International Journal of Multimedia and Ubiquitous Engineering
Vol.10, No.12 (2015), pp.37-52
http://dx.doi.org/10.14257/ijmue.2015.10.12.05

Layering the Internet-of-Things with Multicasting in Flow-Sensors for Internet-of-Services

Rahim Rahmani and Theo Kanter

Department of Computer and Systems Sciences
Stockholm University, Sweden
{rahim, kanter}@dsv.su.se

Abstract

Development of Internet-of-Services will be hampered by heterogeneous Internet-of-Things infrastructures, such as inconsistency in communicating with participating objects, connectivity between them, topology definition & data transfer, access via cloud computing for data storage etc. Our proposed solutions are applicable to a random topology scenario that allow establishing of multi-operational sensor networks out of single networks and/or single service networks with the participation of multiple networks; thus allowing virtual links to be created and resources to be shared. The designed layers are context-aware, application-oriented, and capable of representing physical objects to a management system, along with discovery of services. The reliability issue is addressed by deploying IETF supported IEEE 802.15.4 network model for low-rate wireless personal networks. Flow-sensor succeeded better results in comparison to the typical - sensor from reachability, throughput, energy consumption and diversity gain viewpoint and through allowing the multicast groups into maximum number, performances can be improved.

Keywords: *Flow-sensor, Internet of Services (IOS), Internet of Things (IOT)*

1. Introduction

The Internet of Things (IoT) can be defined as a global network infrastructure based on standard and interoperable communication protocols where physical and virtual “things” are seamlessly integrated into the information network. By definition, ‘Things’ indicate to any physical entity which is able to communicate with each other and take part to develop the concept of Internet of Service (IoS) out of internet connectivity [1];The definition immensely widens the service scope that is obtainable via the Internet. The establishment of IoT infrastructure leads to pervasive computing and ambient intelligence developments through communication and resource sharing among billions of physical objects within dynamic and configurable networks [2]. A joint collaboration of internet of service and OpenFlow is capable of grasping the dream to obtain software applications, business model, and present architecture as a service and directing the vision towards the maximum utilization of cloud computing.

The ultimate goal of IoT can be to be adapted and utilized in industrial sectors. Industrial wireless sensor network (IWSN) does not require so many modifications in present wireless sensor networks (WSN) but to emphasize on maximum reliability and real time delivery of context-aware applications. So, these applications are required to be reliable and reliability is required to be provided in lower layers. Reliability is our main concern and that’s why reliability affecting factors (such as reachability, energy consumption, throughput, hops requirement) have been analyzed in this paper. OpenFlow is the technology that can turn the mac and network layer to be more reliable [3].

ISSN: 1975-0080 IJMUE

OpenFlow is one of hot topics now a day but not so many researchers have attempted to apply this protocol to wireless sensor networks within the scope of IoT applied to IoS. We proposed a method for applying OpenFlow in sensor networks in our previously published papers along with a definition and architecture of flow-sensor which claims to enhance reliability comparable to typical sensors [4]. As a prolongation of our previous works, several crucial questions have been pointed out in Internet of Things arena and can be resolved through our proposed notions specified below.

1) At present due to absence of a common, standardized, layered IOT framework supported by context information, Internet of services are limited [5]. We have proposed a 5 layer IoT framework which can outline numerous kinds of physical objects (like RFID tags, NFC, flow-sensor *etc.*) and their employment, synchronization within the current internet framework along with diverse services and systems (for example cloud computing, business support system *etc.*)

2) Currently a variety of tasks are assigned to various networks to collect services from there. Nevertheless multicasting services over a broadcasting physical medium can distribute the tasks to a group of sensors within the same network.

3) Presently transport layer is only responsible to provide reliability which designates the internet layer to be unreliable and let alone the below layers. But OpenFlow supported sensors are found to be the best candidate since it is delimited to low overhead and multicast assistance as supported by CoAP application. Besides it can turn the MAC layer to be more reliable in comparison to typical sensors and the network layer accordingly.

4) Nowadays network isolation is problematic, exorbitant but imperative for virtual networking. Same applications necessitated to be performed by the groups of sensor those might be located in distant physical locations.

5) Right now communications between sensors inside any specific network is straightforward but challenging from group of networks viewpoint. Virtual links entitled to be inaugurated among several sensor networks from different services point of view.

6) At the moment any sensor network is mostly reliant on the access point for route initiation, traffic control, reachability, hops, energy requirements *etc.* But according to the sensor network definition, the network should be dynamically self-structured and self-constructed and the nodes, themselves, within the network should have the ability to establish and maintain mesh connectivity automatically. On the other hand any sort of inactivity of the access point can create lots of problems for the sensor networks from a reliability point of view.

Conceivable utilization comprises real time environment alertness, behavior monitoring of any living and/or moving objects, control feedback system, improve resource utilization, industrial control automation mechanism and also in some additional regions where usual and normal attempts were confirmed to be very expensive and unreliable [6].

This paper is systematized in the following approach: Section II defines the background and motivation; Section III presents previous work in the area as related work; Section IV portrays layer designing of Internet of Things; Section V describes the conceptual model; Section VI presents the performance evaluation; Section VII provide Challenges and Open Issues in Security and Privacy and the conclusions are provided in Section VIII.

2. Background and Motivation

The Internet-of-Things involves communications and collaborations between living and dead objects from remote observations viewpoint. Solely IP connectivity can’t permit the sensor to get incorporated into the internet infrastructure due to its inadequate resources, *i.e.* memory, bandwidth, power and communication competences. Dynamic connectivity with the internet reasoned to enhance the possibility over seamless integration between sensors and internet of things [7]. Task assessment sanctions assistances through heterogeneous network and remote access can be possible to attain a definite set of forthcoming challenges through exploitation of OpenFlow technology.

OpenFlow splits up the data traffic into data packet (underlying router and/or switch supported) and control packet (controller based) which set the physical devices into simple forms meanwhile complicated intelligence applications become eradicated. Nowadays OpenFlow is adopted by numerous switch/router vendors and capable to support layer 2, 3, and 4 headers. It is also proficient to put together the circuit and packet switching technology though treated separately [8], [9]. Utilization of OpenFlow in sensor networks can play an important role to enhance reliability in lower layers.

