IOT Fault Management Platform With Device Virtualization

Siddesh P M[1], Pundalik Chavan[2]
[2] Assistant Professor
[1, 2] Atria Institute of Technology

Abstract- *The Internet of Things (IoT) has been developing rapidly. In a Field Area Network (FAN), where different IoT gadgets with various conventions and information groups are associated, shortcomings can without much of a stretch happen because of the FAN's insecurity. In this paper, a novel stage is proposed to give an issue the board capacity to the convoluted FAN. The stage conceals the contrasts between the gadgets by virtualizing them and gives shortcoming investigation techniques adaptably as per the FAN parts with a module structure.*

Keywords- Internet of Things, IoT Platform, Network Management, Virtualization.

I. INTRODUCTION

The IoT (Internet of Things) has been accepting expanding consideration in numerous fields. In IoT frameworks, sensors or actuators associated with the Internet assume a urgent job; they gather helpful data from the physical world or produce a physical effect in a told manner through the Internet. IoT end gadgets, for example, sensors and actuators can interface with the Internet in two different ways. In a first manner, the end gadgets direct access to the Internet through the WAN (Wide Area Network) with versatile advances, for example, 3G, LTE, and WiMAX. In a second manner, a gateway (GW) mediates between the end gadgets and the WAN. The end gadgets send the information to the GW, where the information is amassed before sending it to the WAN. To interface with the GW, LAN (Local Area Network) and PAN (Personal Area Network) advances can be utilized. The extent of this work at present covers the home and plant conditions where the IoT gadgets don't move around inside a huge area.

In this manner, the last access type is appropriate as far as the correspondence charge. The network between the GW and the end gadgets is known as a Field Area Network (FAN). In a FAN, diverse end gadgets are associated either legitimately to the GW or by means of network hardware, for example, passageways and facilitators. Embraced correspondence conventions and information groups shift crosswise over various end gadgets. In this manner FANs become heterogeneous and confused. Moreover, the FAN circumstance and design powerfully change due to, for instance, expansion, substitution, and expulsion of end gadgets and changes in detecting interims.

Numerous IoT gadgets are less dependable and utilize remote advancements. In this manner, the connections between the GW and the end gadgets will in general be shaky, so it is hard to keep up FAN solidness. Flaws can undoubtedly happen and prompt the debasement of administration quality. Consequently, issue the board is important in the FAN. At the point when a deficiency occurs, the recuperation activities from them dependent on topology recognition and issue recognizable proof must be taken. Flaws can happen both to the gadgets (for example end gadgets and network gear) and to the network. A similar issue can even be brought about by various variables and once in a while competitor remedial activity can be various.

In any case, the fulfillment of a flaw the executives are confronting the accompanying issues:

- The assortment of conventions and information organizations of IoT gadgets requires expounded advancement of capacities.
- Any flaw location and ID techniques can't exist which spread the various correspondence innovations or gadget attributes. In this paper, a novel deficiency the executive’s stage is proposed to defeat the previously mentioned issues.
- In this stage the contrasts between the gadgets are covered up with the goal that the explained advancements coming from such contrasts are decreased.
- Fault detection and identification methods are implemented as plug-ins so that each method is flexibly provided according to the FAN components.

The proposed stage gives a deficiency the executives capacity to each FAN freely from its parts and understands the steady activity of the FAN. The rest of this paper is composed as pursues. Segment II displays the job of stages in the IoT

and how a deficiency the executives work is considered among the current IoT stages. Subtleties of the proposed stage, including its virtualization idea, capacities, and engineering, are portrayed in Section III. For instance, of shortcoming discovery and determination work, which is practicable to the stage, obstruction source distinguishing proof is inspected in Section IV. At last, Section V gives the decision and a rundown of future work to be led.

