

Network Working Group  
Internet-Draft  
Intended status: Standards Track  
Expires: 29 July 2022

D. von Hugo  
Deutsche Telekom  
B. Sarikaya  
25 January 2022

The Need for New Authentication Methods for Internet of Things  
draft-hsothers-iotsens-ps-01.txt

Abstract

The document attempts to establish the need for new authentication methods in the Internet of Things (IoT) as a future networking area beyond 5G going into 6G for standardization. Several scenarios are described where the current authentication protocols do not work or are insufficient. Next we discuss a few new approaches such as Wireless LAN/6G sensing and LED light based which can be further explored.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 29 July 2022.

Copyright Notice

Copyright (c) 2022 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Conventions and Terminology . . . . .	4
3. Need for New Authentication Models . . . . .	4
4. Academic Approaches to Sensing Based IoT Authentication . . . . .	5
5. IoT Authentication Protocols . . . . .	6
6. IoT Authentication Problem . . . . .	7
6.1. Architectural and Procedural Issues for Future IP-based IoT-Authentication . . . . .	7
7. IANA Considerations . . . . .	9
8. Security Considerations . . . . .	9
9. Acknowledgements . . . . .	9
10. References . . . . .	9
10.1. Normative References . . . . .	9
10.2. Informative References . . . . .	9
Acknowledgements . . . . .	13
Authors' Addresses . . . . .	13

## 1. Introduction

Future networking to make full use of 5G capabilities or even resembling an evolution to beyond 5G will have to exploit a much more heterogeneous environment in terms of network and device connectivity technologies and applications. In addition, ease of use for customers and human-independent operation of a multitude of devices and machines (things) has to be provided.

Therefore current authentication models like 802.1X [IEEE802.1X] which are based on human intervention do not fit well. Also this model does not scale well for the Internet of Things (IoT).

We can summarize the use cases we are currently considering here: Authenticating the device that is playing a melody, or a person has just touched; authenticating devices, i.e. smart teapot with certain manifests, like blinking red and blue; authenticate the device when a camera is pointed at it; and the like [Henning].

In looking for possible approaches for new authentication methods, we have identified a few which will be shortly introduced in this document.

Detection and interpretation of audio signals by microphones and corresponding

software has been under investigation since some time and can be achieved with high precision nowadays. Coding of haptic information is currently under standardisation at IEEE P.1918 [P1918].

Using an objects' position to grant authentication could be achieved via geometrical information (as e.g., position and orientation of a trusted device like the camera) or via radio sensing.

IEEE 802.11 has a project on Wireless LAN (WLAN sensing) and 802.11bf task group (TG) in charge of this project [BFSFD]. Use cases for 802.11bf TG includes room sensing, i.e., presence detection, counting the number of people in the room, localization of active people, audio with user detection, gesture recognition at different ranges, device proximity detection, home appliance control. There are also health care related use cases like breathing/heart rate detection, surveillance of persons of interest, building a 3D picture of an environment, in car sensing for driver sleepiness detection [BFUseCases].

TGbf is also working on Specification Framework Document with an outline of each the functional blocks that will be a part of the final amendment like wireless LAN sensing procedure [BFSFD]. TGbf sensing is based on obtaining physical Channel State Information (CSI) measurements between a transmitter and receiver WLAN nodes, called stations (STA). Using these measurements, presence of obstacles between a transmitter and receiver can be detected and tracked. This way, using feature extraction and classification of artificial intelligence (AI), more higher level tasks like human activity recognition and object detection are available for authentication purposes, while corresponding authentication context information can be obtained through computation of phase differences, etc.

TGbf Wi-Fi Sensing (SENS) is achieved by signaling between just an initiator and a responder. TGbf may also define more effective collaborative SENS (in short, CSENS) where multiple SENS-enabled devices can collaborate as a group in an orderly fashion to capture additional information about the surrounding environment [Rest21].

## 2. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

Sensing (SENS) is defined as the usage of received Wi-Fi signals from a Station (STA) to detect features (i.e., range, velocity, angular, motion, presence or proximity, gesture, etc.) of intended targets (i.e., object, human, animal, etc.) in a given environment (i.e., house, office, room, vehicle, enterprise, etc.).

