Accepted Manuscript

Cognitive routing protocol for disaster-inspired Internet of Things

Fadi Al-Turjman

PII: S0167-739X(16)30743-9
DOI: http://dx.doi.org/10.1016/j.future.2017.03.014
Reference: FUTURE 3382

To appear in: *Future Generation Computer Systems*

Received date: 6 December 2016
Accepted date: 8 March 2017

Please cite this article as: F. Al-Turjman, Cognitive routing protocol for disaster-inspired Internet of Things, *Future Generation Computer Systems* (2017), http://dx.doi.org/10.1016/j.future.2017.03.014

Cognitive Routing Protocol for Disaster-inspired Internet of Things

Fadi Al-Turjman,
Department of Computer Engineering,
Middle East Technical University,
Northern Cyprus Campus,
99738 Kalkanli, Güzelyurt, Mersin 10, Turkey
Email: fadi@metu.edu.tr

Abstract- In this paper, we propose a framework for data delivery in large-scale networks for disaster management, where numerous wireless sensors are distributed over city traffic-infrastructures, shopping-malls' parking areas, airports' facilities, etc. In general, our framework caters for energy-efficient applications in the Internet of Things (IoT) where data is propagated via relays from diverse sensor-nodes towards a gateway connected to a large-scale network such as the Internet. We consider the entire network energy while choosing the next hop for the routed packets in the targeted wireless sensor network. Our delivery approach considers resource limitations in terms of hop count, and remaining-energy levels. Extensive simulations are performed and achieved results confirm the effectiveness of the proposed approach in comparison to other baseline energy-aware routing protocols in the literature.

Keywords- IoT, Data routing, Smart-cities, Energy-efficiency.

I. INTRODUCTION

Sensing technology has played a significant role in detection and containment of disasters in numerous disciplines. The most notable among these applications are those functioning in harsh environments, such as pollution and flood detection, forestry fire prevention and earthquake monitoring applications [1][2]. For instance, a network of sensors can be used to monitor the motion of toxic gasses over vast areas [3]. In [4], redwood trees in risk have been monitored via a wireless sensor network. Furthermore, the existence of a disinfectant that works better and more efficient than conventional traditional ones, by providing long lasting antiviral effect against major viruses has proved the importance of sensing technology in disaster management [5]. The above mentioned examples are just few of the many areas where sensing technology has made massive improvements. However, this technology is still suffering extreme limitations in terms of energy and connectivity while collaborating in wireless network-based systems.

Connectivity and links between sensing-devices (nodes) distributed to monitor a specific phenomenon have led to the idea of WSNs followed by the Internet of Things (IoT) proposal. Integrating sensing-devices with other heterogeneous network systems such as WiFi, LiFi, LTE, etc. can significantly expand the array of services that can be provided to public users as well as decision makers in critical safety applications. However, several design aspects such as the limited-energy constraints, short communication range between geo-located objects, and the low processing power, need to be incorporated into the routing protocol in order to realize the IoT paradigm. There have been several attempts in the literature to propose lightweight solutions for the IoT paradigm in order to save energy [6]-[8]. However, these solutions are still under investigation. WSNs in IoT consume energy in almost all processes [9]. They consume energy while making data transmission, data sensing and data processing. A few attempts towards achieving energy efficiency in such networks via wireless multi-hop networking have been proposed, e.g. [10]-[12]. However, such schemes either assume static network topology, which render these schemes impractical for real-life network implementations, given that IoT-based networks exhibit random topology due to the mobility of nodes, or are restricted to two hop from source to the sink. Due to the fact that IoT-networks' sensors are usually limited in their processing power, communication range and energy capabilities, design and implementation of routing algorithms are considered a nontrivial task.

Moreover, accommodating various levels of harshness in surroundings in terms of temperature, dust, humidity, etc., dictates a resilience requirement to an expanded set of failure possibilities that includes partial or complete failure of the IoT sensor nodes, and reduced levels of activity or accuracy undergone as batteries deplete, which forms serious threats for losing critical in-network data before being utilized. This requirement stresses the integrity of cognition elements in IoT routing protocols. Moreover, an IoT sensor network needs to sustain different levels of mobility on disaster situations [13]. Since the IoT connected things rely on each other to gather and process data, mobility may be temporarily or permanently detrimental to the network operation by breaking some functional communication links that affects the in-network data retrieval. Hence, nodes and links are prone to several risks leading to high probabilities of failures and several nodes in the network may become disconnected/failed. As a reason of that, we are characterizing such circumstances by the Probability of Node Failure (PNF). Consequently, for a successful and reliable operation of the IoT paradigm in disaster-inspired scenarios, a cognitive energy-efficient routing approach shall be applied.

Recently, there have been significant attempts in the direction of building a cognitive sensor network, where researchers have made use of artificial neural networks, genetic algorithms, game theory and even software agents to implement distributed and intelligent decision making in sensor networks [2][18][19]. However, there is no single framework that can be used to implement cognition in sensor networks supporting the IoT paradigm in a way that is domain and application independent.

In this paper, we propose a cognitive data delivery approach that addresses the challenges of data delivery in IoT networks comprised of energy-constrained IoT sensors. Two key elements in cognition are utilized in our approach in order to implement cognition; *reasoning* and *learning* elements. Reasoning is used to differentiate between the attributes of a given traffic flow, and choosing the next hop along the data delivery path to the destination. While reasoning realizes short-term objectives and makes decisions based on the current network status, learning assists in achieving long-term goals of the network, such as improving its lifetime. The feedback received from the previous history of the exchanged messages aids the learning process, and leads to proactive actions. This model will help us to specify which path to follow in order to determine the optimal usage of the available resources for a wide range of IoT applications in safety and security scenarios. Where the proposed approach is energy-efficient and designed to optimize the current network status for guaranteed Quality of Service (QoS) via machine learning [18]. It provides efficient and self-healing data delivery while choosing and selecting reliable communication links [19]. Moreover, the proposed approach caters for the grid-based distribution of the employed IoT sensors on the monitored object to efficiently and effectively cope with the dynamicity of IoT-network topology [20].

The reset of the paper is organized as follows. Section II reviews previous related work in the literature. Section III clarifies our system models. Section IV describes our proposed routing approach for disaster-inspired IoT paradigms. In Section V, performance evaluation results for the proposed approach in comparison to other related approaches are detailed. Finally, Section VI provides concluding remarks.

II. Related Work

Connectivity in IoT relies on finding reliable routes from IoT "things" to the Internet gateway. Utilizing duty-cycling, a routing algorithm can be designed to significant balance the network load and optimize the energy-consumption, especially in energy-constrained IoT networks. In mission critical IoT networks, it is also important, when designing the routing algorithms, to facilitate prioritization between the different traffic types. Another critical problem to overcome is the uneven energy consumption across the network where elements near the gateway would deplete their energy faster than those which are far away. And hence, feedback from the MAC and physical layers, in addition to information about the residual energy and the current load of the distributed nodes, can be utilized to identify and avoid unreliable links in order to effectively prolong the network lifetime and increase the network throughput. There are considerable advantages in coupling an IoT routing protocol with the underlying MAC layer protocol through a cross-layer design. Reducing the ratio of lost packets during channel impairments is an important reliability objective, as well [21]. Where, energy saving via cognitive radio can be applied at the MAC layer of the network stack to achieve this target [22][23]. The MAC layer is usually expected to adapt the number of retransmissions depending on channel quality. Current MAC protocols, typically limit the number of back offs and retransmissions. However, the unique characteristics of the short-range communications and the specific challenges of IoT mainly energy and processing constraints in addition to the random network topology, prevent the direct implementation of traditional WSNs' routing schemes without modification. In the following, we discuss traditional WSNs' protocols with preferable features to be considered in an IoT routing protocol.

Multipath versus single-path routing: Recent studies show that multipath routing protocols for sensor networks are better than single-path routing protocols in terms of QoS. In fact, multipath routing protocols provide lower probability of packet loss while utilizing redundant paths towards the sink [14]. The Reliable Information Forwarding using multiple paths (ReInForM) protocol as described in [15] employs a probabilistic flooding to deliver information awareness packets with desired priority levels of reliability at proportional costs for sensor networks. This routing mechanism is based on local knowledge of network conditions, such as channel error, hops-to-sink counting, and connectivity-degree. Unfortunately, this protocol is not designed specifically for real-time traffic; therefore, it does not consider delay deadlines of packets when selecting the multiple paths. A chosen path might not be able to meet the delay requirements, yet it will be used to propagate duplicates potentially consuming valuable energy and unduly occupying useful channel bandwidth without improving the system performance. The work in [29] presents a data flooding dissemination scheme. It assumes a virtual-grid network architecture where sensor-nodes are distributed densely at the vertices of the grid. Utilizing the uniform nodes' patterns and lattice algebra, the scheme dismisses node addressing requirements and employs a simple flooding scheme for data dissemination. While the proposed scheme simplifies the communication model, it overlooks the cost of real-time signal processing. Additionally, it assumes a fixed structure and a static node deployment. Nevertheless, IoT-nodes can move around us for certain health and/or traffic applications [27], and therefore, may need to be associated with different neighbors and may not always follow a fixed structure. Authors of [28] propose a sound routing scheme for energy harvesting in IoT-networks. The routing scheme assumes a hierarchical cluster-based architecture. Packet transmission from the source to the cluster head via single or multi-hop fashion. Still, however, the challenge of limited energy budget at the sensing-node is not considered effectively.

Geo-based routing protocols: These protocols utilize the node position information in order to achieve more efficient routing techniques. For example, the Geographic Adaptive Fidelity (GAF) protocol optimizes the performance of the sensor network by determining the redundant nodes via precisely identify their geographical positions [16]. Where these redundant nodes are considered equivalent and useful in terms of relaying/forwarding packets in the network. Another routing protocol, namely the GEAR (Geographic and Energy-Aware Routing), aims at improving the energy efficiency by forwarding queries to specifically determined regions [17]. In this routing protocol, sensors need to have localization hardware such as a GPS unit or a localization system which can dramatically increase the network cost. Meanwhile, the work presented in [25] proposes a geographic routing protocol; where the IoT-nodes are assumed to include two types of anchor nodes, which have higher communication and processing capabilities than user nodes. User nodes are required to localize their position with reference to these anchor nodes. However, the proposed scheme is topology-dependent and assumes a fixed topology, which may not be applicable for IoT networks. Additionally, the scheme requires addressing for all nodes, which forms a significant challenge in IoT networks with large-scale applications. Moreover, the localization techniques used can be inaccurate and lead to dramatic degradation in energy consumption.

Shortest Path Routing: In the Nearest Neighbor Algorithm (NNA), when a packet is transmitted from a node to another, it follows the shortest path based on the available common control channels. NNA assumes that if a packet always follows the shortest path, it will use it until it reaches destination node. In short, this algorithm uses a 4-direction transmission (left, right, up, down) only so it actually does not consider the shortest path, it considers the shortest neighbor relay node in order to send data. As a result of this, hop count unnecessarily increases and therefore energy consumption is negatively affected. Meanwhile, in the Shortest Path Algorithm (SPA), when a packet is transmitted from a node, the algorithm calculates the shortest path from recent node to destination instead of node-to-node, and the packet follows this path until it reaches to destination. SPA, uses 8-directions (up, upper-left, upper-right, down, down-left, down-right, right and left) and considers the shortest path to destination rather than the shortest neighbor of the relay node. Thus, In SPA hop count decreases and energy consumption of the nodes decreases in comparison with NNA. Nevertheless, SPA is the simplest routing protocol that takes in to consideration the path length as a unique design factor affecting the network energy. In practice, this assumption is not accurate due several other design factors such as the communication link condition and reliability.

In this research, we propose a Cognitive Energy-Efficient Algorithm (CEEA) as routing protocol. CEEA assumes a multitier IoT-network, and cluster/tier-wide synchronization. It is a topology-independent protocol which copes with the randomness nature in IoT-networks. CEEA determines the path from the Routing Node (RN) to the destination node in view of each node's remaining energy. The remaining energy of neighbors of recent RN's is controlled each time before a packet is sent from the RN. If one of the neighbor RNs' energy is below half of its initial value, a new path will be determined for the packet to follow. In addition, when all neighbors' remaining energy is below half of the initial energy, the system uses the same strategy. As a result of that, even if hop count increases in comparison with SPA, energy efficiency is improved for RNs and so is the network lifetime.