OpenFlow maintained sensors are called as flow-sensors which carry out the architecture of typical sensor accompanied by a control interface and one or more flow tables [4]. The flow table holds a header containing source and destination addresses, decision rule for either dropping or forwarding the packets and a counter to maintain a data statistic [10]. The architecture of flow-sensor allows providing multicast services and applications on current routing algorithm leaving the preset IoT infrastructure unchanged.

Internets of things are all about interconnection of different physical objects and communication between several standards. As addressed by IoT forum [5], Due to lack of definite IoT segmentation and specified standard, development in large scale wasn’t fully operational; several application providers, system vendors, device manufacturers have failed to cope-up and collaborate with each other and overall IoS reception and achievement has been obstacles.

Currently the IoT industries are facing the deficiency of unified framework and can’t be functional properly. Thus resulting the IoS received out of IoT infrastructure to be unrelated and independent. Generated services are non-shared and directed to specific users. To be noted these future applications are required to be co-related and merged up to solve socio- economic issues like environment, climate and disaster management, safety measurement, modernization of agriculture and transportation *etc.* [11].

In near future IoT industry will grow up rapidly and will begin full scale production. So, internet of services also needs to be adapted with the dynamic changes occurred or happened all around [12]. The goal of IoT is all-about collaboration and sharing context information among billions of networked physical objects which helps to grasp the dream of ambient networking. A standardized IoT layering framework is required to obtain context services, to replace the devices and provision for new technologies should also be included with a view to achieve ubiquitous computing. As for example, this layer division allows any service support system to be introduced and lead to IoT industry modernization leaving the current architecture unchanged. And most importantly maximum reliability in lower layers can be achieved based on the proposed IoT layered framework that will play an important role in IWSN.

3. Related Work

Multicasting applications are not straightforward for the sensor networks to run over the broadcasting physical medium from a reliability point of view. Several researchers have tried to optimize and implement it but most of the algorithms are too complex to apply in practice on sensor due to low resources as stated earlier. Several reliability factors in several layers like reachability, energy utilization, error checking, throughput, scalability, hops, buffer *etc.* are required to be equally maintained though robust routing was found to be only issue and emphasized by most of the authors. For example authors have proposed several optimized routing algorithms while considering only reliable message delivery and nondeterministic nature of the sensor environment in [13] and [14] where energy consumption, error and latency model were also suggested in [15]. Their provided algorithms included all the lower layers to define their proposed network model.

Design challenges are focused in a multi-hop consequence in [16] and impact of route pruning, bandwidth, and path selection are addressed in [17]. However conclusion was attained without reachability and throughput in mind.

The work presented in [24] studies the state-of-the-art of IoT and presents the key technological drivers, potential applications, challenges and future research areas in the domain of IoT. However the work does not study the impact of sensors-flow in multicasting applications to attained reachability and reliability in mind.

4. Layers for the Internet of Things

IoT and IWSN can be collaborated and can bring revolution towards ubiquitous computing. The responsibilities of IoT are also to measure smart interconnection and intelligent behavior of the autonomous entities. Those duties can be fulfilled through the effectual alliance with context data where a shared intelligence can be formed among devices, technologies and user; a networking and heterogeneous communication to process; analyze and transfer contextual information; we are not concerned about the nodes those are physically integrated into devices rather than randomly placed over an area. It is basically a conceptual framework in order to standardize IoT framework to receive IoS. And the model is logically divided in order to separate placement, sensing, coordinate and applications. Lots of sensors coordinate within themselves in order to generate context data without involvement of any central coordinating system or access points. Groups of sensors send their individual data to nearby sink node. Sink node to IoT gateway, IoT gateway to clouds where context server is placed.

We propose to divide the communication support between the Internet-of-Things (IoT) and the Internet-of-Services (IoS) into five layers as shown in Figure 1. The five layers constitute a generic architecture for interfacing between services and Internet-of-Things infrastructures which leaves the current internet infrastructure unchanged. No supplementary layer is required from placement, event detection, processing and application (service) viewpoint when sensors are integrated into physical devices. But in our scenario we want to separate lower level placement and event detection information from data processing, storing and higher level context application details in order to turn the networks into more extensive and re-usable. These layering concepts will also reduce the confusion about participating objects, connectivity among them, topology definition & data transfer, cloud computing for data storage and business support system and above all service requested by the end user and offered by acting entities. To be noted each layer is individual, can be divided into several sub layers based on the technology and services involvement and required to be treated separately based on the tasks assigned. In this paper reliability affecting factors of a specific level of networking and communication layer has been measured and that’s why that particular layer was emphasized in comparison to other layers.