Collaborative sensing (CSENS) defines the operation in which multiple SENS enabled devices can collaborate as a group in an orderly fashion to capture additional information about the surrounding environment and allow for more precise detection thus enabling a more reliable authentication.

Multi-band sensing is defined as sensing using both sub-7-GHz Channel State Information (CSI) measurements that provide indication of relatively large motions and that can propagate through obstacles (e.g., walls) and 60-GHz Received Signal Strength Indicator (RSSI) measurements at mmWave that provide highly-directional information through the usage of beam forming toward a given receiver, but have small range due to the presence of blockers (e.g., walls).

## 3. Need for New Authentication Models

Aim of this document is to lay ground for the need for new authentication models in the framework of devices (e.g., machines in IoT communication) within a (wireless or wireline-based) network. Currently employed authentication models (such as e.g., 802.1X certificate model) is based on a human being using the machine and providing credentials (e.g., user name/password or a permitted digital certificate) to the authenticator. Similarly, for user equipment (UE) to access a cellular network the device has to be equipped with a USIM and the user has to provide a secret key, i.e., PIN (Personal Identification Number). With the use case of massive IoT (mIoT) as foreseen, e.g., in 5G and with an increasing amount of devices within a household (smart home) and/or in the ownership of a customer (smart watch etc.) the need for an ease-of-use admission model arises.

Focusing on corresponding procedures starting with detection (sensing) of a new device and subsequent mutual authenticating of the device by and to the network a set of potential technologies are

identified and described to allow for analysis in terms of criteria as reliable operation (working), scalability, ease of use and convenience, security, and many more. Sensing could be a basis for new authentication models yet to be found because sensing (together with intelligent interpretation using possibly neural network models) will allow the detection of the device playing a melody, blinking red and blue, being pointed at, or somebody just touched and the like. Furthermore, the method should be applicable to future generations of network and of users, upcoming new applications and devices, assuming that today's established standard procedures do not fulfill the requirements sufficiently.

New authentication methods could leverage collaborative and multi-band sensing technologies to enable sensing with much higher precision and capacity using the state-of-art equipment. Also equally important is the use of all artificial intelligence and neural networks research results developed by the academia.

#### 4. Academic Approaches to Sensing Based IoT Authentication

The following list of literature on sensor data and WiFi sensing for securing and authenticating a user and a device shows the wide range of approaches and interest in this topic [Rest21].

[Ma], [Wang], [Zhu], [Wang2], [Qian] provide a holistic overview on the evolution of Wi-Fi technology and on investigations in opportunistic applications of Wi-Fi signals for gesture and motion detection.

[Henning2] is investigating geospatial access control for IoT. There are attribute, role and identity based, time based and geospatial access control techniques. Real-world IoT access control policies will be a combination of all three, leading to powerful access control techniques to use in practice such as in university campus. Such access control or authorization techniques will likely be used in conjunction with these new IoT Authentication models.

Other notable literature includes [Al-Qaness] on the so-called device-free CSI-based Wi-Fi sensing mechanism, [Pahlavan] using Wi-Fi signals for gesture and motion detection as well as for authentication and security, [Lui] distinguishing between Line-of-Sight (LOS) and Non-Line-of-Sight (NLOS) conditions in case of obstacles appearing between the transmitter and the receiver [Guo] studying HuAc (Human Activity Recognition) as a combination of Wi-Fi-based and Kinect-based activity recognition system, [FURQAN] analyzing the wireless sensing and radio environment awareness mechanisms, highlighting their vulnerabilities such as dependency of sensing modes on external signals, and provides solutions for

mitigating them, e.g., the different threats to REM (radio environment mapping) and its consequences in a vehicular communication scenario.

[Ma2] has studied reliable SENS algorithm for human and animal identification. The aim is to make it resilient to spoofing and adverse channel conditions, i.e., presence of noise and interference from other technologies.

[Restuccia] investigates data driven algorithms, neural networks, especially convolutional neural network (CNN) or digital signal processing (DSP) block to classify complex sensing phenomena. Also [Liao] and [Liao2] proposed to enhance security of industrial wireless sensor networks (IWSNs) by neural network based algorithms for sensor nodes' authentication and implementations in IWSNs have shown that an improved convolution preprocessing neural network (CPNN)-based algorithm requires few computing resources and has extremely low latency, thus enabling a lightweight multi-node PHY-layer authentication.