III. System Model

The main objective of IoT in smart environments is to monitor physical and/or chemical changes and pass the information to a data center for processing [30]. IoT nodes may have varying sensing capabilities. Due to energy constraints, nodes do not communicate with each other but rather pass the sensed data to routing nodes (RN). RNs take collected data to a Gateway (GCN) that is usually connected to the internet for remote collection/processing. This communication type continues till the IoT network death. IoT networks have to overcome several challenges. Energy consumption for communication is the most significant one. Energy-efficient routing protocols can significantly prolong the IoT-network lifetime. In this section we list the assumed system model for the proposed CEEA routing protocol.

A. Network Architecture

The typical communication range in IoT is expected to be between 1 cm and 150 m [9]. This means that the transmission range is still limited, making multi-hop routing particularly important for IoT networks. Furthermore, when IoT nodes are mobile, the direction of a communication route is not deterministic and is dependent on the drift velocity of sensory machines, which may lead to communication delay. This necessitates efficient schemes for multi-hop path creation and management. IoT networks can be divided into three categories: in-object, on-object and off-objects IoT. An overview of the structure of IoT network under such circumstances can be summarized as:

- IoT Sensor-Nodes (SNs): These are assumed to be small and simple IoT sensor-devices. Due to their limited energy, limited memory and reduced communication capabilities, they can only perform simple computation task and can transmit over very short distances. The nodes could be composed of sensor and communication units.
- Relay-Nodes (RNs): These are the Relay (Routing) devices with slightly larger computational resources than SNs and can aggregate information from a limited number of SNs and also can control the behavior of SNs by sending simple instructions (such as on/off, sleep, read value, etc.). These added capabilities would increase their size; thus, their deployment would be more invasive.
- Cognitive Relay Nodes (CRNs): They are used to aggregate the information forwarded by RNs and send the information to other CRN devices. At the same time, they can send the information from short-range-scale to large-scale. In this paper we identify these nodes as cognitive nodes (CRNs).
- Gateway (GCN): It enables to control or monitor the entire IoT system remotely over the Internet.

It's worth pointing out here that IEEE 802.15.4 protocol is considered at the CRN to specify a sub-layer for Medium Access Control (MAC) and a physical layer (PHY) for low-rate wireless private area networks (LR-WPAN) because of some desired features such as low power consumption, low data rate, low cost, and high message throughput [9]. Thus, the IEEE 802.15.4 based CSMA access method can be considered at the MAC layer. This inherently reflects the communication channel reliability. Based on [26], this channel reliability can be characterized by a reliability design factor as follows:

$$C_R = \left((1 - P_{blocking}) * (1 - P_{c-fail}) * (1 - P_{p-discard})\right) \quad (1)$$

Where $P_{blocking}$ represents the blocking probability due to a buffer-full condition; P_{c-fail} is the common channel access failure probability due to channel condition (i.e. SNR) and $P_{p-discard}$ is the probability that a packet is discarded on reaching the maximum number of retries limit. This reliability factor is responsible to make a decision when equivalent energy levels' at RNs are faced. And it reflects the probability that a frame is not blocked, lost due to common channel access failure, or discarded as a result of reaching the maximum number of retries limit.

B. Lifetime of IoT Network

IoT Network Lifetime is defined as the time or number of transmission rounds beyond which the network can no longer deliver useful information to the outside end-user. This is reflected by the network's inability to find a data delivery path with satisfactory values for quality of information (QoI) attributes such as delay, reliability and throughput, as determined by the end-user [28]. This definition not only provides information to satisfying the application requirements, but also considers the status of the network and sensing resources in defining the network lifetime. It also justifies the fact that if the network does not have the necessary resources to send packets, it cannot satisfy the end-user, and so it should be considered as a dead IoT network. The IoT network lifetime can therefore be evaluated in three ways;

1) Lifetime Based on Number of Alive SNs

Several variants do exist with this model. The simple model identifies the time until the death of the first SN in the network as the lifetime of the network. Another variant evaluates lifetime until the death of 'k' out of 'n' SNs in the network, where k <n. The lifetime is the range between the death of '*k*' nodes from '*n*' nodes in non-critical ones [31].

2) Lifetime Based on SN Coverage

This model defines the lifetime of the network in terms of the coverage of region of interest. If it is used to ensure that all points inside a region of interest are covered, it is denoted by volume coverage. When an identified number of target points are to be covered, it is denoted as target coverage.

3) Lifetime Based on Coverage and Alive SNs

This type of metrics is mostly found in Ad-hoc IoT networks. In this option, lifetime is defined as the period during which most of the nodes are connected with each other. Because in IoT each node has to communicate with a gateway node, this metric cannot be used as is. Another issue with this metrics is that the lifetime is based on the total number of packets transmitted to the gateway. Nevertheless, in most of the related works this metrics become useless [32].

C. Energy Conservation & Dead Node Issue

Energy conservation is one of the most important issues in IoT design. SNs are restricted in carrying out the network layer functions, their main task is to flood the data to their one hop routers. Hence, the multi-hop forwarding between source and gateway is normally performed by RNs which have relatively higher capabilities than SNs. And thus, we define the energy consumed at a RN by $\boldsymbol{E_{RN}} = \boldsymbol{C}\ (\boldsymbol{T} * (\boldsymbol{E_{TX}}) + \boldsymbol{R} * (\boldsymbol{E_{RX}}))$. Most of the energy consumption at the RN is due to data communication, indicated by E_{TX} for energy consumed during transmission and E_{RX} for energy consumed during data reception. C represents the cost function of the energy consumed T represents the number of transmitted packets and R represents number of received packets. As discussed above CRN main function is data aggregation and routing of traffic received from the RNs via cognition elements. The capabilities of the CRN are higher than those of RN, hence our assumption of the cognitive decision process to be performed by the CRNs, which is expected to consume additional energy compared to regular RNs [33]. Additional energy consumption is divided into two parts: one is protocol overhead incurring during cognitive data delivery due to feedback from the IoT-network during the learning process and the exchange of values of QoI attributes such as delay, reliability and throughput while making routing decisions and the other one is the increased transmit power for increasing the communication range of CRNs. Accordingly, $\boldsymbol{E_{CRN}} = \boldsymbol{C}\ (\boldsymbol{T} * (\boldsymbol{E_{TX}}) + \boldsymbol{R} * (\boldsymbol{E_{RX}})) + \boldsymbol{C}(\boldsymbol{Ag} * (\boldsymbol{E_{ag}})) + \boldsymbol{C}\ (\boldsymbol{P} * (\boldsymbol{E_{cog}} - \boldsymbol{E_{pro}}))$, where T, R, Ag, and P, represents the total number of packets that are transmitted, received, aggregated and processed by the cognitive elements respectively, in each transmission round. $(T * (E_{TX}) + R * (E_{RX}))$ is the energy cost incurred during data transmission and reception, $C(Ag * (E_{ag}))$ represents the energy cost incurred during data aggregation and $C(P * (E_{cog} - E_{pro}))$ indicates the energy cost due to protocol and processing overhead during the cognitive processes. Consequently, we can assume:

$$\boldsymbol{E_{CRN}} \geq \boldsymbol{E_{RN}} + (\boldsymbol{Ag} * (\boldsymbol{E_{ag}}) + \boldsymbol{C}\ (\boldsymbol{E_{cog}} - \boldsymbol{E_{pro}})\ ) \qquad (2)$$

If the RN and CRNs use the same transmit power, the equality sign becomes positive in Eq. (2). In order to ensure that the energy cost of $CRNs$ does not offset the advantages it offers in terms of adapting to traffic flow dynamics and network topology alterations, the cost can be optimized by maximizing the number of RNs and minimizing the number of $CRNs$ in the deployment [28].

In this work, we refer to one-hop neighbors' communication as the first tier of nodes. Since no other node can reach the monitoring station directly, traffic from every other node will have to be forwarded, in the last hop, by one of these first tier nodes. Similarly, the two-hop neighbors of the monitoring station will forward data for all nodes except the one-hop neighbors and themselves, etc. If the spatial distribution of nodes is assumed to be uniform, then the traffic load is equally distributed. Each first tier node will forward hardly the same amount of traffic, and all first tier nodes will die at times very close to each other, after the network is first put into operation. Once all of the first tier nodes are dead, no other node will be able to send data to the gateway node, and the lifetime of the network will be over. Increasing the number of nodes in the network accentuates this effect, since there is more traffic to forward and the first tier of nodes has a smaller share of the total energy budget. In general, the network death in IoT can be associated with several cutoff criteria such as the first node death, the percentage of dead nodes, or the number of dead nodes rising above a level where the routing to the sink node is no more possible [34]. Nevertheless, as we are experimenting with the clustering based protocols, in which the energy is evenly distributed throughout the mobile IoT-network, we consider the first scenario for the definition of the network lifetime. Because, when the first node dies, the number of dead nodes increases in the later rounds, and within 5-10 rounds the whole network becomes nonoperational. According to preliminary results, non-position-based routing protocols outperform geo-based protocols in terms of network lifetime. The primary reason for this behavior is that location-based protocols consume energy in terms of localization services. Moreover, the number of control messages plays a vital role in the network lifetime.

D. Communication Model

Radio interference, antenna shape and orientation, distance and environmental factors may vary during the network lifetime and affect link quality between the sensor nodes [20]. Despite the fact that the locations of sensor nodes are fixed as well as every node is configured with the same transmission range, environmental variations result in asymmetric links between nodes [24]. Therefore, these routing approaches shall estimate link quality to find the optimal path. Considering that the communication is at varying-range scale, the study of the communication in very short range is essential. And hence, we consider the proposed path loss formula in [34] at Short-range communication, which has two parts: the absorption path loss and the spread path loss. Meanwhile, energy-aware frameworks depend heavily on two main principles in their communication design. First principle is the number of hops without delay constraint. Second, is the number of hops with the delay constraint.

Number of Hops without Delay Constraints

If there is no delay constraint on the system, the highest achievable transmission rate is given by equation 18 in [34]. The bandwidth is divided into i sub-bands the i-th sub-band is centered around frequency $f_i, i = 1, 2, \ldots$ and it has width Δf. If the sub-band width is small enough, the channel appears as frequency-nonselective and the noise p.s.d. can be considered locally flat. The resulting capacity in bits/s is then given by where d is the total path length, S is the transmitted signal p.s.d., A is the channel path loss, and N_0 is the noise p.s.d. Based on [35], we find the end-to-end capacity of N hops path by

$$\boldsymbol{C_{e2e} = C_I(1 - F_{AVG})^N} \qquad (3)$$

where C_I is the channel capacity contributed by the first hop, N is the hop count determined by the forwarding scheme and F_{AVG} is the average capacity loss factor per hop. The value of F_{AVG} is calculated as follows:

$$\boldsymbol{F_{AVG} = F\left(\frac{d_0 - d_{AVG}}{d_0}\right)} \qquad (4)$$

where F is the capacity loss factor and d_o is a constant that denotes the reference distance from source-to-sink [35].

Number of Hops with Delay Constraints

The predictions about the preferred number of hops made in the previous section were based on the assumption that the block lengths used by channel codes can be randomly large. In many applications there is a strict limit on the tolerable end-to-end delay. There are several factors of delay in short-range communication systems. In the following we list these factors:

- *Waiting* for the data source to emit enough bits to form a block of a desired length (for channel coding);
- *Processing* delay caused by encoding/decoding the information bits for transmission;
- *Transmission* and *reception* of the whole encoded message.

If the communication system involves multiple hops, the latter three elements are repeated several times, increasing overall delay. To compensate for this, shorter block lengths must be used at a cost of reduced error-correcting capabilities at each link [28].

IV. Cognitive Energy-Efficient Approach (CEEA)

In this section we propose a novel energy aware data delivery approach for the energy-constrained IoT. Let's assume that a randomly selected sensor n by GCN, depending on the harvested energy, is to be used for data retrieval. The random number of relay nodes within the communication range of the sensor n can be characterized by a spatial Poisson process X. Let the sensor n be at point $z \in \mathbb{R}^2$ and define $l(z, X)$ as the shortest distance from the sensor location z to the nearest point of X such that $l(z, X) \le r$, and only common control channels are considered. Since X is a spatial Poisson process, then $l(z, X) \le r$, if and only if $RN(d(z, r)) > 0$, where $d(z, r)$ is a disc of radius r centered at z. Conclusively, the probability of having at least one relay neighbor within the transmission range of the sensor n is given as follows.

$$P(l(z, X) \le r) = 1 - exp(\beta_{harv} A_d(d(z, r))) \qquad (5)$$

where A_d is the area of the disk $d(z, r)$, and where β_{harv} denotes the rate of harvested energy of a senor. Note that $exp(\beta_{harv} A_d(d(z, r)))$ denote the probability that no relay node is within the transmission range of the sensor n; i.e. the network lifetime of the neighborhood of sensor n is expired. When the lifetime of the neighborhood nodes is expired, the IoT-network is assumed dead. Thus, assuming $f(n_j)$ is the cost function of transmitting from RN_j to GCN, $g(n)$ is the energy of neighboring RNs, $h(n)$ is the minimum distance from a neighbor RN_j to GCN, $i(n)$ initial energy of the neighboring RN. Our approach relies on a "*cognition process*" that has three main criteria in data routing: 1) Evaluation criteria; $f(n_j)$= Cost(Neighbor RN to GCN) and $h(n_j) = min(f(n_j))$, this is guaranteed by lines 11 to 18 in Algorithm 1.a, 2) Selection criteria; $g(h(n_j)) > i\,(h(n_j)) * 50\%$, this section is found between lines 19 and 21, and 3) Termination Criteria; all one-hop RNs are dead or $P(l(z, X) \leq r) = 0$.