II. RELATED WORK

Since the dawn of the IoT era, IoT systems have been developed vertically specialized in each application and device interface (e.g. silo approach). IoT platforms achieve interoperability among such vertical systems. The common functions which are application agnostic such as configuration, discovery, data collection, analysis and device management are provided as a platform so that the development costs can be reduced. To foster the integration of IoT systems, a myriad of commercial and open-sourced ones are provided [1]. Provision of such common functions has been standardized by some bodies. In the architecture standardized by oneM2M, CSE (Common Service Entity) provides several common functions. ETSI M2M also defines three types of SCL (Service Capability Layer) for each component: network domain, gateway and device. Several works have studied the IoT platform functions. Mineraud et al. [1] analyzed the problems in existing IoT platforms and emphasized the importance of fault management from a perspective of guarantee of data processing. Rayes and Salam [2] categorized and presented the essential management functions of the IoT platform. They consider fault management to be the most challenging and important function and list some requirements this function should support. Sheng et al.

proposed an IoT architecture with management platform [3]. Their platform supports device registration, provisioning, device management, resource observing and application data transmission. Fault management is one of the independent functions of service applications, and consequently it should also be provided as a function of the platform. Wetzker et al. discussed a failure analysis methodology and requirements and a design to realize it as a system based on their painful hands-on experiences of wireless troubleshooting [4]. In their proposed system, packets of multiple technologies and spectrum are captured and analyzed for root cause identification. However, to deal with the faults in a FAN, it is required to gather not only packets or spectrum but also information from the various devices and make it easily utilized. There have been few discussions about software architecture to foster utilization of data from devices for fault management, to the best knowledge of the authors.

III. PLATFORM DESIGN

In this area, the required capacity of FAN the executives are portrayed, trailed by a clarification of the plan idea and subtleties of the proposed stage:

A. FAN Fault Management Functions

The motivation behind flaw the executives is to understand a remote and stable FAN task with and limited human intercession. The means it takes comprise of deficiency location, underlying driver distinguishing proof (conclusion) and recuperation upheld by data social affair and topology acknowledgment.

1) Information Gathering

This capacity empowers data to be occasionally assembled from the FAN so as to perceive the topology and to oversee flaws. The data can be classified into the accompanying:

- Device Information (device depiction, for example, an ID and a gadget type)
- Link Information (which speaks to each link status and correspondence medium)
- Execution Information (gadget execution, including battery level, and CPU and memory use, and network execution, including PER (Packet Error Rate), RSSI (Received Signal Strength Indicator) and LQI (Link Quality Indicator))

So as to distinguish the underlying driver of a shortcoming, the conceivable outcomes ought to be investigated from each view point. For instance, an inaccessible gadget might be ascribed to a dead battery or to debased link quality. These conceivable causes can't be resolved from any of these data types. Accordingly, thorough data gathering is fundamental to limit the hopefuls and distinguish the main driver.

2)Topology Recognition

This capacity perceives the network topology dependent on the assembled data. Topology acknowledgment assumes a significant job in deficiency recognizable proof as a broken gadget can influence others which are associated with it. At the point when a gadget builds up an error, knowing whether different gadgets have experienced a correspondence

error can be a helpful piece of information for issue distinguishing proof. Information of the topology is likewise imperative when taking remedial activities. When exchanging channels of a gadget, all gadgets which are associated with it must be controlled to empower them to be moved to a similar channel.

3. Fault Detection and Diagnosis

An issue can be recognized from irregular conduct in execution indicators, for example, surpassing limits. The recognized deficiencies must be analyzed to distinguish their main drivers as recuperation moves can't be made without first deciding the causes. Flaw causes can be recognized dependent on how irregular execution data carries on. A few deficiencies can be cleared by one of a few restorative activities, for instance impedance can be settled either by ceasing the obstruction source or by changing to a less blocked channel. For such blames, in the conclusion of the creators, giving however much data on deficiency causes as could reasonably be expected could help in the distinguishing proof of the most suitable arrangement.

4. Recovery

After identifying the root causes, recovery from the fault takes place. Some recovery actions can be performed remotely by controlling the devices while others must be performed manually, such as removing the physical shielding objects in the FAN.

B. FUNDAMENTAL CONCEPT: FAN VIRTUALIZATION

Virtualization by and large alludes to the sensible division or conglomeration of equipment assets for a particular reason, paying little mind to any physical requirements. For instance, server virtualization can improve the accommodation of activity by considering a solitary physical server as a few servers with various OSs and assets, for example, recollections and plates, without meddling in each administration. This is a case of virtualization by partitioning equipment assets into a few coherent ones. Virtualization likewise alludes to the collection of a few physical servers, similar to database bunching for a database with high accessibility and execution. In the proposed virtualization, be that as it may, it implies abstracting an entangled FAN in an effectively sensible manner for the executive's applications.