Further research on these and similar issues can be found in [Tian], [Bai] [Axente].

## 5. IoT Authentication Protocols

Since IoT applications cover a broad range of domains from smart cities, industry, and homes to personal (e.g., wearable) devices, including security and privacy sensitive areas as e-health, and can reach a huge number of entities the security requirements in terms of preventing unauthorized access to data are very high. Therefore very robust authentication mechanisms have to be applied. At the same time depending on the specific scenario a trade-off between resources as processing power and memory and security protocol complexity has to be considered. Also a plethora of attack scenarios has to be in focus as well as scalability of the considered implicit and explicit hardware- and software-based authentication procedures. [RFC8576] serves as a reference for details about IoT specific security considerations including the area of authentication and documents their specific security challenges, threat models, and possible mitigations. Also the OAuth [RFC6749] protocol is referred to which extends traditional client-server authentication by providing a third party client with a token instead of allowing it to use the resource owner's credentials to access protected resources while such token resembles a different set of credentials than those of the resource owner.

## 6. IoT Authentication Problem

Most of the state-of-art identification techniques to authenticate the user use finger prints a.k.a. touch id and facial identification and they use detection by touch, accelerometer, and gyro sensors or cameras. They are based on creating a signature, or the user's already stored password [Wang3].

On the other hand to authenticate a device based on a set of characteristic parameters which should be flexibly chosen by the owner and subsequently made known to the authentication system will require a certain level of processing and storage capacity either within the local system components (e.g., the device itself and the wireless point of attachment or access point) and/or within the network (e.g., an edge cloud instance or a central data base). The result of the detection process (e.g., radio wave analysis outcome in terms of parameters as modulation scheme, number of carriers, and fingerprinting) has to be compared with the required (correct) parameter values which are safely stored within the network components. On all levels of handling these data, i.e., storage, processing, and transport via a communication network, the integrity of the content has to be preserved. One should keep in mind, that any unintended authentication request should be prevented to minimize the risk of occasional attachment to networks and subsequent exposure to attack to sensitive user data.

### 6.1. Architectural and Procedural Issues for Future IP-based IoT-Authentication

Authentication for IoT may rely on a protocol such as 6LowPAN (Low-power Wireless Personal Area Network) which is defined for optimizing the efficient routing of IPv6 packets for resource constrained machine- type communication applications.

[RFC8995] on 'Bootstrapping Remote Secure Key Infrastructure' (BRSKI) deals with authentication of devices, including sending authorizations to the device as to what network they should join, and how to authenticate that network by specifying automated bootstrapping of an Autonomic Control Plane (ACP). Secure Key Infrastructure (SKI) bootstrapping using manufacturer- installed X.509 certificates combined with a manufacturer's authorizing service, both online and offline, is called the Bootstrapping Remote Secure Key Infrastructure (BRSKI) protocol. Bootstrapping a new device can occur when using a routable address and a cloud service, only link- local connectivity, or limited/disconnected networks and includes support for deployment models with less stringent security requirements. When the cryptographic identity of the new SKI is successfully deployed to the device, completion of bootstrapping is achieved. A locally issued certificate can be deployed to the device via the established secure connection as well.

LED light based authentication attempts to authenticate hard to reach IoT devices using LED light indicator available on the device. Here LED light is used as an out-of-band channel in addition to a wireless LAN peer-to-peer connection to the device using a smartphone over TLS connection which is not secured. Smartphone initially obtains device's public key certificate. Smartphone as the client requests certificate fingerprint over visible LED light channel. Device transmits fingerprint by modulating LED. Client receives data with camera and decodes. Client compares TLS certificate fingerprint with received fingerprint to complete authentication. LED light based authentication does not support multiple ways of getting the hash value from the device. Although most devices have LED type of output leading to visible light communication, some devices have speaker type of output and not readily visible [Lins18], [Oden18].