Algorithm 1.a: Pseudo-code of the CEEA algorithm.

1 **Function: Cognition process in CEEA**
2 **Input**
3 Source RN
4 **Output**
5 RN index chosen by CEEA to deliver data towards GCN.
6 **Begin**
7 **Initialize**
8 Hop Count =0; //for RNs beginning of round.
9 Identify source RN as a start node for current round.
10 List all neighbor RN indices from source RN
11 **If** source RN has one-hop, send directly to GCN.
12 **Else If** there is least one RN connected with this RN
13 **For** each source RN index 'j' do
14 $f(n_j)$= Distance (Neighbor RN to GCN)
15 $g(n_j)$= Energy (Neighbor RN's energy)
16 $h(n_j) = min(f(n_j))$
17 $i(n_j)$= InitialEnergy (RN's initial Energy)
18 **End**
19 **If** $g(h(n_j)) > i\,(h(n_j)) * 50\%$
20 Chosen RN Index = $g(h(n_j))$
21 **End**
22 **End**
23 **End**
24 **Else**
25 There is no source RN
26 **End**
27 **If** RN's energy when connected with GCN < 0,
28 **Then** disconnect from path
28 **End**
29 Update neighbor energy information of source RN
30 **Termination Criteria**
31 $P(l(z, X) \leq r) = 0$ in Eq. (5) is equal to 0.
32 **End**
33 **Return** $g(h(n_j))$

In the above Algorithm, elements of cognition in the utilized *cognition process* form the two main constituents of our proposed approach. The elements that help in implementing cognition in the cognitive nodes are: *reasoning* and *learning* elements.

A. Learning

Learning is used in our CEEA approach in order to determine the most appropriate paths towards the GCN that satisfy the

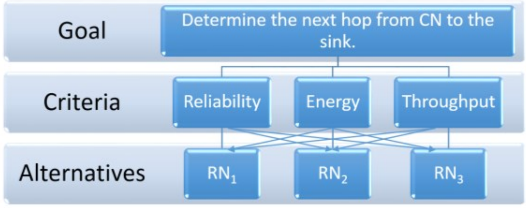

Fig. 3. The AHP Hierarchy.

IoT-network requirements. This cognition element uses a direction-based heuristic to determine the data delivery path through RNs that lie in the direction of the GCN. Hence, each time the *cognition process* has to choose the next hop, the direction-based heuristic eliminates RNs that increase the distance between the current RN and GCN. Knowledge of the positions of the CRN and its one-hop RNs is used by the heuristic to determine the set of such RNs, which we call forward-hop-RNs. Thus the forward-hop-RNs of a CRN identified by the direction-heuristic is constituted by those RNs that reduce the distance between the CRN and the GCN. This information is stored in the CRN for use in the next transmission rounds. Thus the direction-based heuristic, along with feedback from the network about the chosen paths helps the *cognition process* to learn data delivery paths to the sink, as the network topology changes.

Example 1: Assume S_1 and S_2 have data to be sent to destination nodes D_1 and D_2. R_n are all the available relays towards the destination. Out of these relays, it is determined that R_5 as shown in Fig. 1 has the lowest link outage probability to D_1 and D_2. Therefore, S_1 initiates routing data to R_5. Meanwhile, S_2 also forward a high traffic of data to R_5 (depicted by solid paths in Fig. 1). When multiple source nodes start routing their data to R_5 as well, the route to R_5 may get congested. A cognitive network with *learning* capabilities will be able to identify the congestion at R_5 (by observing the decrease in throughput). Sharing this observation with neighboring nodes, the cognitive IoT-network would be able to respond to the congestion proactively, by routing the data through a different path involving nodes R_4, R_8 and R_9 as shown in Fig. 2.

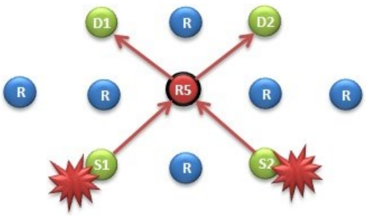

Fig. 1. Classical routing in a sensor network.

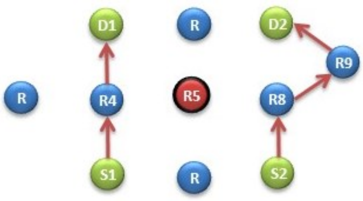

Fig. 2. Cognitive routing in IoT-networks.

B. Reasoning

In the CEEA approach, we assume a modified version of the Analytic Hierarchy Process (AHP) [36] for implementing the reasoning element of cognition in the IoT. AHP supports multiple-criteria decision making while choosing the data path. For example, if we have a delay-sensitive data, the node which provides the lowest delay, will be chosen even though it might degrade other metrics such as the network energy or throughput. If two next-hops guarantee the same delay then the next attribute to compare will be energy, and then, throughput, assuming that energy is the next desired attribute in the IoT-network. AHP provides a method for pair-wise comparison of each of the attributes and helps to choose the node that can provide the best network performance on the long run. The following subsequent example has more details on the utilized AHP. While AHP calculations help in deciding the next-hop, it also help in planning for future actions. The *cognition process* enables the CEEA approach to maintain the calculated values of the IoT-network attributes, which can be used in future transmission rounds. Hence, these values are not necessarily calculated at every transmission round.

Example 2: Assume a three level hierarchy in the AHP: *Goal*, *Criteria* and *Alternatives* as shown in Fig. 3. A fundamental scale for pairwise comparisons is then used to set priorities for the IoT-network attributes/criteria at the CNs. Given the very limited energy constraint in IoT, we would assign the highest priority to energy, followed by *reliability* and then *throughput*. We tabulate the relative priorities of these attributes using pair-wise comparison in [36] and generate Table I. From Table I we generate Table II. Then, we apply the following steps:

1. *Represent the values of Table II in the matrix form*

$$A = \begin{bmatrix} 1 & 4 & 6 \\ 1/4 & 1 & 3 \\ 1/6 & 1/3 & 1 \end{bmatrix}$$

2. *Compute the Eigen vector of the matrix A,*
3. *Isolate the absolute, real values of the Eigen vector,*
4. *Compute the relative priority values.*

Note that our goal is to find the best next-hop, which provides the highest value for a specific attribute, as shown in Table III.

Table I. Pair-wise comparison of the IoT-network attributes.

Energy (Kj)	4	Reliability	1
Energy (Kj)	6	Throughput (Mbps)	1
Reliability	3	Throughput (Mbps)	1

Table II. AHP for QoI Attributes v/s Goal.

Goal - Best attribute	Energy (Kj)	Reliability	Throughput (Mbps)	Relative Priorities of the attributes
Energy (Kj)	1	4	6	0.691
Reliability	1/4	1	3	0.2176
Throughput (Mbps)	1/6	1/3	1	0.0914

Table III. AHP evaluating the overall priorities for all possible RNs.

Best candidate for next hop RN_x	**Priority with respect to**			
	Energy (Kj)	**Reliability**	**Throughput (Mbps)**	**Goal**
RN_1	0.252	0.015	0.101	0.375
RN_2	0.2	0.018	0.11	0.329
RN_3	0.164	0.019	0.116	0.296

Algorithm 1.b: AHP analysis for path selection in *cognition process*

1. **Function AHP (priorities of the attributes P)**
2. **Input**
3. P: End-user defined priorities on the attributes for requested data
4. **Output**
5. RN_x: Forward-hop $RN_x \in \{ RN_1 \ ..... \ RN_n \}$ with best P
6. **Begin**
7. **Initialize**: priority matrix for traffic type; Success=0;
8. **While** $P(l(z, X) \leq r) > 0$ in Eq. (5)
9.   *AHP_analysis*(Next-hop RNs v/s attributes)
10.   Next hop $RN = RN_x$
11.   Transmit data to next-hop RN
12.   **If** (next hop = GCN)
13.   Success=1;
14.   **Else**
15.   *Choose next-hop RN*
16.   goto step 8
17.   **End**
18.   **If** *(Success==0)*
19.   GCN Retransmits request
20.   **End**
21. **End**

If energy consumption is measured as a function of the number of events taking place before the data packet arrives to the sink, the hop count can be used to approximate the energy cost. Accordingly, the modified AHP steps in prioritizing the IoT-network attributes and identifying the best next-hop are described in Algorithm 1.b.

V. Performance Evaluation

In this section, we evaluate the performance of the proposed CEEA. We use MAEB, GEAR, ReInForM and LinGo algorithms as baseline evaluation algorithms. Based on the aforementioned system models, we summarize these four baselines' categories as follows.

Geographic and Energy-Aware Routing (GEAR)

In this approach, sensor nodes must have a hardware component for positioning such as a GPS unit or a localization system. GEAR routing protocol is used to improve the efficiency in terms of energy consumption via forwarding queries to targeted regions. The forwarding scheme operates at two phases; *setup* phase and *operation* phase. Setup phase designed to assist sensor nodes in measuring their distances from the anchors. In the operation phase, a source sensor node incorporates its location information in a packet header. A receiving node checks its location, the destination location and source location for either forwarding or dropping the received packet.

Reliable Information Forwarding Using Multiple Paths (ReInForM)

ReInForM employs a probabilistic flooding procedure to deliver information-aware packets at a predetermined priority level. This leads to more reliable routing protocol at a proportional data delivery cost. The routing mechanism is based on local knowledge of network conditions, such as channel error, and hop-count to sink.

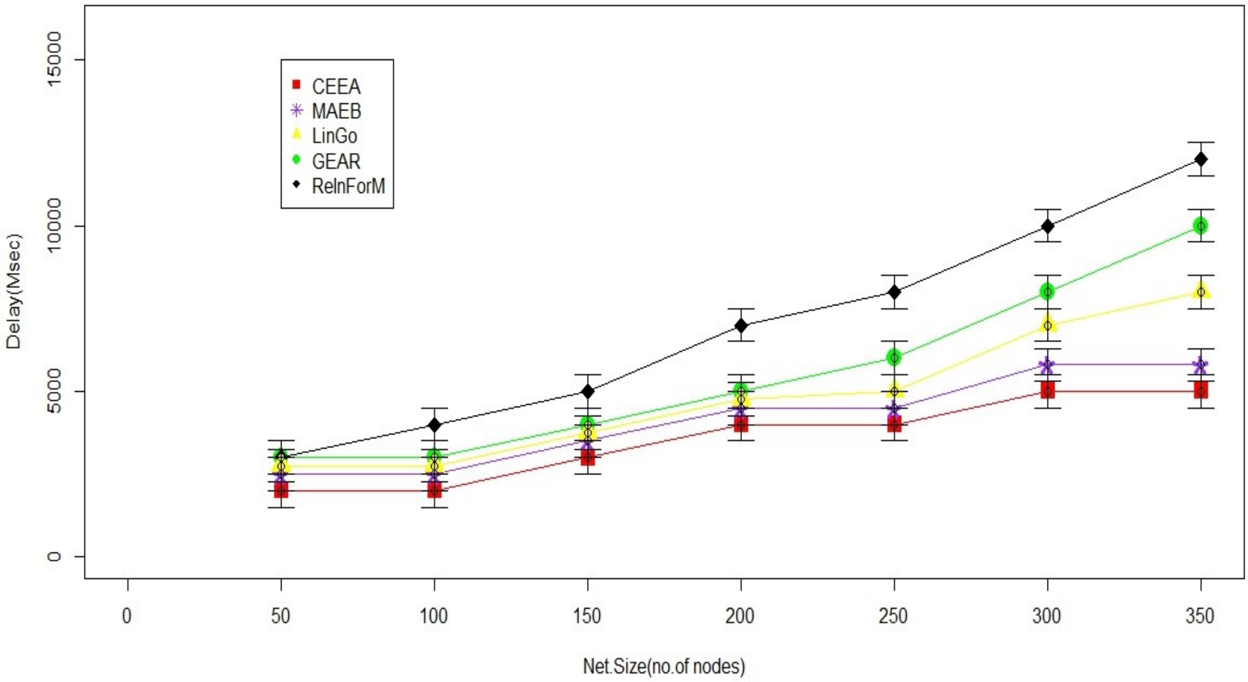

Fig. 4. Delay vs. the number of nodes in an IoT network.