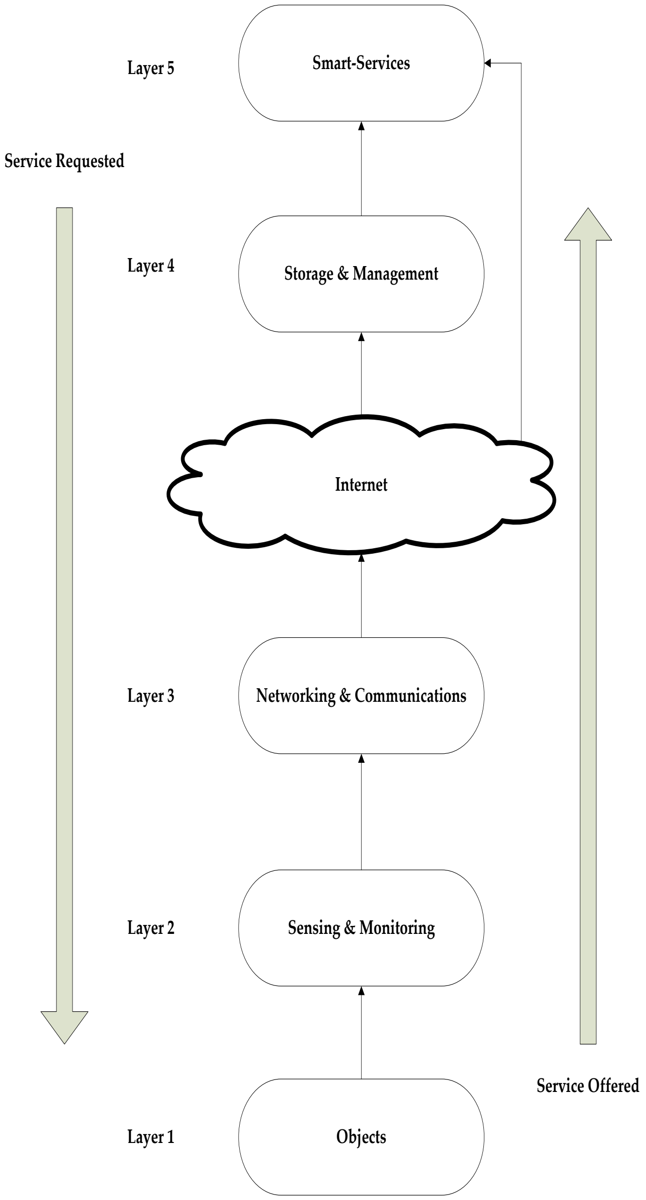

Figure 1. 5 Layer Service Oriented IOT Design Model

A. Layer 1: Object

Layer 1 includes the placement of small range communication devices such as RFID tags, NFC, sensors, actuators *etc*. Next generation internet is highly dependable on the incorporation of regular objects founded in our surroundings those can be uniquely recognizable and controllable into Internet of things.

B. Layer 2: Sensing and Monitoring

Monitoring of the entities is performed by RFID tags, NFC and sensing by flow-sensor. Their effective joint collaboration is designed in layer 2. RFID tags, those are attached to physical entities cannot transfer data via any multi-hopping. That’s why a large number of RFID tags create a network with a small number of flow-sensors to transfer data. The important advantages in RFID tagging are the placement and energy consumption. Because these are too small to get fitted anywhere and receive energy through reading the objects.

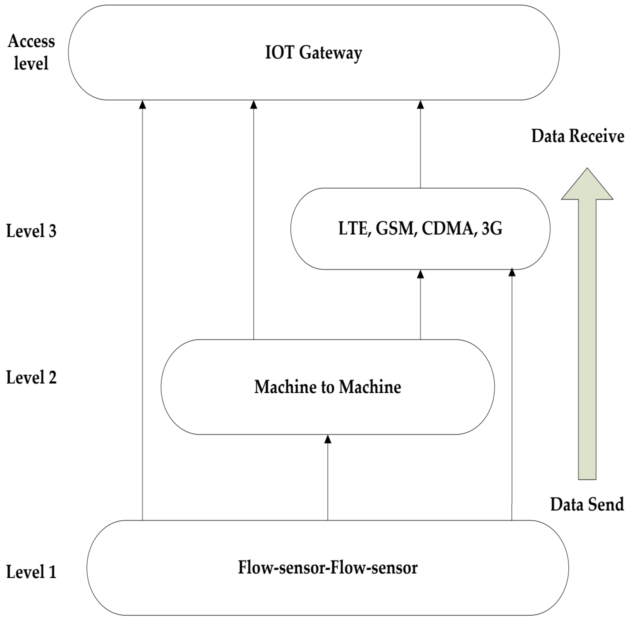

Figure 2. Physical Object to IOT Gateway; 3 Level Communications

C. Layer 3: Networking and Communications

Layer 3 can be diagramed into 3 levels as shown in Figure 2 based on the application required and devices & technology involvement. Data will be reached to internet via IoT gateway covering the mapped levels. Level 1 and Access levels are important whereas involvement of level 2 and level 3 are application specific. Level 1 will be simulated in section IV and performance result will be analyzed accordingly. Example application alternatives are depicted below.

ALT 1: Level 1 → IoT Gateway: Example application can be home automation. All kinds of home appliances like refrigerator, washing machine, microwave *etc.* can be monitored (temperature, sound, motion *etc.*) through RFID tagging. RFID tags can send data to actuator to control the event or to flow-sensor in order to publish the result in internet. The flow-sensor can forward the data via multi-hopping and can use the SOHO router proxy as an IoT gateway.

ALT 2: Level 1 → Level 2 → IoT Gateway: Example application can be automotive management system; real time data, site facts, anti-theft security, roadside assistances *etc.*

ALT 3: Level 1 → Level 3 → IoT Gateway: Example application can be ‘ user current status update’ in social networking sites. One of the important challenges of future internet and internet of things can be data streaming of real time applications. This problem can be solved with joint networking of RFID tags (only for sensing); flow-sensors (data forwarding) and cell phone (access point) and results can be published on social networking sites like twitter, Facebook *etc.*

ALT 4: Level 1 → Level 2 → Level 3 → IoT Gateway: Example application can be tracing and tracking. A close interactive service is required between device and device manufacturer to make those devices perfectly operational where nearby base station will work as an IoT gateway.

Real time data is one of the most important features in IoS to be received from IoT framework and also required to be maintained for IWSN. These data are the context data, changeable over time and required to be stored in clouds to receive results at any time regardless user and event position.

D. Layer 4: Storage and Management

Storage and management layer involves data storage & system supervision, software services and business management & operations. Though they are included in one layer, the business support system resides slightly above of cloud computing service whereas OpenFlow is placed below of it to include virtualizations and monitor management.

Any business models can find benefits from cloud computing infrastructure. As for example cost and flexibility solution for small business whereas total IT problems for large companies. It adds advantages for companies, their employees, consumers, and distributor. So, it can be said in a sentence that the overall business solution can be provided.

OpenFlow is capable to affix virtual layers with the fixed layers leaving the running infrastructure unaffected. We have illustrated virtualization of Internet of Things through OpenFlow in one of our previous papers which can assist to succeed improved reachability, bandwidth, robust routing, *etc.* and can guide to a better reliability thereby [4].

