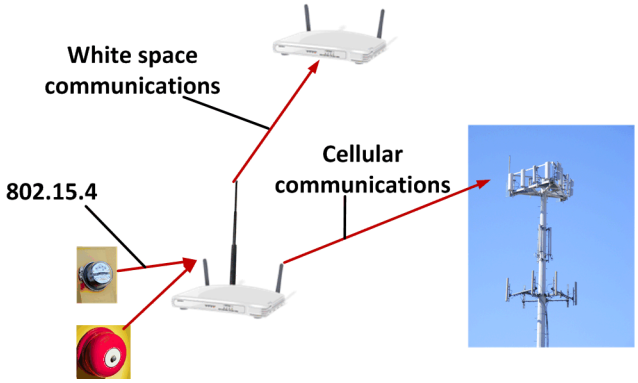

Fig. 5: This figure shows the benefits of radio diversity available in multi-radio enabled devices. Each of the radios shown in the figure operate in different center frequencies. Thus improving availability of channel to support communications in the self-organized network even if other channels are busy.

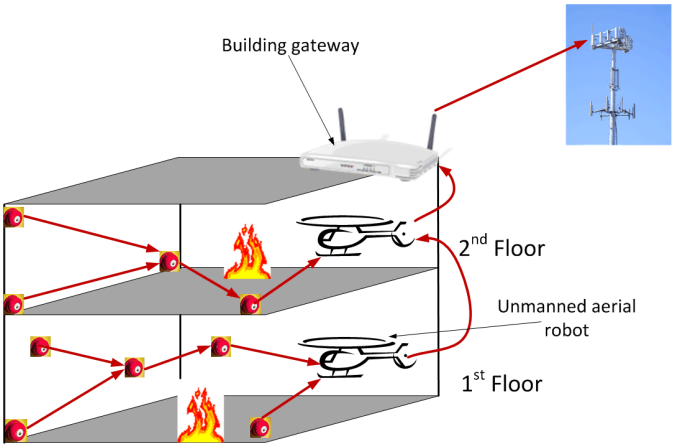

Fig. 6: This figure shows the use of unmanned aerial robots to collect data from discrete self-organized networks in two floors of a building on fire. The unmanned aerial robot then reports data to the building's IoT gateway. The building gateway then relays the fire sensor data to the internet which could then reach the fire emergency services.

assurances for achieving network availability and reliability in self-organized networks in the IoT, although cost of such devices will still remain to be a concern.

Challenge: A model that predicts where best in the IoT should devices with higher radio functionality be placed for efficient and reliable self-organization.

D. Low-Power Computing and Load Balancing

Capacity limits for wireless networks have been studied from an information theoretic perspectives [16]. However, we envision that while these research results hold true, the actual capacity of self-organized networks in IoT are dependent on energy decay on the devices. With each device having its own data and forwarded data to transmit, the energy decay across the network is not uniform. Hence, a device might be able to send more data, but might be forced to limit its capacity because of energy decay constraints. This translates to a problem of modeling the energy cost of self-organization in the IoT paradigm. This model will not only help understand capacity of self-organized networks, but also show the limits of scale of such networks and thereby allow researchers to design load balancing schemes for self-organization in the IoT.

As important the communication and network protocol designs are, low-power computing is equally important. Low-power computing is not only restricted to understanding sleep and wake-up cycles of devices, efficient algorithms in IoT, but also goes to the depth of computing. This includes the understanding of trade-offs in changing clock-rates, cost of communication per bit, hardware design etc. Intelligence can be built into devices to make computing decisions based on events they are sensing or depending on the environment they are in. Every opportunity in reducing energy consumption in hardware and software operations could improve the scale and capacity of self-organized networks in the IoT.

Challenge: A deeper understanding of generic computing and communication needs of self-organization towards customizing hardware and software design to aid in low-power computing.

E. Delay Tolerant Networking over Self-Organized Networks

Self-organized networks in the IoT will be limited in scale because of energy constraints or information capacity limits. In a large IoT environment, this creates multiple discrete self-organized networks which still need connectivity to a gateway to the internet. As network designers, we will not know how much more of provisioning is needed to ensure that all the devices in an IoT paradigm will be connected. But we can look for ways in which the data-sinks of these discrete can be connected even if it implies delay in data reaching a functioning gateway to connect to the internet. Thus we envision that this scenario will serve as a good platform to use the services of delay/disruption tolerant network (DTN) technologies over the multiple discrete self-organized networks [17].