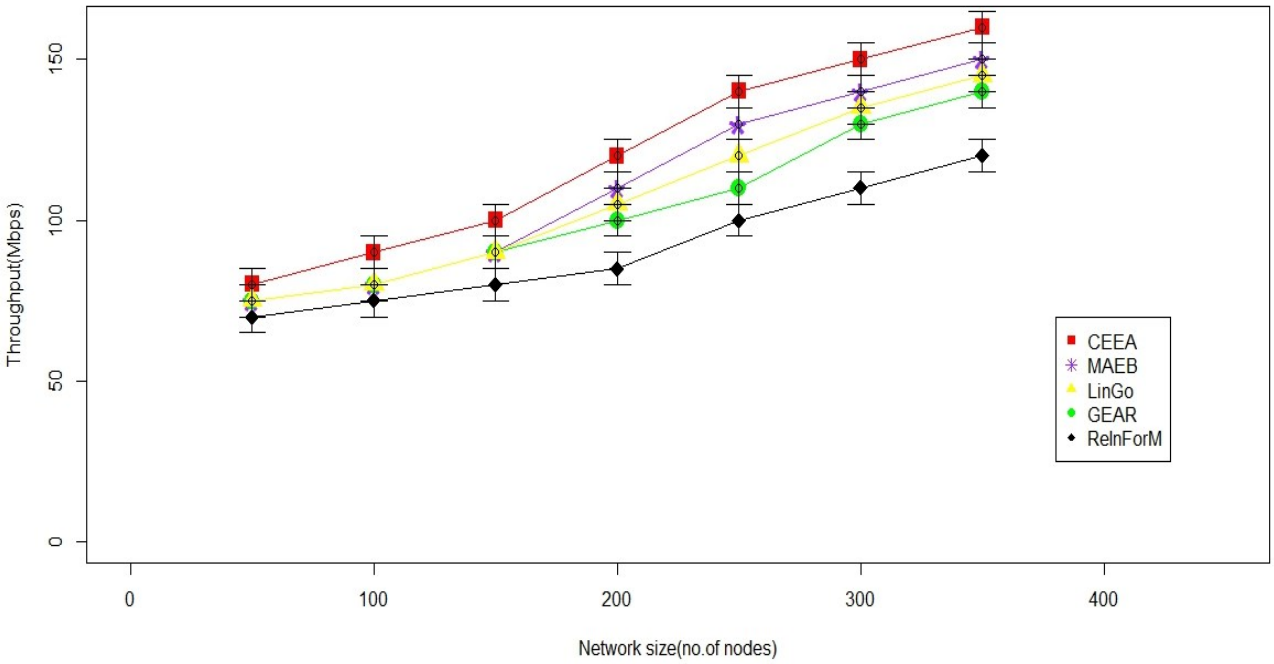

Fig. 5. Throughput vs. the network size.

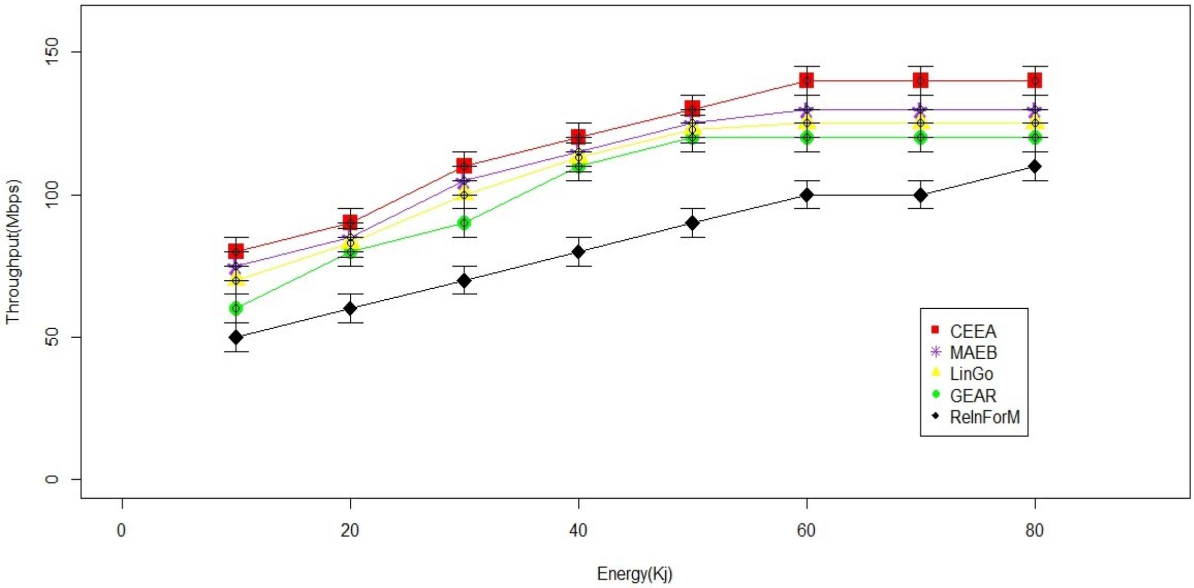

Fig. 6. Throughput vs. the energy consumption.

Movement-Aided Energy-Balance (MAEB)

MEAB has been chosen as a baseline due to movement and energy consideration. It has a neighbor discovery procedure which is conducted by the network cluster heads. They send their data packet to the Gateway following a forwarding rule, in which the distance and velocity to the Gateway and the remaining energy is recorded to select the neighbor cluster heads on the route towards the Gateway.

Link quality & Geographical beaconless OR protocol (LinGo)

LinGo introduces a different progress calculation approach compared to the aforementioned ones [37]. It takes into account both the progress of a given forwarding node towards the destination with respect to the last-hop, as well as the radio range. In this way, LinGO reduces the number of required hops on a data towards the destination node.

Cognitive Networking with Opportunistic Routing (CNOR)

CNOR protocol [38] is designed mainly for scalable WSNs, and tries to combine the advantages of opportunistic routing and opportunistic spectrum access. It is a reactive routing protocol since it discovers routes only when desired. An explicit route discovery process takes place only when it is needed. The destination node of the network begins the route discovery

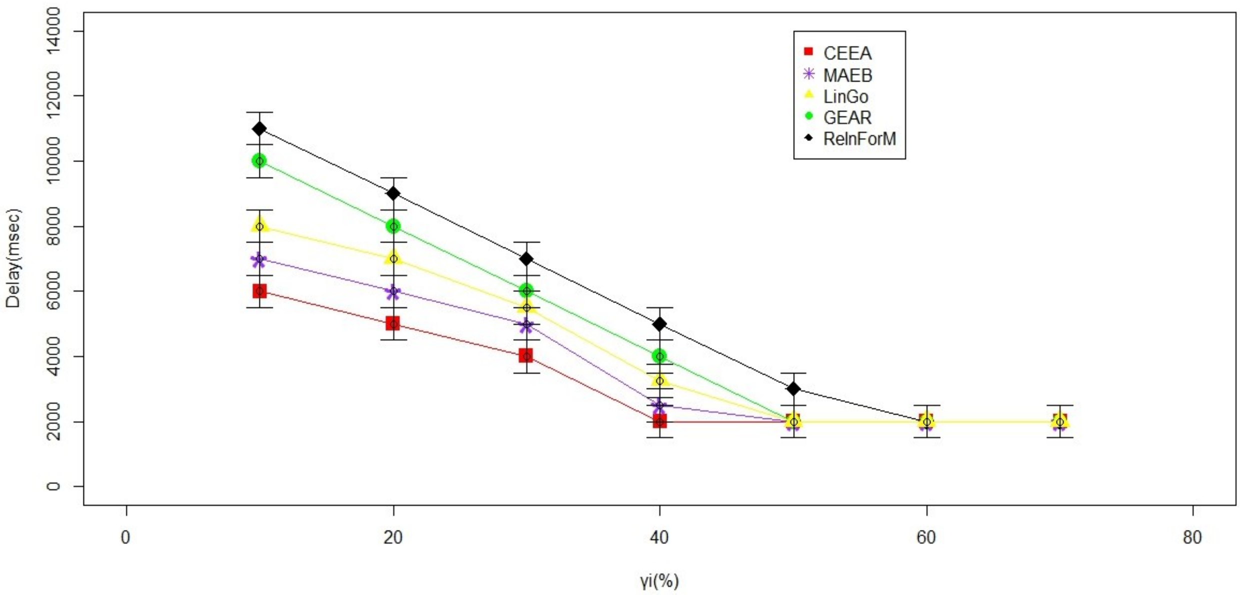

Fig. 7. Delay vs. the average γ_i rate percentage.

process and this process ends when a routing path has been established while a maintenance procedure preserves it until the path is no longer available or desired. As the network scalability is increased, CNOR tends to discover more paths leading to the increase of the network performance.

Energy-Aware Routing for Cognitive Networks (EARCN)

EARCN scheme [39] associates the backward difference traffic moments with the sleep-time duration to tune the activity durations of a node for achieving optimal energy conservation and alleviating the uncontrolled energy consumption in wireless devices. It provides efficient cognitive routing protocol in terms of maximum energy conservation, maximum-possible routing paths establishments and minimum delays, while utilizing secondary communication nodes (e.g., CRNs).

Resilient IoT for Dynamic Sensor Networks (RIDSN)

RIDSN extends AODV protocol to match needs of cognitive ad hoc networks in the IoT paradigm. It dissects the study of any IoT nodal capacity to its "connected" components, and empowers dynamic associativity between things to serve varying functional requirements and levels [40]. More importantly, critical resources in the network will be shared within their neighborhoods. Thus network lifetime will relate to functional cliques of dynamic IoT nodes, rather than individual networks.

A. *Performance Metrics & Parameters*

To compare the performance of these five schemes, the following four performance metrics are used.

1) *Average Delay:* is measured in *msec* and is defined as the average amount of time required to deliver a data unit to the destination.

2) *Idel time:* this metric reflects the ratio of idle time every node spend while just waiting to forward a message. It is measured in μsec.

3) *Throughput:* is set here as a quality measure. It is the average percentage of transmitted data packets that succeed in reaching the destination reflecting the effect of node heterogenuety and delay in IoT setups over the utilized data delivery approach.

4) *Average Price:* this metric is used to observe the influence of the utilized data delivery approach on the overall price to deliver a data unit from source to destination on average. The price charged by each node $\boldsymbol{n_i}$as $\boldsymbol{p_i}$.

$$p_i = \gamma_i * \left[\frac{E_{Tx}(D_k, n_j) + E_{Rx}(D_k)}{e_i} + \boldsymbol{\acute{\pi}_\imath} + \boldsymbol{\acute{u}_\imath}\right] \qquad (6)$$

where $\boldsymbol{\acute{u}_\imath}$ is the available buffer space at node i, and $\boldsymbol{\acute{\pi}_\imath}$ is the power amount to be consumed per packet processing at node i. $E_{Tx}(D_k, n_j)$ *and* $E_{Rx}(D_k)$ are the mounts of energy used to transmit a data packet D_k from node i to j and receive a data packet D_k at node i, respectively. And $\boldsymbol{e_i}$ is the instantaneous available energy per node i.

Meanwhile, the three data delivery performance is assessed using the following three parameters:

1) The size of the network in terms of total node count. This reflects the application's complexity and the scalability of the exploited routing scheme. Knowing that larger node count in a data path raises the risk of node failure and, hence, dropped packets.