In this paper, the thought proposed the virtualization stage which conceals the heterogeneous and muddled structure of a FAN to ease issue the board. This stage has an adjustment highlight to digest the conventions and the information designs, and pluggable issue the board highlights. The previous element empowers the stage and applications to gather data from gadgets and to control them by setting up a typical API. Then again, the last empowers to choose and tweak the flaw discovery and determination techniques adaptably relying upon the different correspondence innovations and gadget attributes.

C. PLATFORM FUNCTION

Among the flaw the executive's capacities, the stage gives the for the most part requested capacities paying little heed to FAN segments. Different capacities which may require customization are acknowledged in an adjustable way or by applications.

1) Information Gathering

The hindrances against the smooth usage of accumulated data are the diverse conventions and information designs. Besides, a few snippets of data are determined or demonstrated in various ways as per every remote chip. For instance, because of the constrained portrayal in the determination, how to ascertain and demonstrate LQI in IEEE802.15.4 is commonly left to the individual seller. Likewise, a few indicators like RSSI may require esteem offset. Nonetheless, stage modules and applications which can perceive the distinctions of the conventions and the information groups require elaboration and subsequently are difficult to broaden. In this way, the conventions and the information groups should be deciphered and bound together autonomously with the goal that the stage and applications can use the information effectively. Since it relies upon a FAN which conventions and information positions are utilized, the stage needs the modules to change over them.

2) Topology Recognition

The topology can be perceived in a typical manner to all FANs as long as the essential information is recovered. Subsequently this capacity does not have to embrace a module structure.

3) Fault Detection and Diagnosis

Fault identification and determination techniques apparently should be elaborately created in light of the fact that they every so often should be tweaked by every correspondence innovation or gadget trademark. Thus, this capacity must be acknowledged in a module structure and the strategy for every innovation and trademark are executed in the module.

4) Recovery

Some remedial activities can be naturally executed with no manual mediations by simply controlling the gadgets from the stage. The stage has the way to execute such controls.

It is not practical, in any case, to endow the entire recuperation procedure to the stage since this is a delicate theme that relies upon the activity arrangement of the FAN. Consequently, the applications ought to be in charge of choosing the suitable remedial activity as opposed to the stage. In this manner, the applications can tell the administration administrator of the shortcoming subtleties or issue an order to the stage to play out a recuperation activity. Once in a while, performing remote recuperation activities isn't as basic as is sounds. Some of them are expected to require a rationale to perform. For instance, consider the changing of the direct of ZigBee communication.

Albeit changing channels itself can be performed by sending a direction from the stage, the end gadgets must move to another channel before the organizer, generally, there are no methods for correspondence between the facilitator and the end gadgets.

D. PLATFORM ARCHITECTURE

The engineering understanding the previously mentioned capacities is given and illustrated in Fig. 1. We have built up two kinds of API (Application Programming Interface): Device API and Management API. Gadget API gives brought together strategies and information models to empower the applications and the higher modules in the stage to assemble data and control gadgets, giving no consideration to the convention and information configuration of every gadget. For data assembling, this API characterizes what execution data is to be recovered from every gadget.

For instance, RSSI, LQI and Round-Trip Time are assigned for the gadgets with radio advances. Then again, for gadget control, it gives the directions to execute recuperation activities and to change the interims of data recovery or estimation. It is imperative to help such an interim change to pursue the dynamic status change of a FAN and accomplish productive recovery. Management API is figured with the point of acquiring the topology and the shortcoming investigation results generated by the stage. The API for the topology gains the IDs and the availability of the considerable number of gadgets interfacing with the GW. The API for the flaw examination results gets the ID of a gadget and returns each issue event and goals with their timestamps. The profits can be restricted by a time go as an information. The stage receives a module structure with the goal that the accessible information arrangements, conventions and shortcoming types can be modified.

It is best that shortcomings can be overseen remotely and subsequently the proposed stage ought to be given on the cloud through the Internet. In such a case, the change of correspondence conventions ought to be attempted in the GW as a standout amongst the most crucial capacities the stage ought to give, and the higher modules and applications can migrate to the cloud. Every stage module is delineated in the accompanying:

1) PROTOCOL CONVERSION

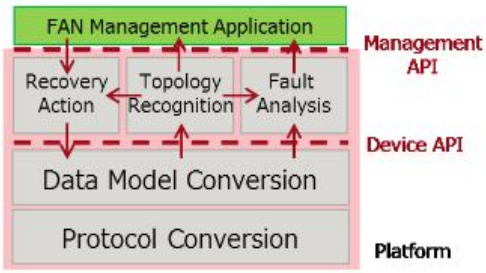

Fig. 1 Platform Architecture indicating data flow between the modules and application.