Note that LED light based authentication is similar to EAP-NOOB, Nimble out-of-band authentication for EAP [RFC9140] where Zigbee or 802.15.4 channel is the main channel and blinking LED light is used as out-of-band channel. In the main channel, the device is connected to the Internet over 802.15.4 channel to a controller (a laptop, acting as a Wi-Fi access point) which connects over the Internet to AAA server as EAP server where the user has an account. In the OOB channel, the device is connected to a smartphone using blinking LED light and the smartphone is connected to AAA server using its 4G/5G air interface. OOB channel enables the device to send critical data needed i.e. a secret nonce to EAP server. EAP-NOOB protocol architecture includes RADIUS which is used to encode EAP messages and constrained Application Protocol, CoAP which is a simplified HTTP. CoAP is used in transporting the nonce. EAP-NOOB requires AAA server and user account on the server, i.e. human interaction.

When compared to a fully certificate-based or secure key infrastructure based authentication, however, a mechanism relying on WiFi sensing gesture detection does not require the user to know any key, identifier, or password for the device to be authenticated. A pre-defined type of access to the device (e.g., physical, photographic or video representation, unique description in terms of parameters, etc.) shall be sufficient for authentication.

## 7. IANA Considerations

TBD.

## 8. Security Considerations

This document raises no new security concerns but tries to identify how to increase security in future IoT by discussing the issues of robust but easy to apply authentication mechanisms.

## 9. Acknowledgements

Discussions with Jan Janak, Henning Schulzrinne helped us improve the draft.

## 10. References

### 10.1. Normative References

- [RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <<https://www.rfc-editor.org/info/rfc2119>>.
- [RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <<https://www.rfc-editor.org/info/rfc8174>>.

### 10.2. Informative References

- [Al-Qaness] Al-Qaness, M.A.A., Abd Elaziz, M., Kim, S., Ewees, A.A., Abbasi, A.A., Alhaj, Y.A., and A. Hawbani, "Channel State Information (CSI) from Pure Communication to Sense and Track Human Motion: A Survey", *Sensors* 2019, 19(15), 3329, July 2019.

- [Axente] Axente, M.-S., Dobre, C., Ciobanu, R.-I., and R. Purnichescu-Purtan, "Gait Recognition as an Authentication Method for Mobile Devices", *Sensors* 2020, 20, 4110 , July 2020.
- [Bai] Bai, L., Zhu, L., Liu, J., Choi, J., and W. Zhang, "Physical Layer Authentication in Wireless Communication Networks: A Survey", *Journal of Communications and Information Networks* Vol.5, No.3, September 2020.
- [BFSFD] IEEE, "Institute of Electrical and Electronics Engineers, IEEE P802.11 - TASK GROUP BF (WLAN SENSING) 11-21/0504r2 "Specification Framework for TGBf"", July 2021.
- [BFUseCases] IEEE, "Institute of Electrical and Electronics Engineers, IEEE P802.11 - TASK GROUP BF (WLAN SENSING) 11-20/1712r2 "WiFi Sensing Use Cases"", January 2021.
- [FURQAN] Furqan, H.M., Solaija, M.S.J., Tuerkmen, H., and H. Arslan, "Wireless Communication, Sensing, and REM: A Security Perspective", *IEEE Open Journal of the Communications Society* Vol. 2 , January 2021.
- [Guo] Guo, L., Wang, L., Liu, J., Zhou, W., and B. Lu, "HuAc: Human Activity Recognition Using Crowdsourced WiFi Signals and Skeleton Data", *Hindawi Wireless Communications and Mobile Computing*, Volume 2018 , February 2021.
- [Henning] Schulzrinne, H., "Do We Still Need Wi-Fi in the Era of 5G (and 6G)?", February 2021.
- [Henning2] Jan Janak, Luoyao Hao and Henning Schulzrinne, ., "How do we program the Internet of Things at scale?", September 2021.
- [I-D.irtf-t2trg-secure-bootstrapping-00] Sethi, M., Sarikaya, B., and D. Garcia-Carrillo, "Secure IoT Bootstrapping: A Survey", Work in Progress, Internet-Draft, draft-irtf-t2trg-secure-bootstrapping-00, 7 April 2021, <<https://www.ietf.org/archive/id/draft-irtf-t2trg-secure-bootstrapping-00.txt>>.
- [IEEE802.11] IEEE, "IEEE Std. 802.11-2016", December 2016, <<https://standards.ieee.org/findstds/standard/802.11-2016.html>>.