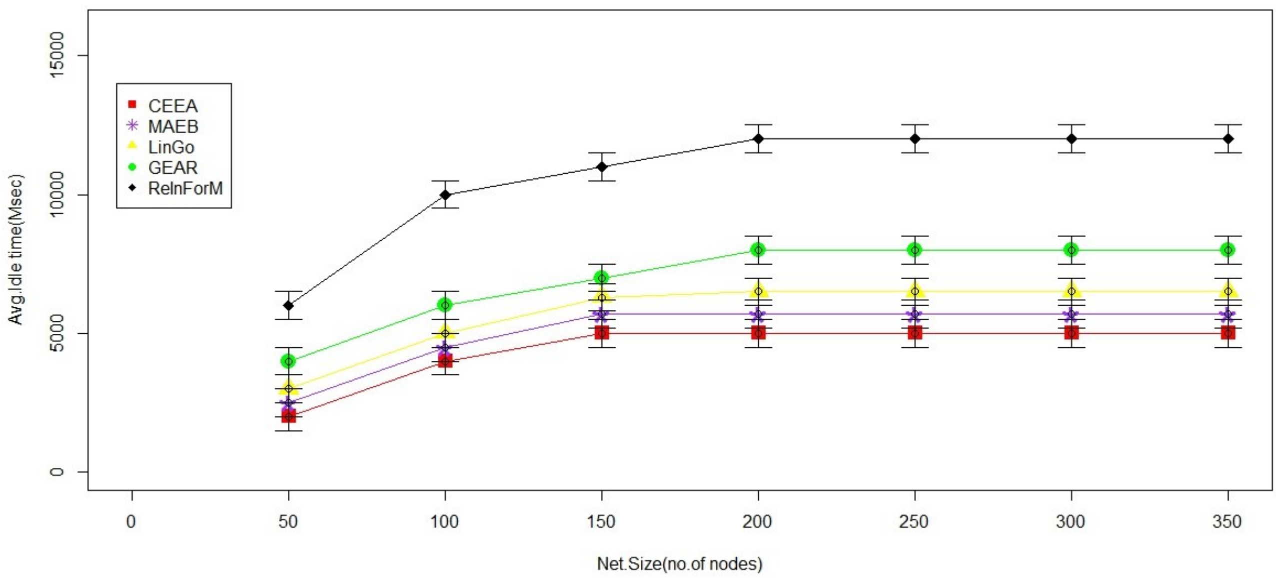

Fig. 8. Avg. idle time vs. the network size.

2) Energy: Average energy consumption rate per data unit ($\acute{\pi}_\iota$) as an indicator of the network power saving. This metric is measured in *Kjoule*. This parameter is thus asumed to be always greater than zero in the following simulation results.

3) PNF (%): It is the probability of a physical damage and/or a battery depletion for the deployed sensor node due to a disaster harsh-operational conditions. This parameter is chosen to reflect the impact in case of disaster scenarios or fragmented networks in IoT.

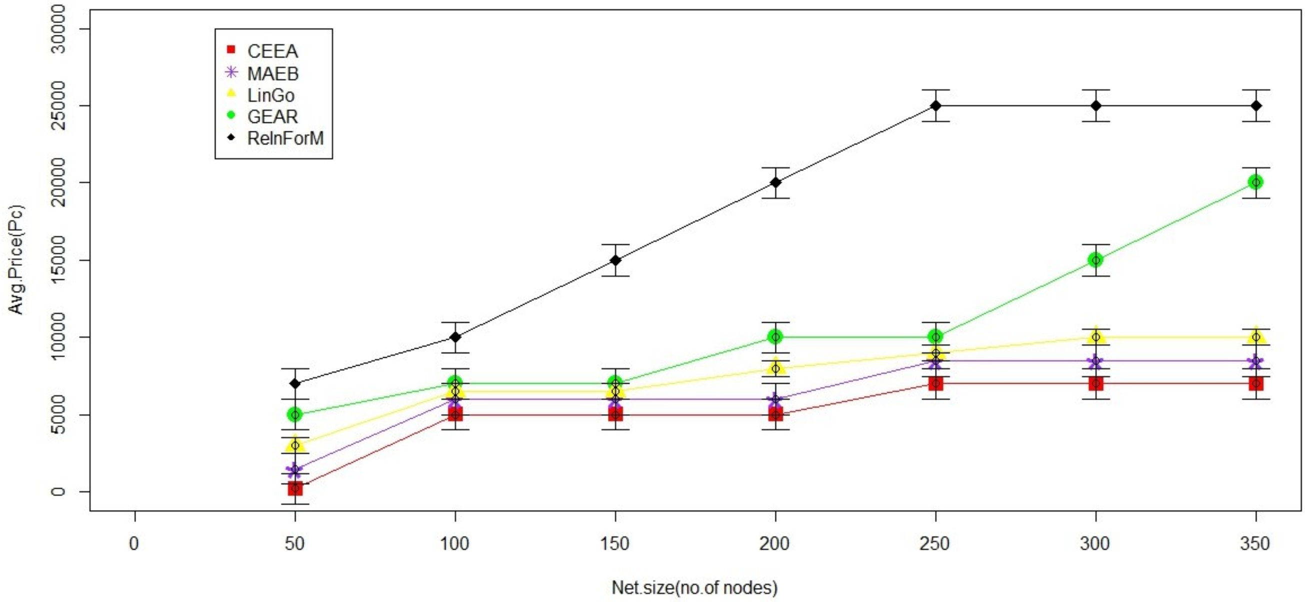

Fig. 9. Avg. price vs. the network size.

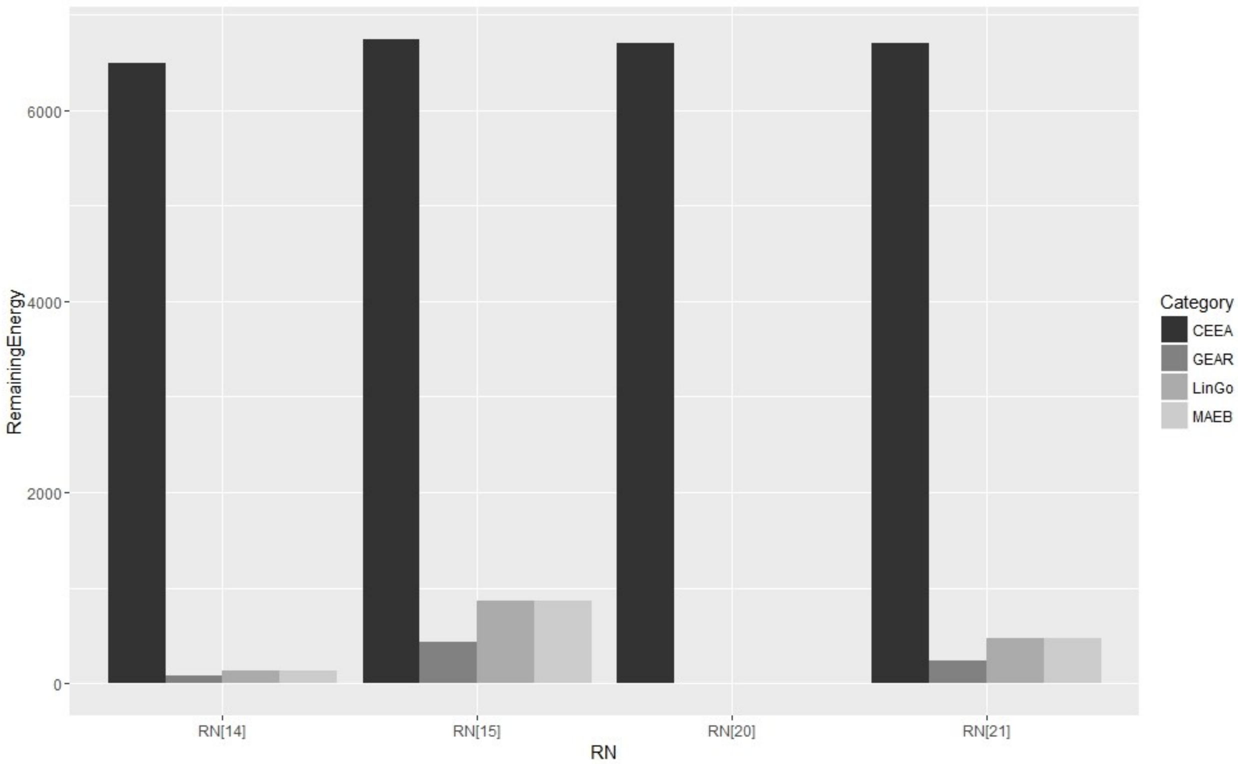

Fig. 10. Comparison of One-hop RNs' Energy Level.

4) Cost ($\boldsymbol{\gamma_i}$) to observe the influence of the charged price rate over the utilized data delivery approach. It is a pricing factor for each node in the IoT measured in *$/byte*. This is can be set as a flat rate per number of bytes transmitted, where setting it to a relatively high value would diminish the chances of $\boldsymbol{n_i}$ to be selected for relaying the data packet D_k.

B. Experimental Setup

In order to limit our search space, we assume a virtual grid, where SNs are placed on the grid vertices. We assume up to 1500 total SNs communicate with one GCN via 36 RNs. We used NS3 as simulation tool for this purpose. The simulation is processed in three platforms which are Windows, Linux and OSX for validation purposes. We executed our simulation 100 times for each experiment and plotted the average results. More details about our simulation are summarized in Table IV.

Table IV: Simulation parameters and values.

Parameter	Value
Targeted area	1000m x 1000m
Number of nodes	SNs: 350, RNs: 36, GCN: 1
Communication Range	SN: *142m*, RN: *300m*, GCN: *500m*
Initial Energy	SN: *31104J*, RN: *110160J*, GCN: *Unlimited*
Energy Consumption	SN and RN (Receiving): *31.2 uJ/bit* SN and RN (Transmitting): *53.8 uJ/bit*

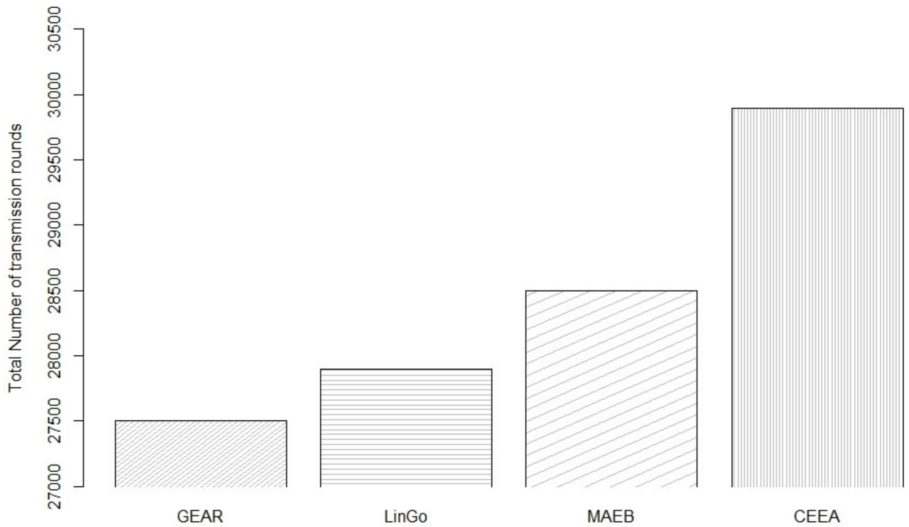

Fig. 11. Comparison of the 4 data delivery techniques based on total number of transmissions.

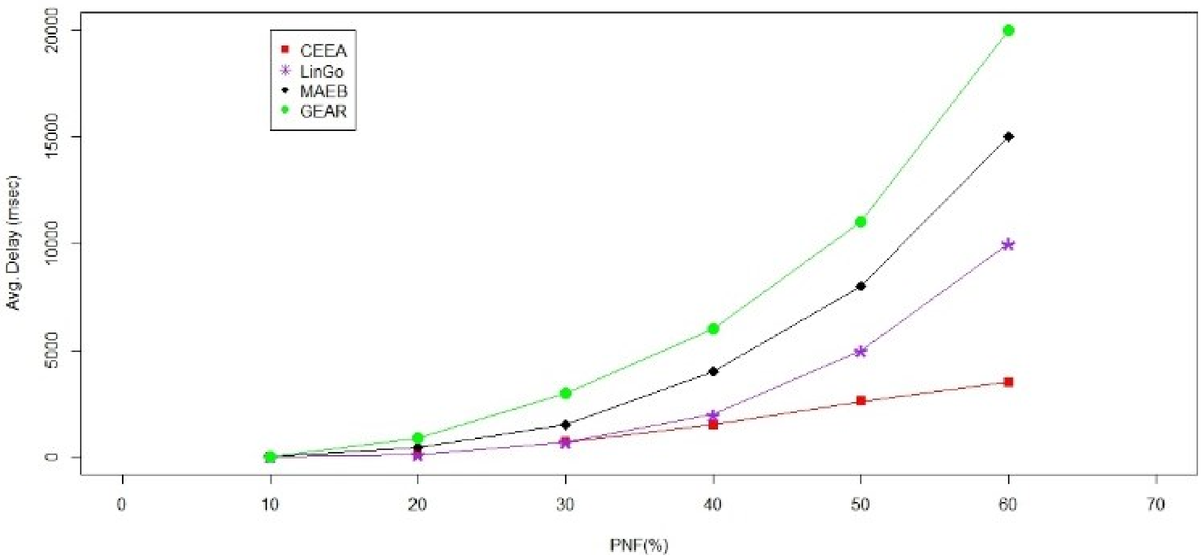

Fig. 12. Average delay versus the probability of node failure in the network.