The convention and information organization of every gadget is changed over into a key-esteem pair by this module. Receiving a module structure empowers different conventions to be bolstered and new conventions to be presented easily.

2) DATA MODEL CONVERSION

The module assumes a job in changing over a key-esteem pair, whose unit or significance may be distinctive relying upon the gadget, into usually interpretable information. In spite of the fact that LQI, for instance, may be spoken to in various ways, the applications and Fault Analysis module can use LQI changed over in a brought together manner paying little heed to such contrasts. Plus, this module abstracts the models of the directions to control gadgets for remote recuperation. For the gadgets without recuperation rationale as referenced in the past subsection, the module in this module gives one. Along these lines, the applications can overlook the contrasts between the upheld elements of the gadgets.

3) TOPOLOGY RECOGNITION

Topology Recognition This module perceives the topology dependent on accumulated Device Information and

Link Information. The applications can use the topology by means of the Management API.

4) FAULT ANALYSIS

Issue Analysis This module is for flaw investigation of network and gadgets with brought together data by Device API. Regardless of whether the contrasts between correspondence advances, gadget types, and blames to be recognized and analyzed require customization, deficiency examination techniques in a module structure would probably extend over these distinctions. The investigation consequences of this module are accessible through Management API from the applications

E. IMPLEMENTATION

The proposed stage and a management application dashboard have been actualized, which was running as the application on it, is appeared in Fig. 2. This management application imagines the FAN topology and status, comprising of Wi-Fi, Bluetooth and ZigBee gadgets, and the gadget with an issue is featured in red. For the ZigBee network, the interferer recognizable proof strategy portrayed in Section IV was embraced. In this execution, HTIP [5] (Home-network Topology Identifying Protocol) was utilized to recover data from the FAN. This convention was initially intended for acquiring a home network topology and has been institutionalized as ITU-T G9973. This convention has been reached out to have the capacity to gather some helpful data to blame determination like channel.

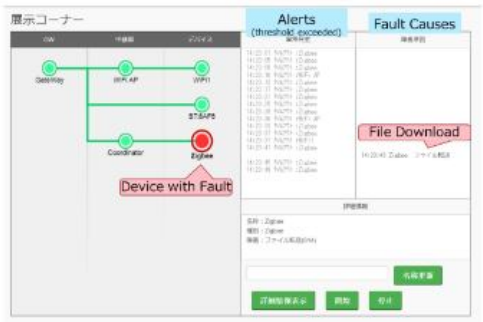

Fig. 2. FAN Management Application Dashboard

Furthermore,this protocol has been extended to allow inclusion of hardware status such as CPU usage, in the data collected and to allow the setting of measurement and collection intervals for each device.

IV. EXPERIMENTAL RESULTS OF SAMPLE FAULT ANALYSIS

A. OBJECTIVES

To demonstrate the viability of the proposed stage, an issue examination was performed utilizing execution data which can be for all intents and purposes recovered from gadgets and sent to the stage. As referenced in the past segment, to deal with a deficiency properly, it is alluring to depict its motivation in however much detail as could reasonably be expected.

FANs are often operated at 2.4 GHz, where numerous radio advancements, for example, Wi-Fi, Bluetooth, and ZigBee (IEEE802.15.4), exist together and impedance effectively happens. To exacerbate the situation, electromagnetic commotion produced from certain machines, including microwaves, can meddle with these radio advancements in this band. While Wi-Fi acquires impedance, Bluetooth and ZigBee are progressively defenseless against Wi-Fi and different sources because of their lower control and smaller transmission capacities. ZigBee particularly has no obstruction evasion capacities, not at all like Bluetooth utilizing Adaptive Frequency Hopping, and consequently is most inclined to impedance. Until this point, a few works have tended to obstruction in ZigBee networks [6-10]. Be that as it may, in most of these works, RSSI is estimated at an amazingly high rate and such a fast RSSI testing isn't practical in prevalent IoT gadgets.