E. Layer 5: Smart Services

As stated earlier any kind of services can be mapped through this simplified IoT model. Besides the model is relaxed to invite any technology to be involved since heterogeneity management is also supported. Another important advantage is to leave the established infrastructure of the internet and cloud computing technology untouched and running as well. Possible services comprise e-health, vehicle monitoring, battle ground assessment, home automation security mechanism, disaster management *etc.* [18].

5. Conceptual Modeling

A. Model: Reachability

Node reachability can be defined as the possibility to reach a destination or adjacent node which lies within the transmission range of source node and/or a forwarding node in a multihopping scenario. K denotes the set of reached nodes where and node reachability of a given node x, λx(k). So, the network reachability can be expressed as λ(K) and for maximum reachability, λ(K) →100%.

B. Model: Reliability

Reliability or reliable message delivery is one of highest concern for industrial wireless sensor networks. Lots of factors can affect the reliability factor actively and passively. But in our model reachability, link condition, physical resources, error probability, energy consumption, transmission power, buffer length and number of hops have been considered for network and communication layer.

To maximize reliability of a node x, $\sum_{x} R(x)$ needs to be ensured where Source node,

$$x = \{1,2,3,...., x\} \mathit{where} \ , x \geq 1 \text{ and } M \times S_x \leq C(W_x, E_p) \mathit{where} \ , C = (C_l, l \in L(x)) \quad (1)$$

$$S_x \in C(E_p), S_x \in C(F), S_x \in \prod(W)$$

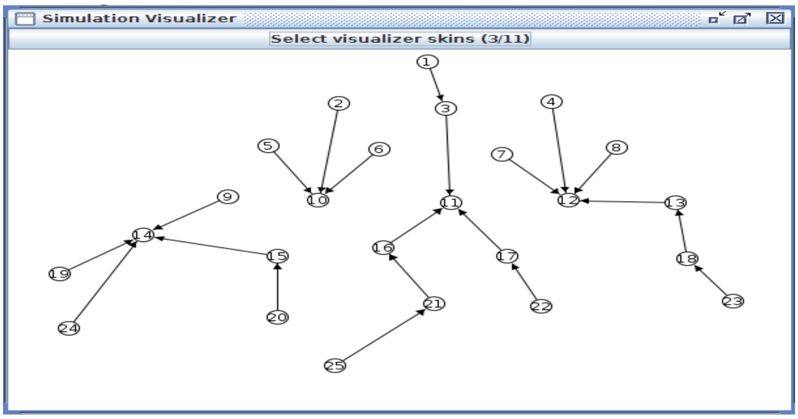

Figure 3. The Network Gets Divided Into Four Multicast Groups (4 MG)

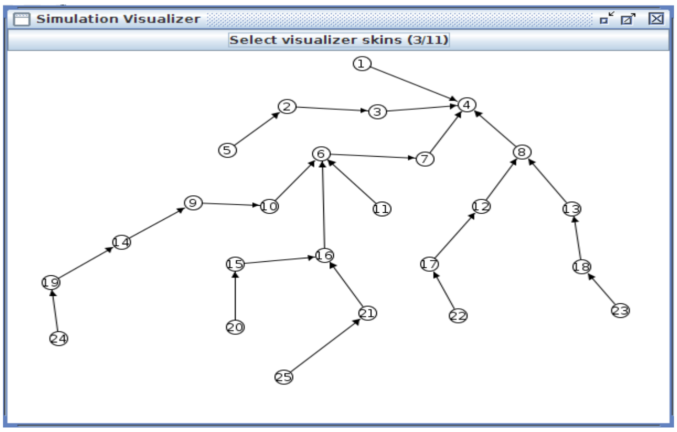

Figure 4. All Four Multicast Groups are Merged Into 1 Group and Directing their Traffic Towards an Example Sink Node 4

Here, M represents routing matrix, C stands for the finite capacity of a buffer-less channel, L for a set of links, F for contention matrix and Π for scheduling matrix. For the node x, Sx= source rate at the physical layer, Wx= physical layer resources, Ep= probability of error, l= link capacity.

Number of packets in   and d(N) stands for the aggregation of packets in a flow.

$$P_{ch}(x) = \begin{Bmatrix} True & , ifC \geq \sum_{N} d(N) \\ False & , otherwise \end{Bmatrix} \quad (2)$$

Signal to noise ratio (SNR) at *x* can be defined as [23], $\Gamma_x = \dfrac{\sum_{y \in U_x} P_{x,y}}{\sum_{y \in U_x} P_{x,y} + N_{ext}}$

(3)

Where $P_{x,y}$ represent power received by *x* generated from *y*, N_{ext} stands for external noise and U_x for group of transmitters projected to node *x*. The SNR should be kept below the threshold level to maintain reliability.

$$P_{sig}(x) = \left\{ \begin{array}{l} True \quad , if\, \Gamma_x \le \Gamma_x^{thres} \\ False \quad , otherwise \end{array} \right\} \tag{4}$$

For a given node *x*, link *l* and time *t*, $x_s(t) \ge 0, \forall x$; $\lambda_l(t) \le 0, \forall l$ and rate of receiving forwarding packet from

Node $y = \lambda_{x,y}$; current buffer state should be less than the total buffer size otherwise congestion can occur.

$$P_{con}(x) = \left\{ \begin{array}{l} Trueif \quad \left\{ \begin{array}{l} \lambda_{fw}^{x} \le \lambda_{fw}^{thres} \\ \beta_{x}^{cur} \le \beta_{x}^{total} \end{array} \right\} \\ False \quad , otherwise \end{array} \right\} \tag{5}$$

The transmission energy of node *x* can be modeled as [19].

$$E_x = \left\{ E_y + \frac{P_x\left(E_x - E_y\right)}{P_{ref}} \right\}. \tag{6}$$

It is important to read the current energy state and required to be more than the threshold level during the transmission.