Unmanned aerial robot swarms are being developed for high precision surveillance and reconnaissance purposes in adversarial conditions [18] [19]. Thus the use of indoor localization and swarm navigation technologies comes handy to connect the discrete self-organized networks to the internet as shown in Figure 6. While the use of such technologies with self-organized mesh introduces a delay in the data being received at the end point, it will continue to enable end-to-end connectivity. Using DTN over self-organized networks has multiple advantages. First, it imposes no additional requirements in device design to interact with data mules. Second, self-organizing can occur to the extent the devices can support the operations and allowing for further connectivity to be established by the data mules. Finally, locally self-organized networks need not have global knowledge of the IoT's functioning and thereby eliminating the need for self-adaptation to changes in other IoT environments.

The problems that need to be addressed with DTN over self-

organization are many. First, a service to detect the presence of all self-organized networks in an IoT environment in adversarial conditions. Second, a process to automate the prioritization of data collection schedules from the various self-organized networks. Third, the storage needs for the devices in the IoT to support data storage while they wait for the data mule to collect the data.

Challenge: Reliable and automated detection of self-organized networks and prediction models for storage needs to support DTN over self-organized networks.

V. Related work

Self-organization has been studied and algorithms proposed for specific applications or network environments. Some examples of these are the self-organization of communications in sensor networks, mobile ad-hoc networks and smart meter infrastructures in smart grids. All these prior work does have certain components of self-organization we discussed in Section III. While these solutions work well for the applications they were intended for, modifications to these solutions could work for some components of self-organization in the IoT, but will not treat the IoT as one system. Hence, we believe that this work will motivate the design of self-organization in the IoT that will be cognizant of the system's behavior as a whole.

Self-organization has been studied in the realm of sensor networks and mobile ad-hoc networks [20][21]. The goal of self-organization is to ensure connectivity of all network nodes to a data collector in a homogeneous network. The self-organization involves grouping network nodes into clusters [9] [22] [23] [24], and then interconnecting clusters to a data collector using multi-hop communications.

In some applications cluster heads are pre-defined during network deployment and in others network nodes assume the role of cluster head based on heuristics, both of which can complete clustering and cluster head election in constant time [21]. These heuristics for example are, a node when it senses no cluster head in its vicinity, becomes a cluster head with a certain nonzero probability [22] [23], or a node in radio proximity to all other nodes in a cluster chooses to become a cluster head [24], or nodes in proximity to other clusters could become cluster heads to provide inter-cluster connectivity. Low Energy Adaptive Clustering Hierarchy (LEACH) was proposed as a clustering scheme for the wireless sensor networks [22]. Results of this work could help improve cluster head selection in the IoT if there is diversity in radio technologies on a multi-radio platform. But it is still remains to be explored of how this could solve the energy management problem in self-organization in the IoT. Additionally, all these schemes of self-organization and clustering have been studied for homogeneous networks and thus it is not entirely clear if they will be directly applicable for heterogeneous networks in the IoT paradigm. However, these solutions will serve as a starting point for understanding the changes or new proposals needed for the *local connectivity and path establishment* and the *service recovery management* components of self-organization in the IoT.

Wireless mesh networks have been proposed and studied with the aim of improving the distributed nature of networking [25]. Heterogeneity has been part of designs for wireless mesh networks. Wireless mesh networks have the property of self-healing when routes fail among the mesh routers. This property is good when the lower layer mesh clients have other mesh routers to reach to, ensuring that connectivity to the internet is still not lost. But when no mesh router is in the vicinity, then the *neighbor discovery* and *local connectivity and path establishment* components have to work together to establish paths to a functioning mesh router.

Cross-layer designs have been discussed in the realm of many network applications [13]. The interactions between multiple layers of a network stack has been discussed to improve network reliability. Additionally, the cross-layer designs have been developed for specific application's performance improvements. But little work has been done on using cross-layer designs for self-organization for heterogeneous networks. Cross-layer design to our best knowledge lends well into the system perspective one needs to have to design self-organization algorithms. We discuss two such cross-layer design based self-organization for smart meters in the smart grid.