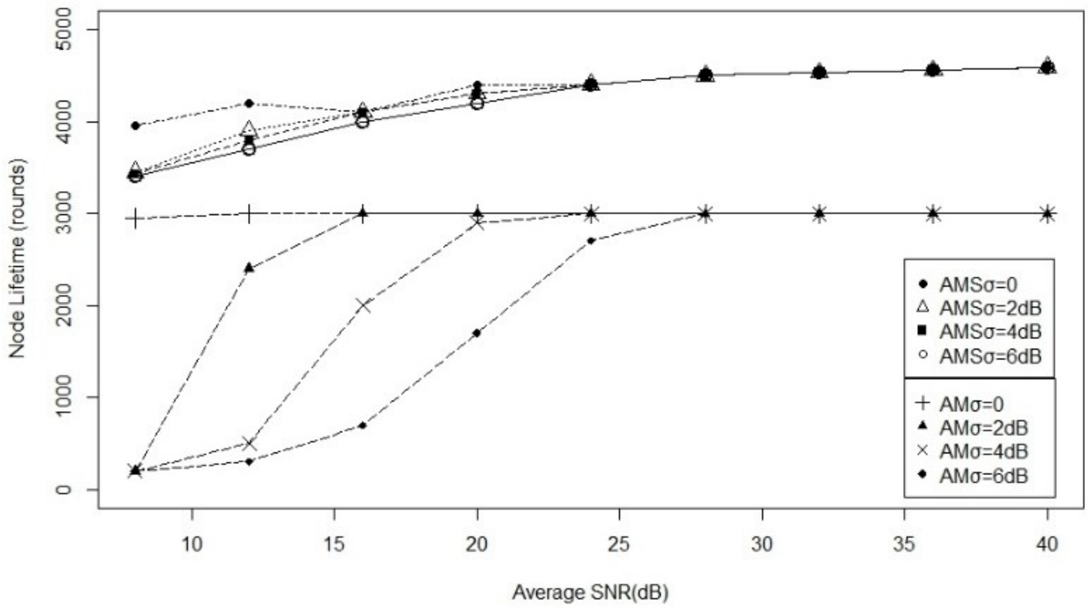

Fig. 13. Node lifetime using Adaptive Modulation (AM) vs. Adaptive Modulation and Adaptive Sleep (AMS).

C. Simulation results

In Fig. 4, the experienced delay in delivering data packet is plotted against the size of the network for the different simulated algorithms. We observe that ReInForM has the highest delay, while CEEA has the lowest delay as the number of nodes increases. Therefore, we can say that CEEA is more delay-tolerant in comparison to all of the sampled algorithms. We also observe that there is a monotonic increase in delay for ReInForM algorithm, while MAEB has a slightly higher delay than CEEA with a constant difference at every node. For CEEA and MAEB, we observe a steep increase between 100 and 200 nodes while RelnForM has its steepest slop between 150 and 200. For LinGo and GEAR we observe a fairly continues increase in delay as the number of nodes increase since they are more dependent on the network nodes' geolocations.

Fig. 5 shows the experienced network throughput versus the number of nodes for the sampled algorithms. We can observe that there is a general increase in throughput of the sampled algorithms as the size of the network increases. MAEB, LinGo and GEAR have the same throughput until the size of the network is about 150 nodes, after which MAEB gives a higher throughput. Also, it's worth remarking here that LinGO adds redundant packets in order to increase the packet delivery probability while experiencing link error periods. This leads to significant increment in the overall throughput in comparison to GEAR and ReInForM methods. From the graph, we can also observe that in all instances, CEEA has a higher throughput than the others do, and ReInForM has the lowest throughput. And hence, we can conclude that CEEA has a better throughput as the network size increases compared to the sampled algorithms. This can be returned to the efficient retransmission approach in CEEA algorithm in comparison to other approaches in the literature. This makes it also the most scalable approach for the next generation IoT networks where the connected network nodes are dramatically increasing a day after a day.

Plotted curves in Fig. 6 show the average consumed energy against throughput for the different examined algorithms. We notice that there is almost a liner increase in energy consumption while applying the RelnForM approach as the network throughput increases, while CEEA, GEAR, LinGo and MAEB forms a concave-like curves. We also observe that for every amount of energy consumed, RelnForM has the lowest throughput. While on the other hand, CEEA has the highest throughput for the same amount of energy. For this reason, we can conclude that CEEA is the most efficient algorithm in terms of energy consumption compared to the sampled ones. Moreover, we notice that when the energy budget is greater than or equal to 60 *Kjoule*, the network throughput is saturated due to other design factors such as the network size and cost factor ($\boldsymbol{\gamma_i}$).

Fig. 7 shows the average charged cost ($\boldsymbol{\gamma_i}$) per network node i against the experienced data delivery delay for all the simulated approaches. From this figure we can observe that with the increase in gamma, there is a general decrease in delay time for all the sampled schemes. Which is an expected network behavior as the flat rate charge increases per node. We also notice that all the schemes reach a certain threshold where the delay becomes constant at 2000 milliseconds. CEEA is the first to get to the threshold when $\boldsymbol{\gamma_i}$ equals to 40, while ReInForM is the last when $\boldsymbol{\gamma_i}$ equals to 60. GEAR and MAEB reaches the threshold at $\boldsymbol{\gamma_i}$ equals to 50. Consequently, we can say that CEEA is the most cost-effective scheme since it has the lowest delay time with the lowest $\boldsymbol{\gamma_i}$.

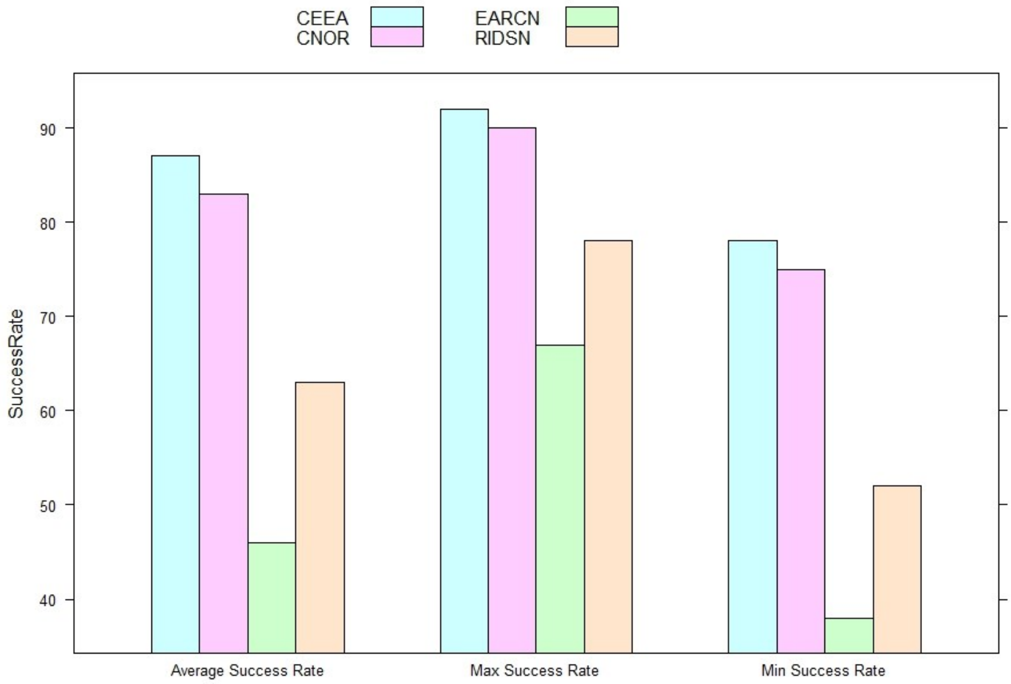

Fig. 14. Comparison of success rates.

In Fig. 8, average idle time is compared under varying total count of network nodes. As the network size, or the number of SNs increases, there is a general increase in the average idle time. However, we observe that CEEA has the lowest idle time compared to other baselines. From Fig. 8 we can also deduce that after a network size of 150 nodes, the average idle time of CEEA remains constant, which means it is not affected by the number of nodes. MAEB has a slightly higher idle time than CEEA whose difference to CEEA remains constant as the network increases in size. GEAR and ReInForM have an increasing idle time until 200 nodes, and then stay in a steady state. Therefore, we can conclude that CEEA is most efficient compared to the sampled baseline algorithms.

Fig. 9 depicts the network size against the average price of all the schemes. From the figure, we can observe that ReInForM has the highest average price. On the other hand, the CEEA approach has the lowest average price under all varying node counts. When the number of nodes reaches 250, the ReInForM approach has a constant and fixed average price. On the contrary, after a network size of 250 nodes, we observe a sharp and liner increase on GEAR and LinGo. Meanwhile, MAEB is the second most scheme that has the lowest average price after the CEEA approach. The achieved price curve of MAEB closely follows that of the CEEA. However, it is still worse than the CEEA. Therefore, CEEA has the best performance in terms of average price as well under all experimented network sizes. The reason is that GEAR, LinGO and MAEB approaches add redundant packets in order to increase the packet delivery probability while experiencing link error periods. This leads to significant increment in the overall price.

In Fig. 10, the Y-axis represents energy level of specified RN's and the X-axis represents the specified RNs and the algorithm types. The reason why RN_{14}, RN_{15}, RN_{20} and RN_{21} are selected is because these RNs have bidirectional connection with the GCN. To transmit packet to the GCN, one of these RNs must be used. We compare these RNs energy levels against the ReInForM, GEAR, LinGo and MAEB algorithms, since they are the most energy-efficient ones. Obviously, GEAR has the worst performance in this figure due to a fairness problem in this algorithm while relaying towards the sink node. Although the energy level of $RN_{14,}$ $RN_{15,}$ RN_{20} and RN_{21} are better for LinGo and MAEB, these RNs' energy levels are significantly outperformed by the CEEA approach. Thus, CEEA increases the network lifetime and it is better in energy saving. Furthermore, when we compare these algorithms in terms of the number of transmission rounds, it can be clearly observed from the simulation results in Fig. 11, that CEEA outperforms GEAR, LinGo and MAEB. Notably, the more savings in terms of remaining energy shown in Fig. 10 by applying the CEEA approach have led to prolonged network lifetime in Fig. 11.

Moreover, we examined the four routing approaches; CEEA, LinGo, GEAR and MAEB in terms of the average delay impacts (Fig. 12) while considering disaster scenarios and/or fragmented network, where failure of a critical node partitions the network into disjoint segments. Based on Fig. 12, we notice a sever effect on the average delay while the probability of node failure (PNF) is increasing. We notice that all approaches are experiencing an exponential increase in the experienced delay as the network becomes disconnected. However, using the proposed CEEA approach the increment is going linear, which can be a very desirable feature in IoT while experiencing harsh operational conditions and sever mobility effects.

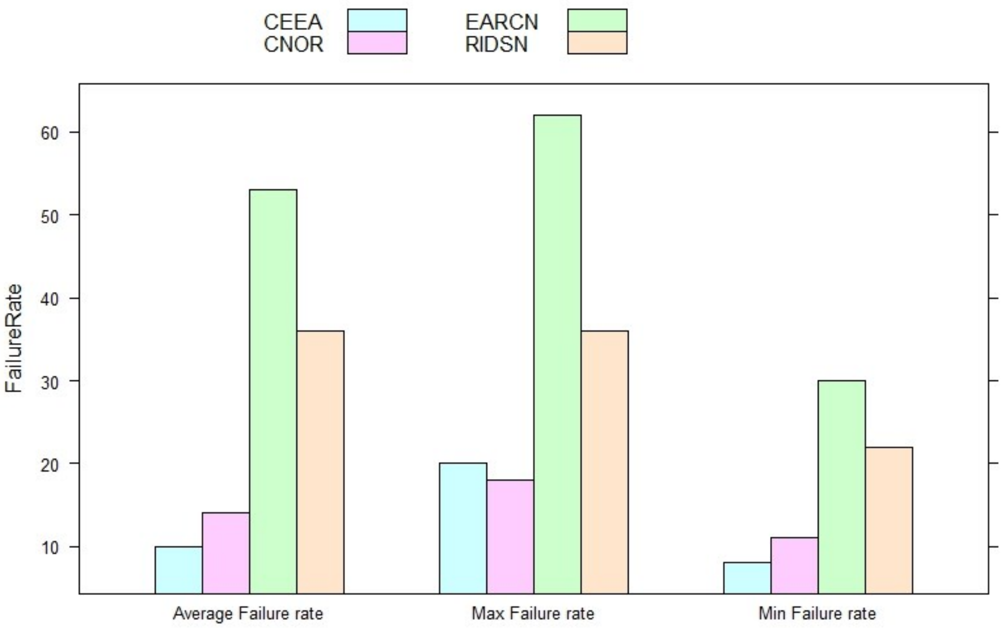

Fig. 15. Comparison of failure rate.