- [IEEE802.1X] IEEE, "Institute of Electrical and Electronics Engineers, "802.1X - Port Based Network Access Control"", January 2020.
- [Liao] Liao, R.-F., Wen, H., Wu, J., Pan, F., Xu, A., Jiang, Y., Xie, F., and M. Cao, "Deep-learning-based physical layer authentication for industrial wireless sensor networks", *Sensors* 2019, 19(11), 2440 , May 2019.
- [Liao2] Liao, R.-F., Wen, H., Wen, H., Xie, F., Pan, F., Pan, F., and F. Xie, "Multiuser Physical Layer Authentication in Internet of Things With Data Augmentation", *IEEE Internet of Things Journal*, vol. 7, no. 3, pp. 2077-2088 , March 2020.
- [Lins18] Linssen, A., "Secure Authentication of Remote IoT Devices Using Visible Light Communication: Transmitter Design and Implementation", Columbia University , 2018, <[https://www.cs.columbia.edu/~hgs/papers/Lins18\\_Secure.pdf](https://www.cs.columbia.edu/~hgs/papers/Lins18_Secure.pdf)>.
- [Lui] Liu, J., Wang, L., Fang, J., Guo, L., Lu, B., and L. Shu, "Multi-Target Intense Human Motion Analysis and Detection Using Channel State Information", *Sensors* 2018, 18(10), 3379 , October 2018.
- [Ma] Ma, Y., Arshad, et al, S., and , "Location-and Person-Independent Activity Recognition with WiFi, Deep Neural Networks, and Reinforcement Learning," , 2021.
- [Ma2] Ma, Y. and G. Zhou, et al, "WiFi Sensing with Channel State Information: A Survey," , *ACM Computing Surveys (CSUR)*, , vol. 52, no. 3, pp. 1-36, 2019.
- [Oden18] Odental, H., "Secure Authentication of Remote IoT Devices Using Visible Light Communication: Receiver Design and Implementation", Columbia University , 2018, <[https://www.cs.columbia.edu/~hgs/papers/Oden18\\_Secure.pdf](https://www.cs.columbia.edu/~hgs/papers/Oden18_Secure.pdf)>.
- [P1918] IEEE Standards Working Group 1918.1, "Tactile Internet", July 2016.
- [Pahlavan] Pahlavan, K. and P. Krishnamurthy, "Evolution and Impact of Wi Fi Technology and Applications: A Historical Perspective", Springer Science+Business Media, LLC, part of Springer Nature 2020 , November 2020.

- [Qian] Xian, K. and C. Wu, et al, "Widar: Decimeter-level Passive Tracking via Velocity Monitoring with Commodity WiFi," Proc. of ACM MobiCom, , 2017.
- [Rest21] Restuccia, F., "IEEE 802.11bf: Toward Ubiquitous Wi-Fi Sensing", arXiv preprint arXiv:2103.14918 7 pages, March 2021.
- [Restuccia] Restuccia, F. and T. Melodia, "Deep Learning at the Physical Layer: System Challenges and Applications to 5G and Beyond," IEEE Communications Magazine, , vol. 58, no. 10, pp. 58-64, 2020.
- [RFC6749] Hardt, D., Ed., "The OAuth 2.0 Authorization Framework", RFC 6749, DOI 10.17487/RFC6749, October 2012, <<https://www.rfc-editor.org/info/rfc6749>>.
- [RFC8576] Garcia-Morchon, O., Kumar, S., and M. Sethi, "Internet of Things (IoT) Security: State of the Art and Challenges", RFC 8576, DOI 10.17487/RFC8576, April 2019, <<https://www.rfc-editor.org/info/rfc8576>>.
- [RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <<https://www.rfc-editor.org/info/rfc8995>>.
- [RFC9140] Aura, T., Sethi, M., and A. Peltonen, "Nimble Out-of-Band Authentication for EAP (EAP-NOOB)", RFC 9140, DOI 10.17487/RFC9140, December 2021, <<https://www.rfc-editor.org/info/rfc9140>>.
- [Tian] Tian, Q., Lin, Y., Guo, X., Wang, J., AlFarraj, O., and A. Tolba, "An Identity Authentication Method of a MIIoT Device Based on Radio Frequency (RF) Fingerprint Technology", Sensors 2020, 20(4), 1213 , February 2020.
- [Wang] Wang, X. and C. Yang, et al, "TensorBeat: Tensor Decomposition for Monitoring Multiperson Breathing Beats with Commodity WiFi," ACM Transactions on Intelligent Systems and Technology (TIST), , vol. 9, no. 1, pp. 1-27, 2017.
- [Wang2] Wang, X. and C. Yang, et al, "PhaseBeat: Exploiting CSI Phase Data for Vital Sign Monitoring with Commodity WiFi Devices," Proc. of IEEE ICDCS, , 2017.