A wireless mesh based multi-hop self-organizing scheme was proposed for the smart meter infrastructure in the smart grid, as an enhancement to Routing Protocol for Low Power and Lossy networks (RPL) [26]. Their proposal is shown to work for 50 smart meters which were connected within 4 hops and mooted the possibilities of using multi-channel communication for self-organization techniques. But, the use of Carrier Sense Multiple Access (CSMA) provides no network performance guarantees over multiple hops, thus limiting their scale [5]. However, their modification to the RPL serves as a good insight of how *neighbor discovery*, *local connectivity and path establishment* and *service recovery management* can be implemented as one system.

We proposed an application demand and medium access aware self-organizing mesh network system for smart meter infrastructure in the smart grid [10]. This work made leveraged the advantages in using multi-radio multi-channel communications on smart meters. Situational awareness was built into the model and the network self-healed to growth or shrink in network by adjusting the application demand. While resource management was done using contention-free medium access such as Time Division Multiple Access (TDMA), energy management is still a concern. Except for the energy management component, the rest of the components were considered as part of one system in the self-organization design which allowed for the proposed solution to scale. The proposed solution scaled well to connect about $10,000$ smart meters during outages. However, load balancing techniques are needed to ensure that the overall longevity of the network is not a function of only a few smart meters towards the data sink.

Thus we see that several prior work have attempted to solve or shown how each of these individual components of self-

organization can work for specific network applications. These network applications have spanned wireless areas such as ad hoc networks, wireless sensor networks and cognitive radios. Also, these works have been mainly solved by isolating the effects of other components which is good for those network applications of interest. However, the IoT is not one single network application, but a system of these network applications interacting with each other. Hence, the fundamentals of stand alone solutions of other network applications could still hold true for the network self-organization components in IoT, but what is needed an eco-system that seamlessly integrates all these solutions for self-organization in the IoT.

VI. Conclusion

Distressed situations comprising disasters and outages are a reality and disrupt communications in the IoT paradigm. Thus in order to restore network connectivity and the services supported by the devices, self-organization is needed. We presented a survey of existing techniques to self-organize in other network applications. We then identified, illustrated and discussed the key components of self-organization in the IoT. The five components of self-organization we identified are *neighbor discovery*, *medium access control*, *local connectivity and path establishment*, *service recovery management* and *energy management*. We believe that all these components are part of a cycle which makes self-organization as a continuous process until the normal operations are restored. All of these components are vital to efficient self-organization and are expected to cooperate, which emphasizes the need for one to treat IoT as a large and distributed system and design the self-organization algorithms. Keeping this perspective in mind and the related work so far, we discussed research opportunities for self-organization in the future. We discussed the need for cross-layer design for efficient self-organization, ability to support heterogeneity in network service models in self-organized networks, advantages of multi-radio communication technologies for self-organization, the need for low-power hardware and software architectures and finally exploring the use of delay tolerant technologies to connect discrete self-organized networks that are limited by scale.

References

[1] L. Atzori, A. Iera, and G. Morabito, "The internet of things: A survey," *Computer Networks*, vol. 54, no. 15, pp. 2787–2805, 2010.

[2] A. P. Athreya and P. Tague, "Survivable smart grid communication: Smart-meters meshes to the rescue," in *2012 International Conference on Computing, Networking and Communications (ICNC)*, Jan./Feb. 2012, pp. 104–110.

[3] D. Falconer, F. Adachi, and B. Gudmundson, "Time division multiple access methods for wireless personal communications," *IEEE Communications Magazine,*, vol. 33, no. 1, pp. 50–57, 1995.

[4] R. Ramaswami and K. Parhi, "Distributed scheduling of broadcasts in a radio network," in *Proceedings of the Eighth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM '89)*, Apr. 1989, pp. 497–504.

[5] I. Rhee, A. Warrier, J. Min, and L. Xu, "DRAND: Distributed randomized TDMA scheduling for wireless ad hoc networks," *IEEE Transactions on Mobile Computing,*, vol. 8, no. 10, pp. 1384–1396, Oct. 2009.