The good performance achieved by CEEA approach in this paper can be returned mainly to the utilized cognitive elements that help a lot in disaster scenarios. In fact, the proposed CRNs make use of the received feedback about the utilized channel condition and modulation rate to determine the sleep time of each node. This concept has been emphasized more in Fig. 7 while assuming realistic channel conditions as summarized in Table VI for energy consumption of the relay node in four modes: sleep mode, receive mode, active mode (ready to transmit but not transmitting), and transmission mode. Fig. 13 displays the mean node lifetime in the network using Adaptive Modulation and Adaptive Sleep (AMS) versus Adaptive Modulation (AM) only. In case of AM, the modulation level (parameter M in M-QAM modulation) is chosen for each packet according to channel condition (i.e. SNR). This case assumes no cognition and the sleep time is predetermined independently from the user requests and/or any changes to application requirements. Meanwhile, the same figure shows the average node life time using an adaptive modulation scheme combined with a scheduled sleep via the AMS mechanism that adapt based on the CRNs feedback. In other words, cognition here is employed at the MAC and PHY layers and sleep times are scheduled according to channel conditions and bit rates. In both cases high traffic patterns (mean packet arrival rate 90%) are assumed and simulated using Poisson distributions and log-normal shadowing where shadowing variance takes values

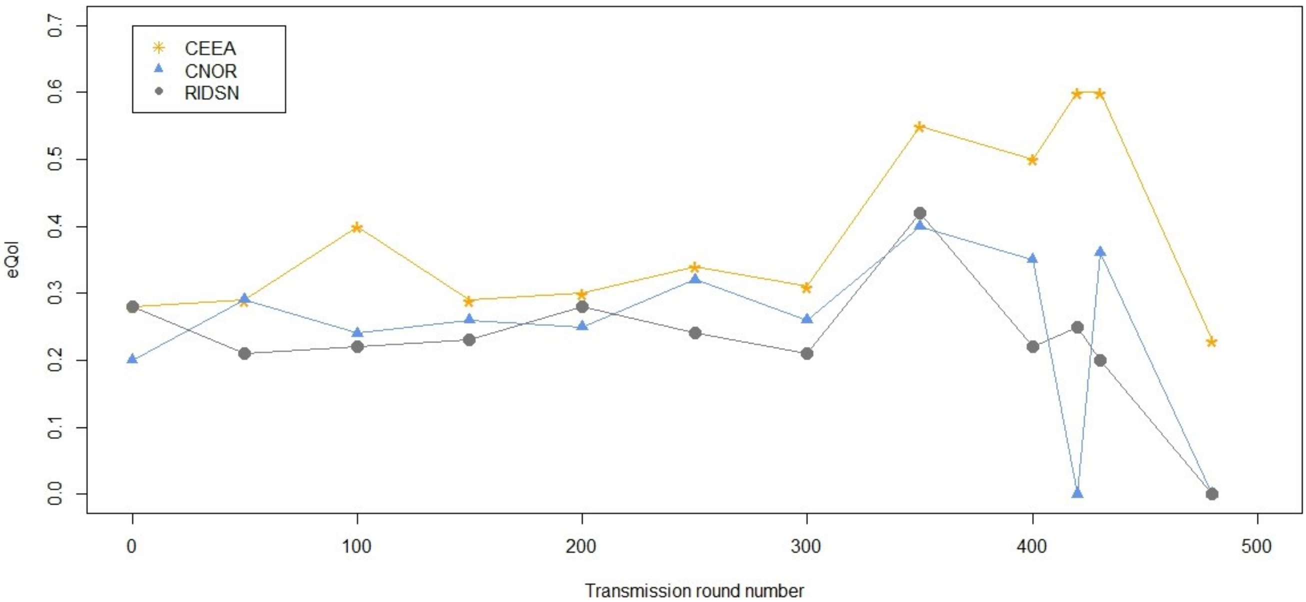

Fig. 16. Comparison of eQoI as observed at the sink over the network lifetime.

from 0 (no shadowing) to 6dB. The figure shows that the cognitive approach significantly outperforms the non-cognitive one in terms of the average node lifetime. This is because M-QAM modulation, when carefully chosen, will require less transmission time, and thus, the cognitive system exploits this information to modify the sleep time accordingly. The improvement made by the cognitive approach is higher for both high traffic intensity and severe channel conditions (i.e. low SNR and high shadowing variance).

Table V. Node parameters used in simulation based on [26].

Parameter	Value
Current consumption in Sleep mode: I_{sleep}	1 µA
Current consumption in Receive mode: I_{rx}	20 mA
Current consumption in active mode: I_{ac}	100 mA
Current consumption while transmitting	120mA
Traffic intensity	90%
Log-Normal Shadowing variance (σ)	0, 2dB, 4 dB or 6dB
BER required (QoS)	10^{-4}
RF Bandwidth used	200kHz

Considering the fact that the proposed CEEA technique is being developed for the use in a dynamic IoT environment, it is desirable to continuously improve the success rate of the data delivery in order to improve the in-network user's experience. Being more sure of getting a response back from the network for each of the queries sent out, can significantly improve the levels of the user's satisfaction with the network. However, the above mentioned benchmarks were not able to efficiently learn and adapt to dynamic network changes such as node failures and remaining energy in the IoT paradigm when we compared to the proposed CEEA data delivery approach. And thus, more cognitive benchmarks; such as CNOR, RIDSN and EARCN have been further investigated in this study against the proposed CEEA approach.

Fig. 14 and Fig. 15 compare the average, minimum and maximum values of success rates and failure rates respectively, for all of the four approaches. We can see that the CEEA approach has the highest average success rate of 88%, and its worst-case failure rate is only 3% more than CNOR. Since it is more desirable to have a higher success rate in smart IoT applications, we further compare the performance of CEEA and CNOR techniques in terms of their effective-QoI (eQoI) as observed at the Sink to identify the best approach of the two. Where the eQoI is the heuristics estimate of the QoI associated with data delivered to the sink at the end of a successful transmission round. In other words, it is an estimate for the value of QoI at the last hop that delivers directly to the sink.

Fig. 16 shows the result of the comparison of the eQoI values for CEEA, and CNOR, with RIDSN, which doesn't use any kind of learning at the CRNs. In general, we observe that using some form of learning at the CRNs improves the eQoI of the data delivered to the Sink. Among the learning techniques, we observe that CEEA performs the best in terms of consistently delivering data with higher eQoI at the sink, even towards the end of the network's lifetime. Now, this eQoI is the hop-by-hop value of QoI associated with the data delivered to the sink with respect to energy, reliability and throughput. In addition, the cumulative delay in receiving a response from the network for an initiated request by the sink node is reflected by the number of hops taken along the path from the source to sink.

Consequently, we compare the hop count against the network lifetime for CEEA, CNOR, and RIDSN, and the results are as shown in Fig. 17. The observation made from the compared techniques is the spike in hop count seen towards the end of the network's lifetime. This is because more number of nodes are lost due to node deaths as the simulations progress, making it increasingly difficult for the remaining alive nodes to find paths to deliver data to the sink. This search for alternate paths leads

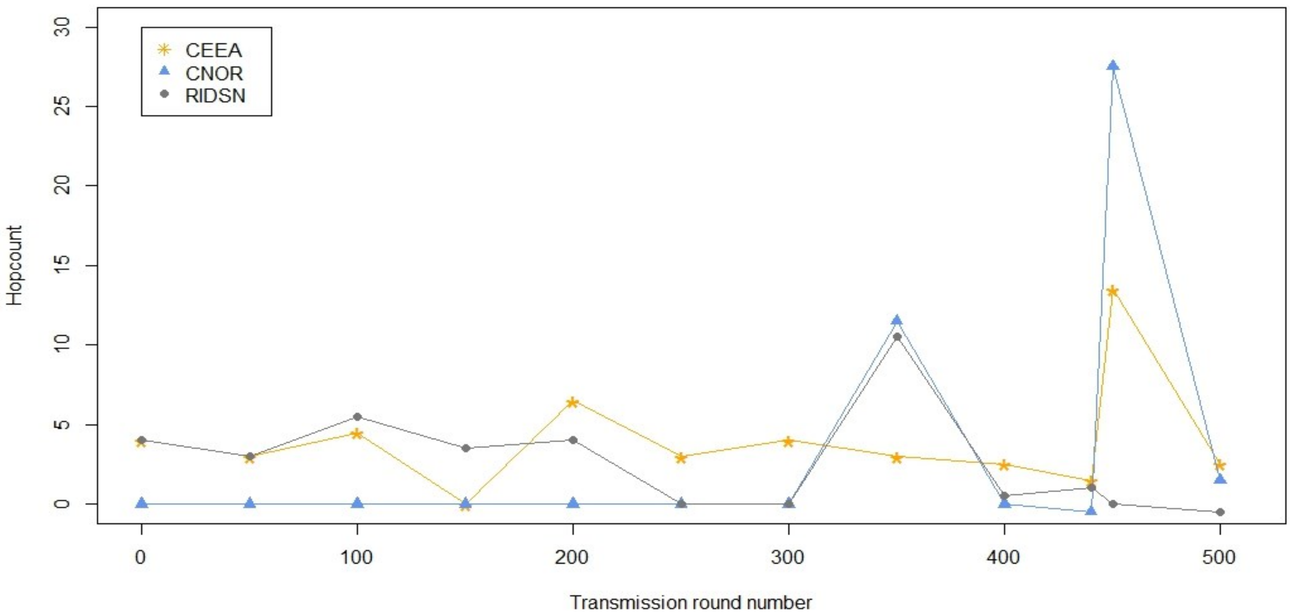

Fig. 17. Comparison of the average hop counts in delivering data from a source to the sink.

to an increase in the hop count. However, one of the marked differences between CEEA and CNOR is that CNOR has a constant hop-count of 2 till about 300 transmission rounds. This is because it starts out with exploiting its knowledge of paths through RNs that are one-hop away from the sink. But CEEA starts with exploring paths and eventually learns the network connections that helps to reduce the worst case hop-count towards the end of the network's lifetime. This difference in strategies accounts for the slightly lower network lifetime of CEEA when compared with CNOR, due to higher energy consumed in exploring the paths. However, when averaged over the entire network lifetime, CEEA is on average, 2 hops more expensive than CNOR, which rewards its higher average rate of successful data delivery and eQoI at the sink.

VI. Conclusion

In this paper, we investigated routing techniques for the IoT paradigm in terms of energy consumption, cost and delay, while experiencing harsh operational conditions and sever energy limitations. We proposed a novel approach for sensor-networks in IoT, called CEEA. We found that CEEA can save considerable amount of energy. Moreover, we showed how the data delivery price can be affected by the network size for varying energy-based routing approaches. Furthermore, the CEEA approach was compared to other cognitive routing approaches in Ad Hoc networks. It was able to provide a 40% improvement in average data delivery success rate, when compared with the RIDSN. CNOR approach performed equally well in terms of the data delivery success rate, but, performed slightly better than CEEA in terms of the energy consumed. On the other hand, the CEEA approach is a better choice when the application requires a higher eQoI at the sink, and higher best case success rate. Consequently, CEEA approach is recommended for disaster-inspired applications which could provide data for other approaches to identify disasters in real-time [41][42][43][44] and it outperforms key other baseline approaches in terms of transmission and energy consumption.

References

[1] F. Al-Turjman, H. Hassanein, M. Ibnkahla, "Efficient deployment of wireless sensor networks targeting environment monitoring applications", *Elsevier Computer Communications*, vol. 36, no. 2, pp. 135-148, 2013.

[2] Hijji, M., Amin, S., Iqbal, R., Harrop, W., "The Significance of Using Expert System to Assess the Preparedness of Training Capabilities against Different Flash Flood Scenarios", *Lec Notes on Software Engineering,* vol. 3, No. 3, pp. 214-219, 2015.

[3] F. Al-Turjman, H. Hassanein, W. Alsalih, and M. Ibnkahla, "Optimized Relay Placement for Wireless Sensor Networks Federation in Environmental Applications", *Wiley Wireless Communication & Mobile Computing*, vol. 11, no. 12, pp. 1677-1688, 2011.

[4] G. Tolle, J. Polastre, R. Szewczyk, D. Culler, "A macroscope in the redwoods", *In Proc. of the ACM Conf. on Embedded Networked Sensor Systems*, San Diego, 2005, pp. 51–63.