C. Example Scenario

The simulation runs on Tmote Sky sensor nodes containing contikiOS, 3.9 MHz, 16 bit CPU and 10KB RAM for 6LoWPAN for both the typical and flow-sensor. ContikiMAC consumes very low power to listen MAC protocol which is utilized to an effective wake-up procedure with 8 Hz frequency. UDGM & constant loss has been exploited as a radio model over RIME communication stack to simulate the scenario in Cooja simulator [23]. The problem is addressed by deploying IETF supported IEEE 802.15.4 network model in the physical layer that is capable to operate in low data rate. Ripple Routing Protocol (RPL) has been utilized since it can support sensor deployment in large scale, require small energy, support multicast traffic *etc.* Different layers (fig 1) will lead to different state and required to be treated separately. The simulation addressed level 1 of layer 3 (Figure 2) as stated earlier based on the research objectives. To be noted in a context aware system the performance results of sensor groups are counted rather than single node performance and that's why sensors are divided into several multicast group with an aim to achieve multitasking networks.

A simple example network with 25 nodes has been formed to simulate the following research set-up. Receiving nodes get connected to the transmitting node and/or sink node based on signal strength. Signal strength is measured based on the SNR value of the receiving nodes.) Several flow-sensor multicast groups are created where each group contains 1 sink node. And other nodes within a multicast group will direct its traffic toward the sink node. The number of multicast groups can be easily upsurge and declined based on the service desired; thus signifies flow-sensors entitled in a multicast group can work for others which leads to resource sharing among the nodes. Traffic flows can be conveniently controlled just by selecting new sink nodes whenever required.

Sink nodes 10, 14, 11 and 12 have created 4 multicast groups (4 MG). Nodes of one multicast group are only allowed to communicate within its group node but not to other nodes of another multicast group. Nodes 10, 14, 11 and 12 contain 4, 6, 8 and 7 nodes respectively within their groups. Any random node selects its sink node based on the signal strength received. Node 3 has chosen 11 as its sink though it could have selected the sink node 10 via node 6 and sink node 12 via node 7. Because node 3 falls within the coverage area of node11 and can reach directly within 1 hop. See Figure 3.

A big group is created out of many small multicast groups as exhibited in Figure 4 to accomplish a common task allocated to the networks which leads to virtual networking. Some nodes are placed in a distant location and not a part of that particular network. Though these nodes can join the network without changing their physical locations and it allows the nodes to share their resources among them. All the four multicast groups have been merged into one big network and directed their traffic towards an example sink 4. This setting allows a network to be virtualized and prioritized any traffic required.

6. Performance Evaluation

Result analysis was performed following the ideal parameter values by default provided in Table 1 else otherwise noted.

A. Result Comparison: Flow-sensor vs. typical sensor

Result analysis was performed following the ideal parameter provided in Table 1 else otherwise noted. The Comparisons were performed between flow-sensor and typical sensors based on the factors namely node density, reachability, transmission (Tx) power and energy consumption.

At low density (0.005 to 0.007 nodes/meter2), the difference was found too less and jump cumulating with the escalation of sensor density. It is also expected that both of them will achieve near 100% reachability in a highly dense network. To touch a reachability of 80%, the flow-sensor required 117 nodes, while the typical sensor required 142 nodes. In ideal case flow-sensor and typical sensor bear the reachability of 61.28% and 44.07% respectively. See Figure 5.

In Figure 6, both of them achieved almost equal reachability (low and high reachability at low and high transmission power respectively). The flow-sensor initiated the better result with the upswing of Tx power until becoming almost constant at 99% reachability on -4.6 dBm. Flow-sensor attained 80% reachability at -8.3 dBm but the typical sensor needed -5.75 dBm.

Table 1. Simulation Parameter

PARAMETER	VALUE OR NAME
Communication stacks	RIME
Radio model	UDGM & constant loss
Node placement	Random 2D position
Topology size	100*100
Number of nodes*	100
Sensor density*	0.01 nodes/meter^2
Data rate	250 Kbit/s
Channel check rate	8 Hz
Simulation delay	0 Sec
Maximum retransmission	15 times
Tx range*	10 meters
Interference range*	10 meters
Path gain	-0.04 dBm
Propagation constant	4
Packet size	125 Byte
Required SNR	4 dB
Tx power*	-10.45 dBm
Receiver sensitivity	-80.5 dBm
Energy consumption	25 nJ/bit
Simulation runs	70+ times

*) will be varied during simulations.

At low density (0.005 nodes/m2) both of them carried out the equal amount of throughput as seen in Figure 7. But flow sensor commenced better results with the growth of sensor density. As for example, to achieve 100 Kbps throughput, flow-sensor demanded 106 nodes however the typical sensor wanted 128 nodes per 100*100 networks. At ideal state, flow sensor and typical sensor succeeded throughput of 83.22 and 52.15 Kbps respectively.

While the number of nodes gets accelerated, the number of packets sent, received and collided also gets increased. But the typical sensor observes the higher amount of packet collision. So, packets are required to be retransmitted for more times and a lower number of packets get received as a result. So, the ratio of received and sent packets becomes lesser in comparison to flow-sensor in high density area. As a result the number of successfully delivered packets gets worse thus lowering the throughput of the typical sensor.

As found earlier, packet sent, received and collision was observed more in a greater amount of nodes. But typical sensor witnessed excessive amount of packet collision which intensifies the total amount of packets in resemblance to flow-sensor. The flow-sensor accomplished better results in high density and the difference endures to upturn with the ascent of the node density. To be noted reachability also influences the energy consumption in wireless multi-hop sensor networks since sensor nodes are required to send/receive packets to/from reachable nodes and increases the energy consumption thereby. In Figure 8, the flow-sensor and typical sensor consumed 0.0131 J and 0.0194 J respectively. To achieve a reachability of 80%, flow-sensor and typical sensor expended 0.017 J and 0.04 J respectively in ideal circumstances.