- [Wang3] Wang, H., Lymberopoulos, D., and J. Liu, "Sensor-Based User Authentication", EWSN 2015, LNCS 8965, 168 , 2015.
- [Zhu] Xiao, et al, F., "R-TTWD: Robust device-free through-the-wall detection of moving human with WiFi,", IEEE Journal on Selected Areas in Communications, , vol. 35, no. 5, pp. 1090-1103, 2017.

#### Acknowledgements

#### Authors' Addresses

Dirk von Hugo  
Deutsche Telekom  
Deutsche-Telekom-Allee 9  
64295 Darmstadt  
Germany

Email: Dirk.von-Hugo@telekom.de

Behcet Sarikaya

Email: sarikaya@ieee.org

Independent Submission  
Internet-Draft  
Intended status: Informational  
Expires: 28 April 2022

K. Makhijani  
L. Dong  
Futurewei  
25 October 2021

Framework For Integrated Industrial Networks  
draft-iotops-km-iiot-frwk-00

## Abstract

Industry control networks host a diverse set of non-internet protocols supporting Industrial-IoT and legacy device connections. The integration between traditional information technology (IT) and operational technology (OT) so far has centered around collection of real-time data from devices in OT environment for consumption within the enterprise IT networks. However, improvements in process control and automation require a far better interworking between the OT and IT applications. This document provides a reference framework for integrated industry networks (IIN). It highlights interfaces and their characteristics required for interconnecting components of OT and IT that maybe moved to the cloud or edges. It suggests the use of IIN to bridge the differences between OT and IETF technologies.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 28 April 2022.

## Copyright Notice

Copyright (c) 2021 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Terminology . . . . .	4
2.1. Acronyms . . . . .	5
3. High Level Considerations . . . . .	5
3.1. Integrated Industrial Network Stack . . . . .	5
3.2. Deployment Considerations . . . . .	7
3.2.1. Limited Domain Network Inspired Framework . . . . .	8
3.3. Alignment with stakeholders . . . . .	9
4. IIoT New Requirements . . . . .	10
4.1. Device to Cloud Mechanisms . . . . .	11
4.2. Preserving Performance and Deterministic Behavior . . . . .	11
4.3. Preserving Safety and Task outcomes . . . . .	11
4.4. Interoperability with IP-world machines . . . . .	11
4.5. Digital Twin . . . . .	11
5. IIN Framework . . . . .	12
5.1. Distributed Architecture . . . . .	12
5.2. Interfaces . . . . .	12
5.3. IIN Device Functions . . . . .	14
5.3.1. Device Specific functions . . . . .	14
5.3.2. Transmission (Transport) Mechanisms . . . . .	14
5.3.3. Routing considerations to provide safety & security . . . . .	14
5.3.4. Traffic Profiles for different type of data . . . . .	15
6. IANA Considerations . . . . .	15
7. Security Considerations . . . . .	15
8. Acknowledgements . . . . .	15
9. Informative References . . . . .	15
Authors' Addresses . . . . .	16

## 1. Introduction

There is very little cross-over between the network technologies used in the OT and IT environment. The OT networks are responsible for automation and process control on premises such as factory floors, manufacturing plants, power grids, oil & gas industry, etc. In contrast, IT networks traditionally facilitated business applications based on data received from OT applications. With increased

automation, and growing demand for remote operations, it is imminent that the two technology domains need to interwork seamlessly and reliably.