[5] M. Z. Hasan, F. Al-Turjman and H. Al-Rizzo, "Optimized Multi-Constrained Quality-of-Service Multipath Routing Approach for Multimedia Sensor Networks", *IEEE Sensors*, 2017. DOI: 10.1109/JSEN.2017.2665499.

[6] C. Dorazio, K-K. R. Choo, and L. T. Yang "Data Exfiltration from Internet of Things Devices: iOS Devices as Case Studies", *IEEE Internet of Things*, vol. PP, no. 99, 2016.

[7] Y. Yang, H. Cai, Z. Wei, H. Lu, K. R. Choo, "Towards Lightweight Anonymous Entity Authentication for IoT Applications", *In Proc. of the Australasian Conference on Information Security and Privacy*, Melbourne, Australia, 2016, pp 265-280.

[8] N. Cahyani, B. Martini, K. R. Choo, M. Al-Azhar "Forensic data acquisition from cloud-of-things devices: Windows smartphones as a case study", *Wiley Concurrency and Computation: Practice and Experience,* 2016. DOI: 10.1002/cpe.3855

[9] L. A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, M. Ayyash, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications", *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.

[10] S. Ali, S. Madani, "Distributed Efficient Multi Hop Clustering Protocol for Mobile Sensor Networks", *International Arab Journal of Information Technology*, vol. 8, no. 3, pp.302-309, July, 2011.

[11] T. M. Cover and J. A. Thomas, Elements of Information Theory, MA: Wiley Press, 1991.

[12] S. A. Nikolidakis, D. Kandris, D. D. Vergados and C. Douligeris, "Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering", *MDPI Algorithms*, vol. 6, no. 1, pp 6,29-42, 2013.

[13] A. Aburumman, and K-K. R. Choo, "A Domain-Based Multi-cluster SIP Solution for Mobile Ad Hoc Network", *In Proc. of the Int. Conf. on Security and Privacy in Communication Systems*, Beijing, China, 2014, pp. 267-281.

[14] A. Aburumman, W. Seo, C. Esposito, A. Castiglione, R. Islam, and K. R. Choo, "A Secure and Resilient Cross-Domain SIP Solution for MANETs using Dynamic Clustering and Joint Spatial and Temporal Redundancy", *Wiley Concurrency and Computation: Practice and Experience,* 2016. DOI: 10.1002/cpe.3978

[15] B. Deb, S. Bhatnagar, and B. Nath, "ReInForM: reliable information forwarding using multiple paths in sensor networks," *In Proc. of the IEEE Conf. on Local Computer Networks*, Bonn, Germany, 2003, pp. 406–415.

[16] L. Villalba A. Orozco, A. Cabrera and C. Abbas, "Routing Protocols in Wireless Sensor Networks", *MDPI Sensors*, vol. 9, no. 1, pp. 8399-8421, 2009.

[17] M. Z. Hasan, H. Al-Rizzo, and F. Al-Turjman, "A Survey on Multipath Routing Protocols for QoS Assurances in Real-Time Multimedia Wireless Sensor Networks", *IEEE Communications Surveys and Tutorials*, 2017. DOI: 10.1109/COMST.2017.2661201.

[18] T. Maniak, C. Jayne, R. Iqbal, F. Doctor, "Automated Sound Signalling Device Quality Assurance Tool for Embedded Industrial Control Applications", *In Proc. of the IEEE Int. Conf. on Systems, Man, and Cybernetics,* Manchester, UK, 2013, pp. 600-611.

[19] F. Doctor, C-H. Syue, J-H. Shieh, R. Iqbal, "Type-2 Fuzzy Sets Applied to Multivariable Self-Organizing Fuzzy Logic Controllers for Regulating Anesthesia", *Journal of Applied Soft Computing*, vol. 38, no. 1, pp. 872–889, 2016.

[20] F. Al-Turjman, "Cognition in Information-Centric Sensor Networks for IoT Applications: An Overview", *Annals of Telecommunications*, vol. 72, no. 1, pp. 1-16, 2016.

ACCEPTED MANUSCRIPT

[21] N. Kumar, R. Iqbal, S. Mistra, J. Rodrigues, “Bayesian Coalition Game for Contention Aware Reliable Data Forwarding in Vehicular Mobile Cloud”, *Elsevier Future Generation Computer Systems*, vol. 48, no. 1, pp. 60-72, 2014.

[22] H. Fang, L. Xu and K-K. R. Choo, “Stackelberg game based relay selection for physical layer security and energy efficiency enhancement in cognitive radio networks”, *Elsevier Applied Mathematics and Computation*, vol. 296, no. 1, pp. 153-167, 2017.

[23] H. Fang, L. Xu, Jie Li and K-K. R. Choo, "An Adaptive Trust-Stackelberg Game Model for Security and Energy Efficiency in Dynamic Cognitive Radio Networks", *Elsevier Computer Communications*, 2016. DOI: 10.1016/j.comcom.2016.11.012.

[24] M. Z. Hasan, F. Al-Turjman, H. Al-Rizzo “Evaluation of a Duty-cycled Protocol for TDMA-Based Wireless Sensor Networks*”, In Proc. of the IEEE Int. Wireless Communications and Mobile Computing Conf.*, Paphos, Cyprus, pp. 964-969, 2016.

[25] A. Tsioliaridou, C. Liaskos, S. Ioannidis, and A. Pitsillides, "CORONA: A Coordinate and Routing system for Nanonetworks." *In Proc. of the ACM Int. Conf. on Nanoscale Computing and Communication*, Boston, MA, 2015, pp. 1-6.

[26] F. Saghezchi, A. Radwan, J. Rodriguez, “Energy-aware relay selection in cooperative wireless networks: An assignment game approach”, *Elsevier Ad Hoc Networks*, vol. 56, no. 1, pp. 96-108, 2017.

[27] S. Mahmud, R. Iqbal, F. Doctor, “Cloud enabled data analytics and visualization framework for health-shocks prediction”, *Elsevier Future Generation Computer Systems*, vol. 65, no. 1, pp. 169–181, 2016.

[28] G. Singh, and F. Al-Turjman, “A Data Delivery Framework for Cognitive Information-Centric Sensor Networks in Smart Outdoor Monitoring”, *Elsevier Computer Communications*, vol. 74, no. 1, pp. 38-51, 2016.

[29] T. El Salti, D. Stacy, N. Nasir, and F. Al-Turjman, “Packet delivery significance and metrics improvements in protocols for 3-D routing in Wireless Sensor Networks” *In Proc. of the Int. Wireless Communications and Mobile Computing Conf.*, Nicosia, Cyprus, 2014, pp. 1130-1135.

[30] S. Oteafy, "A Framework for Heterogeneous Sensing in Big Sensed Data," *In Proc. of the IEEE Global Communications Conf.*, Washington, DC, USA, 2016, pp. 1-6.

[31] B. Baranidharan, B. Santhi, “An Evolutionary Approach to Improve the Life Time of the Wireless Sensor Networks”, *Theoretical and Applied Information Technology*, vol. 33, no. 2, pp.177-183, 2011.

[32] F. Al-Turjman, “Hybrid Approach for Mobile Couriers Election in Smart-cities”, *In Proc. of the IEEE Local Computer Networks*, Dubai, UAE, pp. 507-510, 2016.

[33] A. Al-Hourani, S. Kandeepan, “Cognitive Relay Nodes for Airborne LTE Emergency Networks”, *In Proc. of the IEEE Int. Conf. on Signal Processing and Communication Systems*, Gold Coast, Australia, 2013, pp. 1-9.

[34] J. M. Jornet and I. F. Akyildiz, “Channel modeling and capacity analysis for electromagnetic wireless nanonetworks in the terahertz band”, *IEEE Trans. Wireless Commun*., vol. 10, no. 10, pp. 3211–3221, 2011.

[35] N. Kumar, R. Iqbal, N. Chilamkurti, "Capacity and Load-aware Service Discovery with Service Selection in Peer-to-Peer Grids", *Elsevier Future Generation Computer Systems*, vol. 28, no. 7, pp. 1090-1099, 2012.

[36] G. Singh, and F. Al-Turjman, “Learning Data Delivery Paths in QoI-Aware Information-Centric Sensor Networks”, *IEEE Internet of Things*, vol. 3, no. 4, pp. 572 – 580, 2016.

[37] D. Rosário, Z. Zhao, A. Santos, T. Braun, E. Cerqueira, “A beaconless Opportunistic Routing based on a cross-layer approach for efficient video dissemination in mobile multimedia IoT applications”, *Elsevier Computer Communications,* vol. 45, no. 1, pp. 21-31, 2014.

[38] P. Spachos, and D. Hantzinakos, “Scalable Dynamic Routing Protocol for Cognitive Radio Sensor Networks”, *IEEE Sensors*, vol. 28, no. 15, pp. 4038–4052, 2016.

[39] A. Bourdena, C. Mavromoustakis, G. Kormentzas, E. Pallis, G. Mastorakis, M. Yassein, “A resource intensive traffic-aware scheme using energy-aware routing in cognitive radio networks”, *Elsevier Future Generation Computer Systems*, vol. 39, no. 1, pp. 16-28, 2014.

[40] S. Oteafy and H. Hassanein, "Resilient IoT Architectures over Dynamic Sensor Networks with Adaptive Components," *IEEE Internet of Things*, vol. PP, no. 99, pp.1-1, 2016.

[41] Z. Xu, H. Zhang, C. Hu, L. Mei, J. Xuan, K-K. R. Choo, V. Sugumaran, Y. Zhu, “Building Knowledge Base of Urban Emergency Events based on Crowdsourcing of Social Media”, *Wiley Concurrency and Computation: Practice and Experience,* vol. 28, no. 15, pp. 4038 – 4052, 2016.

[42] Z. Xu, X. Wei, Y. Liu, L. Mei, C. Hu, K-K. R. Choo, Y. Zhu, V. Sugumaran, “Building the search pattern of web users using conceptual semantic space model”, *International Journal of Web and Grid Services,* vol. 12, no. 3, pp. 328–347, 2016.

[43] Z. Xu, X. Luo, Y. Liu, K-K. R. Choo, V. Sugumaran, N. Yen, L. Mei, and C. Hu, “From Latency, through Outbreak, to Decline: Detecting Different States of Emergency Events Using Web Resources”, *IEEE Transactions on Big Data*, vol. PP, no. 99, 2016.

[44] Z. Xu, J. Xuan, Y. Liu, K-K. R. Choo, L. Mei, and C. Hu, “Building Spatial Temporal Relation Graph of Concepts Pair using Web Repository”, *Springer Information Systems Frontiers*, 2016. [In press].

Bio:

Dr. Fadi Al-Turjman is a visiting faculty member at METU University in Cyprus, and adjunct at Queen's University in Kingston, Ontario, Canada. He is working in the area of wireless networks' architectures, deployments, and performance evaluation. Dr. Al-Turjman obtained his Ph.D. in Computer Science from Queen's University in 2011. He received both his B.Eng. (Honors) and M.Eng. (Honors) degrees in Computer Engineering from Kuwait University in 2004 and 2007, respectively. From 2004 to 2007, he was a researcher & lecturer at the departments of Information Science and Computer Engineering at Kuwait University, Kuwait. During this period, he worked on digital systems and wireless sensor networks. From 2007 to 2013, he was a research & teaching associate at Queen's University, Canada. From 2013 to 2015, he worked as an assistant professor at the University of Guelph, Canada and Akdeniz University, Turkey. He has received recognition and best paper awards at top international venues, including IEEE ICC, LCN, GLOBECOM, and IWCMC conferences. He has authored/co-authored more than 70 reputable journals and international conference papers, in addition to 2 patents in his research area. He organized and chaired a number of international symposia and conferences; including the FTRA IET in MUSIC 2012, the IEEE G-IoT in GLOBECOM 2012, the IWCMC'14'16, and the IEEE LCN'12, '13, '14, '15 and '16.

Highlights

In this paper, we propose a framework for data delivery in large-scale networks for disaster management, where numerous wireless sensors are distributed on a city traffic-infrastructures, shopping malls parking areas, airports' facilities, etc. In general, our framework caters for green energy-efficient applications in smart cities where data is relayed via relays from a diverse sensor-nodes towards a gateway connected to a large-scale network such as the Internet. We consider the entire network energy while choosing the next hop for our routed packets in the targeted wireless sensor network in addition to other performance metrics such as system throughput and data delivery cost. Our delivery approach considers resource limitations in terms of hop count, and remaining energy levels. Extensive simulations are performed and the results confirm the effectiveness of the proposed approach in comparison to other baseline energy-aware routing protocols in the literature.