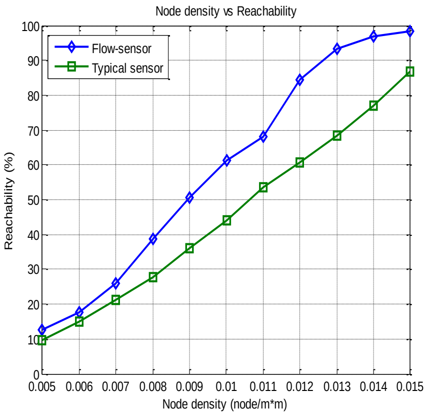

Figure 5. Reachability was Compared Based on Varying Node Density

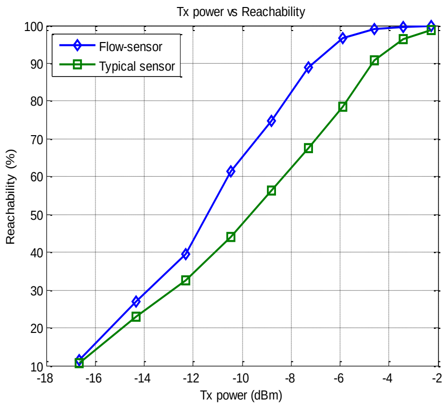

Figure 6. Evaluation of Reachability with Changing Transmission Power

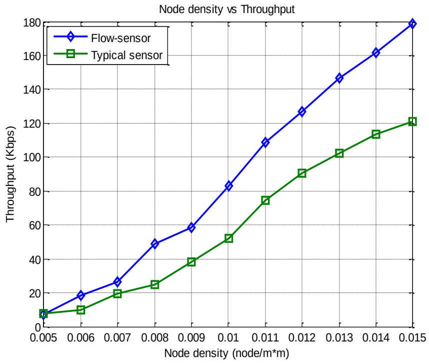

Figure 8. Throughput Comparison on Varying Node Density

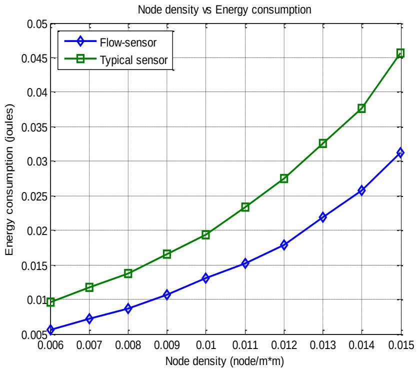

Figure 8. Energy Consumption of Both Type of Sensors were Assessed Based on Changeable Node Density

B. Result comparison: Different multicast groups

The network topology was distributed into 1, 2, 3 and 4 multicast groups denoted as 1, 2, 3 and 4 MG respectively. The comparison was carried out based on node density, reachability, throughput and maximum number of hops.

All of the multicast groups carried almost equal reachability in low density but the difference has been originated with the upsurge in the node density. 4 MG touched 80 % reachability with 122 nodes while 3 MG, 2 MG and 1MG needed 134, 145 and 149 nodes respectively. In an ideal setting 4 MG, 3MG, 2MG and 1MG achieved 57.01%, 47.94%, 40.56 and 34.95% reachability respectively. All the multicast groups are expected to succeed almost 100% of reachability in a very high density network. See Figure 9.

As found in Figure 10, all of them had a trivial throughput at low density but initiated mounting up with high density as expected. Small numbers of nodes generate fewer packets and most of packets get dropped due to lower reachability. And it's almost equal for all groups. As a result network efficiency remains lower for all multicast groups at low density. On the other hand packet drop hardly occurs due to high reachability. But packet collision increases with higher number of nodes. 4 MG had a lower packet collision in comparison to other multicast groups that escalated its success rate in highly dense network and so thus the throughput. At node density 0.01 nodes/m2, 4 MG, 3 MG, 2 MG and 1MG accomplished the throughput of 65.32, 60.4, 54.02 and 48.55 Kbps respectively.

Hops requirements also depend on reachability. At the beginning (lower density), multicast groups contain lower reachability, so the number of hops will also be lower. A higher amount of hops can be achieved when the reachability gets higher which means in higher node density. In an ideal case, 4 MG generated 13.51 hops whereas 3 MG, 2 MG and 1 MG generated 15.09, 17.5 and 21.08 hops respectively as noticed in Figure 11. But the comparison is entailed on equal reachability to know the real hops requirements. 4 MG, 3MG, 2MG and 1MG produced 16.5, 22, 32 and 41 hops respectively to achieve a reachability of 80%.

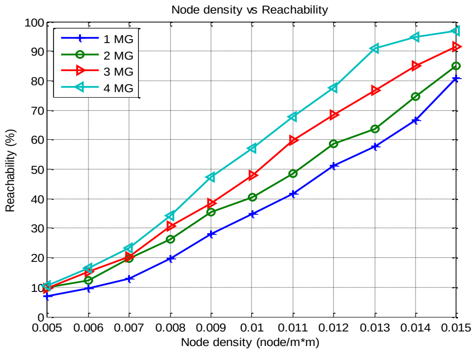

Figure 9. Comparison of Reachability where Node Density was Assumed as Variable

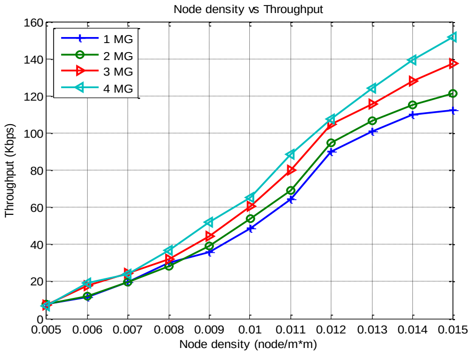

Figure 10. Comparison of throughput Based on Varying Node Density

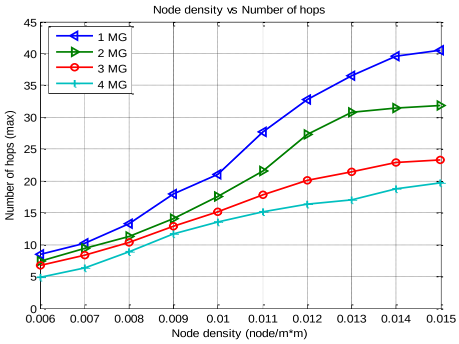

Figure 11. Number of Hops was Compared Based on Varying Node Density

7. Security and Privacy as Open Issues

Based on the workflows in the layering concepts which shown in Figure 1 and according to the security requirements in WSN, this section summarizes security scheme and countermeasure in each layer. By identified the possibility of the threat in WSN which provide the requirements for evaluation of a security scheme and its appropriation for each layer. The attack in WSN can be classified [25] as: Outsider, insider, passive, active, mot-class and laptop-class attacks.