Due to lack of coordination between industrial networks and IETF technologies, their evolution priorities have been different and as a result, current IETF technologies and protocols are not well adapted in industrial networks. Industrial systems and applications are becoming increasingly complex and proprietary as emerging use cases require a higher integration of OT-IT functions.

The OT networks are often tied to a set of non-internet protocols such as Modbus, Profibus, CANbus, Profinet, etc [SURV]. There are more than 100 different protocols each with it's own packet format and are used in the industry. On the other side inventory management, analytics, monitoring, supply chain and simulation software are part of IT and use IP based technologies.

Note: use IETF technology (instead of IP-based) as a more inclusive term.

No two industry sectors are same and present different requirements and challenges on the networks. These differences are even more enhanced in industry automation and operations. The processes, control operations, environmental conditions, frequency and type data collection vary across each sector. Yet, there is a need for common, interoperable, off-the-shelf mechanisms and protocols so that applications can be deployed in relatively shorter time.

Note: maybe later describe examples from different sectors. e.g. petrochemical or mining plant vs manufacturing and transportation. or simply refer to IIC case studies.

This document provides a framework called 'Integrated Industrial Networks' (or IIN for short) and a discussion on integration of process control, monitoring and operations with IT. It proposes (a) an idea about integrated industrial network stack that would support functions and capabilities from both OT and IT systems, (b) a structured deployment considerations, (c) alignment and coordination across stakeholders from other consortia and SDOs.

## 2. Terminology

### Industrial Control Networks:

The industrial control networks are interconnection of equipments used for the operation, control or monitoring of machines in the industry environment. It involves different level of communications - between field bus devices, digital controllers and software applications

### Industry Automation:

Mechanisms that enable machine to machine communication by use of technologies that enable automatic control and operation of industrial devices and processes leading to minimizing human intervention.

### Control Loop:

Todo

### Feedback Control Loop:

Todo

### Programmable logic controllers (PLC):

Industrial computers/servers for the control of manufacturing processes such as assembly lines.

### Supervisory Control and Data Acquisition (SCADA):

Software System to control industrial processes and collect and manage data.

### Distributed Control Systems (DCS):

Systems of sensors and controllers that are distributed throughout a plant.

### Manufacturing Execution System (MES):

Systems that connect production equipment across the factory floor, or multiple plants or sites.

### Fieldbus Devices:

Operational Technology field devices include valves, transmitters, switches and actuators etc.

### Integrated Industrial Network (IIN):

The term introduced in this document to represent a converged view of OT and IT networks.

## 2.1. Acronyms

- \* HMI: Human Machine Interface
- \* MES: Manufacturing Execution System
- \* IIN: Integrated Industrial Network
- \* IIC: Industrial Internet Consortium

## 3. High Level Considerations

In this framework a greater focus is on capturing functional and operational requirements for the emerging use cases. The top three considerations are – first, to identify the components required to fulfill the needs for both IT and OT applications. Second, Integrated Industrial Network (IIN) Framework needs to meet and adapt to evolving deployment strategies that include cloud and edge technologies. Finally, mechanisms to coordinate with stakeholders (domain experts) should also be identified when discussing such a framework.

### 3.1. Integrated Industrial Network Stack

Industrial Networks are a combination of technologies that provide capability for the delivery of process control data to/from (and across) the machines and sensors to different controllers and other application specific servers. Thus, in IIN stack, one end often be an OT device and other end an IT function.

In OT Systems traditionally,

- \* Operations or tasks are Well-defined: the emphasis is on having specific set of tasks performed with definitive outcomes and behavior.
- \* Safety is paramount: protecting and preventing the state of the system from potential harm or disruption. The requirements in networks translate to multiple attributes such as each signals to shut off a valve are received in predictable (or real-time) and are never lost.

In addition, there is also an emergence of new use cases and scenarios in OT:

- \* Multiple applications: Number of use cases are increasing from traditional deployments. A plant may need different industry protocols for different use cases. For example, BACNet for building automation, ModBus devices for valve or pressure control, ProfiBus IP for surveillance.
- \* Virtualization: The role of software PLCs is growing. When met with specific time-specific constraints, virtual PLCs can operate on actuators and sensors as well as physical PLCs. In addition they can be extended to support rich set of new functions controlling different type of end devices from a single PLCs. Not to mention systems such as SCADA, MES, HMI and ICS are also being virtualized and can be deployed and operated in distributed fashion.
- \* Analytics: New kinds of sensors are being deployed to monitor the health of the equipment and environmental conditions. The data collected from sensors helps in predictive maintenance, changing production schedules etc.
- \* Simulation models: TBD.
- \* PLC and OT Cloudification: Due to virtualization of components, it is now possible to place them anywhere in edge or cloud depending on the application design.