In this segment, recognizable proof of an interferer application with AI strategy was performed. ZigBee was picked to get obstruction from Wi-Fi correspondence and a microwave (MWO). RSSI, LQI and Round-Trip Time (RT) were accumulated as a lot of exhibition data for the ZigBee correspondence at 120ms interims.

B. EXPERIMENT

1) GATHERING INFORMATION ON ZIGBEE COMMUNICATION

ZigBee correspondence was directed between the Raspberry Pi-based TX (transmitter) and RX (beneficiary) with an Atmel AT86RF233 ZigBee chip, where LQI was spoken to as an incentive from 0 to 255, with a higher esteem demonstrating a lower error rate. RT was estimated by methods for wpan-ping [11]. TX transmitted a ping solicitation to RX each 120 ms. On accepting the solicitation, RX estimated RSSI and LQI and sent back the

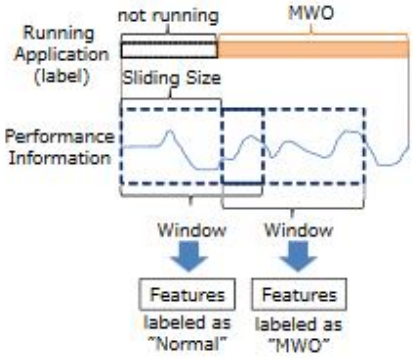

Fig. 3. Feature Extraction and Labeling

estimations to TX accordingly. TX additionally estimated RSSI and LQI when it received the reaction from RX. RT was characterized as the time from the transmission of a solicitation to the gathering of the reaction at TX. The greatest re-transmission number was three, which is widely adjusted by ZigBee gadgets. On the off chance that TX neglected to get a reaction inside 120 ms subsequent to sending a solicitation, the ping trade was viewed as a disappointment (Ping Failure) and the estimations were rounded out as missing qualities.

2) DATA COLLECTION

The information was gathered in a gathering room during the evening more than a few days. TX and RX were set around 3 m separated, and an interferer was set in the center between them. The interferer comprised of a workstation and a portable switch (IEEE802.11n/g/b) or a MWO. Applications with Wi-Fi traffic, document download, video spilling, and VoIP discussion were chosen. These machines and applications would have diverse microwave outflow or traffic designs and in this manner the execution data would likewise carry on contrastingly as indicated by each interferer. The applications, document download and video spilling (YouTube) were performed by means of an internet browser. For VoIP, the PC called to a cell phone associated with a versatile network with Skype. The intensity of the MWO was 200W. The inside recurrence of the interferers was 2412 MHz (1ch) for Wi-Fi and 2450 MHz for MWO, and a partner of ZigBee was 2410 MHz (12ch) and 2450 MHz (20ch) individually. A preliminary took the general 15 minutes, comprising of two 5-minute delays and 5-minute application running between them. For every Wi-Fi application and MWO, four preliminaries were performed.

3) INTERFERER IDENTIFICATION

Highlights were removed from a fixed-width window and marked. The window was set and moved at sliding size width over and again until the finish of the information. The name was the application that was running amid the window, in particular "Typical (without running any applications)", "Document Download", "Video" and "VoIP". The more drawn out status was chosen as a name if there were "Ordinary" and the other running application in one window. The highlights were recorded and separated from execution data. RSSI and LQI were estimated at both TX and RX. RSSI relies upon the time of estimation and a few measurements, for example, a mean and a most extreme may not be connected just to the interferers. It was consequently that these measurements were not utilized as RSSI highlights. The edge for LQI was 180, where PER compared to 0.1. The missing qualities because of ping disappointment are killed so as to figure the highlights from RSSI, LQI, and RT. Postpones included missing qualities brought about by ping disappointments and exorbitantly long RT values, as a ping disappointment may infer that a RT goes past the estimation interim. Consequently, missing qualities and RT values which are more noteworthy than the edge are considered as a postponement. This is demonstrated in twofold with "1" (Delay) for a RT abundance of 25 ms or a ping disappointment, and "0" for every single other case. Over 90% of RT values were under 25ms amid "Ordinary" in the gathered information.

4) EVALUATION AND RESULTS

For the classifier, Random Forest was chosen and actualized in R [12]. The window measure and sliding size were set as 12s separately. Four datasets were generated by choosing a preliminary for every application without covers. These four datasets were assessed utilizing 4-crease cross-approval. In each test, all test information for every application was looked over one dataset (preliminary) and the remaining datasets were utilized as the preparation information.