[6] V. Bharghavan, A. Demers, S. Shenker, and L. Zhang, "Macaw: a media access protocol for wireless lan's," *SIGCOMM Comput. Commun. Rev.*, vol. 24, no. 4, pp. 212–225, Oct. 1994.

[7] P. C. Ng and S. C. Liew, "Throughput analysis of IEEE 802.11 multi-hop ad hoc networks," *IEEE/ACM Transactions on Networking,*, vol. 15, no. 2, pp. 309–322, Apr. 2007.

[8] E. Oyman and C. Ersoy, "Multiple sink network design problem in large scale wireless sensor networks," in *IEEE International Conference on Communications*, Jun. 2004, pp. 3663–3667.

[9] S. Banerjee and S. Khuller, "A clustering scheme for hierarchical control in multi-hop wireless networks," in *Twentieth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2001)*, 2001, pp. 1028–1037.

[10] A. P. Athreya and P. Tague, "Self-organization of a mesh hierarchy for smart grid monitoring in outage scenarios," in *Proceedings of the 4th IEEE PES International Conference on Innovative Smart Grid Technologies*, 2013.

[11] A. Sinha and A. Chandrakasan, "Dynamic power management in wireless sensor networks," *IEEE Design and Test of Computers*, vol. 18, no. 2, pp. 62–74, Mar./Apr. 2001.

[12] A. Eswaran, A. Rowe, and R. Rajkumar, "Nano-RK: an energy-aware resource-centric RTOS for sensor networks," in *26th IEEE International Real-Time Systems Symposium (RTSS 2005)*, Dec. 2005.

[13] V. Srivastava and M. Motani, "Cross-layer design: a survey and the road ahead," *IEEE Communications Magazine,*, vol. 43, no. 12, pp. 112–119, 2005.

[14] K. N. Ramachandran, E. M. Belding, K. C. Almeroth, and M. M. Buddhikot, "Interference-aware channel assignment in multi-radio wireless mesh networks," in *IEEE INFOCOM*, 2006, pp. 1–12.

[15] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "Next generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks*, vol. 50, no. 13, pp. 2127–2159, 2006.

[16] P. Gupta and P. Kumar, "The capacity of wireless networks," *IEEE Transactions on Information Theory*, vol. 46, no. 2, pp. 388–404, Mar. 2000.

[17] K. Fall, "A delay-tolerant network architecture for challenged internets," in *Proceedings of the 2003 conference on Applications, technologies, architectures, and protocols for computer communications (SIGCOMM '03)*, 2003, pp. 27–34.

[18] A. Purohit, Z. Sun, F. Mokaya, and P. Zhang, "Sensorfly: Controlled-mobile sensing platform for indoor emergency response applications," in *2011 10th International Conference on Information Processing in Sensor Networks (IPSN),*, 2011, pp. 223–234.

[19] D. Mellinger, N. Michael, M. Shomin, and V. Kumar, "Recent advances in quadrotor capabilities," in *2011 IEEE International Conference on Robotics and Automation (ICRA),*, 2011, pp. 2964–2965.

[20] J. Yu and P. Chong, "A survey of clustering schemes for mobile ad hoc networks," *IEEE Communications Surveys Tutorials*, vol. 7, no. 1, pp. 32–48, 2005.

[21] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[22] W. Heinzelman, A. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," *IEEE Transactions on Wireless Communications*, vol. 1, no. 4, pp. 660–670, Oct. 2002.

[23] S. Bandyopadhyay and E. Coyle, "An energy efficient hierarchical clustering algorithm for wireless sensor networks," in *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM 2003)*, Mar./Apr. 2003, pp. 1713–1723.

[24] K. Xu and M. Gerla, "A heterogeneous routing protocol based on a new stable clustering scheme," in *Proc. MILCOM 2002*, Oct. 2002, pp. 838–843.

[25] I. Akyildiz and X. Wang, "A survey on wireless mesh networks," *IEEE Communications Magazine*, vol. 43, no. 9, pp. S23–S30, 2005.

[26] P. Kulkarni, S. Gormus, Z. Fan, and B. Motz, "A self-organising mesh networking solution based on enhanced RPL for smart metering communications," in *2011 IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM)*, Jun. 2011, pp. 1–6.