The security scheme has to meet the requirements such as Resiliency, Energy efficiency, Flexibility, Scalability, Fault-tolerance, Self-healing and Assurance.

In light of the above observation and according the security requirement in WSN are explored in the following subsections.

A. Security scheme in layer 1 (Object):

This layer is responsible for placement of small range communication devices as object and an outside attacks obtain a node as a member of commodity sensor nodes (objects) and induce the network to accept them as legitimate nodes, security scheme should be able to protect against the attacks by controlling the unique publish subscription id as key exchange between objects and sink in the multicasting groups.

B. Security scheme in layer 2 (Sensing and Monitoring):

This layer is responsible for monitoring of entities to be performed and sensing by flow-sensor. An eavesdropping attacks obtain an adversary can gain access to private information by monitoring transmissions between nodes. Security scheme should be able to provide encrypting sensor node communications solves eavesdropping problem.

C. Security scheme in layer 3 (Networking and Communication):

This layer is responsible for communication from flow-sensor to IOT Gateway. The attacks in this layer can be spoofed, selective forwarding and sinkhole, wormholes, acknowledgment spoofing and flooding.

Security scheme should be able to ensure secure operation even in the presence of a small number of malicious network nodes. Node-to-node authentication is one basic building block for enabling network nodes to prove their identity to each other. Node revocation can then exclude malicious nodes. To achieve resilient a security scheme should be still protect against the attacks even in case of few nodes are compromised. Security scheme should be able to scale without compromising the security requirements.

D. Security scheme in layer 4 (Storage and Management):

This layer is responsible for data storage and system management. The attacks in this layer can be 1) on secrecy and authentication 2) on network availability 3) stealthy attacks against service integrity.

Security scheme should be able to provide cryptographic in this layer which can protect the secrecy and authenticity of communication path. Even security scheme should be able to key management which should be flexible so as to allow for different network deployment methods such as random node scattering and predetermined node placement.

E. Security scheme in layer 5:

Since flow-sensor network are tools for collecting information and an adversary can gain access to sensitive information either by accessing stored sensor data or by querying or eavesdropping on the network. Sensor networks aggravate the privacy problem because they make large volumes of information easily available through remote access. Security & privacy scheme should be able to ensuring that sensed information strays within the sensor network and is accessible only to trusted parties is an essential step toward achieving privacy.

8. Conclusion

In this paper we addressed how to mitigate heterogeneous Internet-of-Things infrastructures, such as inconsistency in communicating with participating objects, connectivity between them, topology definition & data transfer, access via cloud computing for data storage. Since CoAP and RESTful services in combination with IPv6 are insufficient, we propose a layered framework of the IoT along with OpenFlow in order to mitigate heterogeneous communication. With an aim to accomplish extensive services, interconnection of devices and sharing of context information among different system standards, the proposed layered framework can turn the total system to be less complicated and more interoperable. Our solution is applicable in random topology circumstances where nodes are to be placed in multiple networks. It is possible to create multiple multicast groups under a single network and/or a big network out of nodes of different networks for the sake of achieving resource sharing within sensor networks. That means it allows establishing of multi operational sensor networks out of single network and/or single service network out of participation of multiple networks based on the services required.

Promising results show that flow sensor succeeded better results in comparison to typical-sensor by 17.21% points more reachability (Figure 5), 31.07 Kbps more throughput (Figure 7) and 0.0063 J less energy (Figure 8) in an ideal consequence. On the other hand, for achieving 80% reachability, flow sensor required less density by 0.0025 nodes/m2 (Figure 5) and less energy by 0.023 J (Figure 8). Flow-sensor also achieved a diversity gain of 2.55 dB (Figure 6). At equal throughput (100 Kbps), flow-sensor desired less node density by 0.0022 nodes/m2 (Figure 7).

Following the ideal parameter, 4 MG confirmed much better performance than 3MG, 2MG and 1MG; As for example, more reachability by 9.07%, 16.45%, 22.06% points (Figure 9), more throughput by 4.92, 11.3, 16.77 Kbps(Figure 10) and less hops required by 1.58, 3.99, 7.57 (Figure 11) respectively. Also less node density by 0.0012, 0.0023, 0.0027 nodes/m2 (Figure 9) and less hops required by 5.5, 15.5, 24.5 respectively at 80% reachability (Figure 11). Besides 4 MG necessitated less density by 0.0004, 0.0009, 0.0015 nodes/m2 at 100 Kbps throughput (Figure 10).

Our projected layer designing are completely application aware and service oriented that obtains smart services out of the Internet of Things model. Three layers are sited below the internet medium like object, sensing & monitoring and networking & communications while two layers above of it like storage & management and smart services with an aim to synchronize with established internet infrastructure. The offered layering structure is capable to model the placement of physical objects, management system and collect the services from them.

Flow-sensor packets can be sent to any nodes even if it is sited on different networks. It allows virtual links to be created among different groups of sensors through sink nodes' negotiation. Flow-sensors are capable to create groups of sensors where data packets can be transferred discretely to individual groups without some complicated algorithms; sink nodes are required to be defined and to direct the traffic towards it. Nodes of other networks entailed to join in common networks and accomplish the task altogether through their virtual presence. Besides non-reliable internet services will be able to provide more reliable services without any modification of the IP protocol that might turn out a huge achievement in terms of reliable message delivery.