To accomplish a preparation balance among the classes, the information having a place with the "Typical" class was haphazardly tested and the amount of information from each class was roughly equivalent. Order execution was assessed by exactness, review and F-measure, and the normal estimation of each list is appeared. While all lists were over 80% for "Ordinary", "Record Download" and "VoIP", the F-proportion of "MWO" accomplished just 60% and "Video" accomplished under half.

V. CONCULSION AND FUTURE WORK

In this paper, a novel stage to deal with the convoluted FAN, where different gadgets with various correspondence advancements and conventions are associated,

is proposed. The stage encourages the capacities required for stable FAN activity: data gathering on gadget and network status, topology arrangement, and shortcoming management by virtualizing the gadgets in a FAN. Interferer ID for ZigBee was likewise contemplated as one of the conceivable deficiency investigation elements of the stage.

The accompanying stays for future work:

- Spectrum analyzers and packet captures are important instruments to overview the remote condition. At the point when these gadgets are utilized for issue investigation in the stage, how to learn from them will be contemplated.
- The questions from the stage to gadgets may not generally be effective in light of the fact that the correspondence situations of FANs are flimsy. Thus, Device API ought to be planned with the goal that the gadgets self-sufficiently tell the stage of the information while thinking about the network circumstance. Be that as it may, a few sorts of data, for example, RT utilized in Section IV, need an inquiry. Along these lines, the likelihood of deficiency examination without such question based data will be investigated.
- The stage bolsters remote recuperation from deficiencies with some rationale to be performed properly. Notwithstanding, extra rationale on account of recuperation activity disappointment might be required, for example, setting back to a unique channel if disengagement proceeds in the wake of moving. Subsequently, how to give such rationale will likewise be examined.

VII. ACKNOWLEDGMENT

The work has been done in the university and home. I would like to thank Mr. Pundalik Chavan for his guidance and support. Heencouraged me to write this research paper. I am also grateful to my family for putting up with me.

REFERENCES

[1] J. Mineraud, O. Mazhelis, X. Su and S. Tarkoma, “A gap analysis of Internet-of-Things platforms,” Computer Communications, vol. 89, pp. 5-16, 2016.

[2] A. Rayes and S. Samer, “Internet of Things-From Hype to Reality,” Springer, 2017.

[3] Z. Sheng, C. Mahapatra, C. Zhu and V. C. M. Leung, “Recent Advances in Industrial Wireless Sensor Networks Toward Efficient Management in IoT,” IEEE Access, vol. 3, pp. 622-637, 2015.

[4] U. Wetzker, I. Splitt, M. Zimmerling, C. A. Boano and K. Römer, “Troubleshooting Wireless Coexistence Problems in the Industrial Internet of Things,” 2016 IEEE Intl Conference on CSE and IEEE Intl Conference on EUC and 15th Intl Symposium on DCABES, Paris, France, Aug 2016, pp. 98-109.

[5] S. Zacharias, T. Newe, S. O’Keeffe, and E. Lewis, “Identifying sources of interference in RSSI traces of a single IEEE 802.15. 4 channel,” In Proc. of the 8th ICWMC, Venice, Italy, June 2012.

[6] M. Hou, F. Ren, C. Lin and M. Miao, “HEIR: Heterogeneous interference recognition for wireless sensor networks,” In Proc. of 2014 IEEE 15th WoWMoM, Sydney, Australia, June 2014.

[7] V. Iyer, F. Hermans and T. Voigt, “Detecting and Avoiding Multiple Sources of Interference in the 2.4 GHz Spectrum,” In Proc. of 12th EWSN, Porto, Portugal, February 2015.

[8] F. Hermans, O. Rensfelt, T. Voigt, E. Ngai, L. Norden, and P. Gunningberg, “SoNIC: Classifying Interference in 802.15.4 Sensor Networks,” In Proc. of the 12th IPSN, Philadelphia, US, April 2013.

[9] A. Hithnawi, H. Shafagh, and S. Duquennoy, “TIIM: Technology-independent Interference Mitigation for Low-power Wireless Networks”, In Proc. of the 14th IPSN, Seattle, US, April 2015.