References

[1] D. Christin, A. Reinhardt, P. S. Mogre and R. Steinmetz, "Wireless Sensor Networks and the Internet of Things: Selected Challenges", Multimedia Communications Lab, Technische Universitat Darmstadt, Merckstr, Darmstadt, Germany.

[2] O. Vermesan, P. Friess, P. Guillemin, S. Gusmeroli, H. Sundmaeker, A. Bassi, I. S. Jubert, M. Mazura, M. Harrison, M. Eisenhauer and P. Dood,. "Internet of Things Strategic Research Roadmap".

[3] D. Simeonidou, R. Nejabati and S. Azodolmolky, "Enabling the Future Optical Internet with OpenFlow: A Paradigm Shift in Providing Intelligent, Optical Network Services", School of Computer Science and Electronic Engineering, University of Essex, UK.

[4] A. Mahmud, T. Kanter and R. Rahmani, "Flow-sensor Mobility and Multicast Support in Internet of Things' Virtualization, Dept. of Computer and Systems Sciences", Stockholm University, Sweden, International Conference on ICT Convergence, IEEE, Jeju Island, South Korea, in press, **(2012)**.

[5] "IOT Forum, Internet-of-Things Architecture – Updated reference model for IoT v1.5".

[6] L. Atzori, A. Iera and G. Morabito, "The Internet of Things: A survey", University of Cagliari, Italy, Computer Networks, vol. 54, no. 15, **(2010)** October 28.

[7] C. Alcaraz, P. Najera, J. Lopez and R. Roman, "Wireless Sensor Networks and the Internet of Things: Do We Need a Complete Integration?" Computer Science Department University of Malaga, Malaga, Spain.

[8] "OpenFlow Switch Specification", http://www.openflow.org/documents/openflow-spec-v1.1.0.pdf.

[9] R. Sherwood, G. Gibb, K.-King Yap, G. Appenzeller, M. Casado, N. McKeown and G. Arulkar, "FlowVisor: A Network virtualization Layer", Technical reports, Deutche Telecom and Stanford University, **(2009)** October.

[10] N. McKeown, T. Anderson, H. Balakrishnan, G. Parulkar, L. Peterson, J. Rexford, S. Shenker, and J. Turner "OpenFlow: Enabling Innovation in Campus Networks", **(2008)** March 14.

[11] R. Kraut, M. L. Maher, J. Olson, T. W. Malone, P. Pirolli and J. C. Thomas, "Scientific foundations: A case for technology- mediated social- participation theory", IEEE, **(2010)**.

[12] "Vision and Challenges for Realizing the Internet of Things", Cluster of European Research Projects on the Internet of Things (CERPIoT), http://www.internet-of-things-research.eu/pdf/IoT_Clusterbook_March_2010.pdf.

[13] J. Luo, P. Th. Eugster and J. P. Hubaux, "Route Driven Gossip: Probabilistic Reliable Multicast in Ad Hoc Networks", School of Computer and Communication Sciences Swiss Federal Institute of Technology, Lausanne, Switzerland.

[14] E. Felemban, C. G. Lee, E. Ekici, R. Boder and S. Vural, "Probabilistic QoS Guarantee in Reliability and Timeliness Domains in Wireless Sensor Networks", Electrical and Computer Engineering, Ohio State University, Columbus: Ohio.

[15] M. M. Perianu and P. Havinga, "RMD: Reliable Multicast Data Dissemination within Groups of Collaborating Objects", University of Twente, Enschede, the Netherlands.

[16] G. Wagenknecht, M. Anwander, M. Brogle and T. Braun, "Reliable Multicast in Wireless Sensor Networks", Institute of Computer Science and Applied Mathematics, University of Bern, Neubrueckstrasse 10, 3012 Bern, Switzerland.

[17] B. Chen, K. Kumar, M. Reddy and M. Welsh, "AdHoc Multicast Routing on Resource Limited Sensor Nodes", Division of Engineering and Applied Sciences, Harvard University, Cambridge, MA 02138.

[18] M. Gigli and S. Koo, "Internet of Things: Services and Applications Categorization", Dept. of Math and Computer Science, University of San Diego, USA.

[19] "The Contiki OS", http://www.contiki-os.org/p/download.html.

[20] T. Gross, T. Egla and N. Marquardt, "Sensation: A Service-Oriented Platform for Developing Sensor-Based Infrastructures", Faculty of Media, Bauhaus-University Weimar, Germany, **(2006)** April.

[21] P. Korteweg, A. M. Spaccamela, L. Stougie and A. Vitaletti, "Data Aggregation in Sensor Networks: Balancing Communication and Delay Costs", Theoretical Computer Science, vol. 410, no. 14, **(2009)** March 28, pp. 1346–1354.

[22] K. Aberer, M. Hauswirth and A. Salehi, "Middleware support for the Internet of Things", School of Computer and Communication Sciences, Lausanne, Switzerland.

[23] T. T. Thi Thuy, "Routing protocols in Internet of Things".

[24] D. Bandyopadhyay and J. Sen, "Internet of Things: Applications and Challenges in Technology and Standardization" Wireless Pers Commun, Springer, vol. 58, **(2011)**, pp. 49–69.

[25] E. Shi and A. Perring, " Designing Secure Sensor Networks," wireless Commun. Mag., vol. 11, no. 6, December **(2004)**, pp. 38-43.

Authors

Rahim Rahmani, earned a Ph.D. in communications in heterogeneous networks and he is an Associate Professor of Computer Science at the Department of Computer and System Sciences of Stockholm University, where his research focuses on Collaborative ubiquitous services and security and Ubiquitous networks. He has served as reviewer and in technical committees of international conferences. He is a member of the editorial board of International Journal of Wireless Networking and Communications.

Theo Kanter, he earned a Ph.D. in computer communications, from the Royal Institute of Technology. Theo has held a number of leading positions in telecommunications research. From 1999 to 2007, he was a senior scientist at Ericsson Research. He is now a professor at the Department of Computer and System Sciences at Stockholm University, where he leads research in adaptive and context-aware mobile communication, service architectures and self- organizing application infrastructures.