Some of the reasons why leveraging IETF technologies would be beneficial:

- \* Scalability: IETF solutions are designed for scale and perform well when dealing with large-scale network connectivity and reachability.
- \* Monitoring: Available solutions for health, operations and management of the network devices.
- \* Security: Comprehensive set of security solutions (at least in IT applications).

Note: we can add more details on routing, device and service discovery or even transport.

See Section 4 for details.

### 3.2. Deployment Considerations

A conceptual industry adopted reference model for network segmentation is known by Purdue model or ISA-95 [ISA95]. It shows hierarchical levels through which ordered connectivity between the components (or entities) in Industry Control Systems (ICS) is established. These levels range from 0 at the lowest level for the physical devices to applications at level 5. Those levels also include other control and management equipments (potentially treated as in-network functions and capabilities).

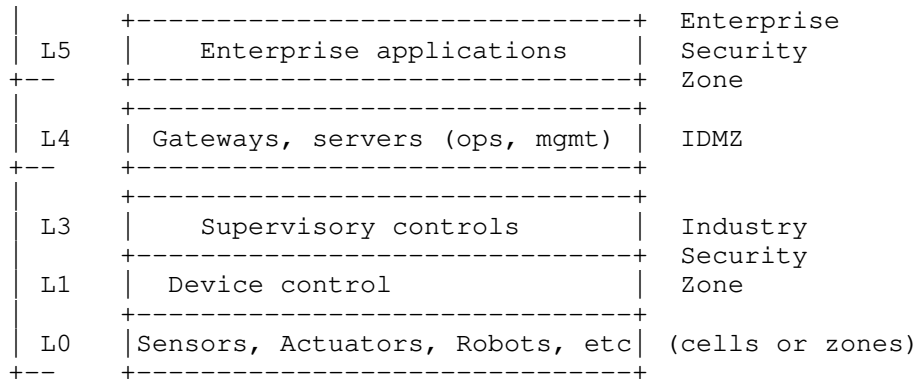


Figure 1: ISA 95 or Purdue model of Automation Pyramid

The scope and functions in each zone in [ISA95] are summarized below:

- \* Enterprise Security Zone: The IT applications reside in enterprise networks and perform tasks necessary for business operations such as inventory control, supply-chain logistics, schedule and capacity planning. They need to collect data from the OT systems in order to make those decisions.
- \* Industrial Demilitarized Zone: The OT and IT networks were designed to prevent direct communication between them. The IDMZ serves as an information sharing layer between the IT and OT (L4 and L3) systems. This indicates that additional security rules, inspection and protection of device identity and access is necessary when transiting from L3 to L4.
- \* Manufacturing Zone: Consists of Levels 0 through 3 site wide production system.
  - Site operations (L3): Supports side-wide view of the production system. Also provide data to L4.

- Area supervisory control (L2): Performs operation and control over a zone or smaller area in a production floor. Each area has specific set of tasks or operations to perform.
- Basic control (L1): For the actual control of the equipment. L1 components send commands to L0 equipments to perform tasks (e.g. start motor, alter pressure level, or reduce motor speed).
- Process(L0): Level for the process equipments performing actual operations are performed. This include equipment and devices such as motors, pressure valves, temperature, speed, etc sensors, etc.

### 3.2.1. Limited Domain Network Inspired Framework

Effectively, industrial networks are under a single administrative control or a limited group of administrators. They are expected to extend across different geographies and over a range of distances.

RFC 8799 [LDN] introduces a formal structure and taxonomy to describe large-scale private networks called limited domains. LDNs use public Internet for connectivity across multiple sites and adhere to Internet protocols. However, within a site, it is acceptable to use proprietary protocols. Thus, an LDN comprises of Internal, External and Boundary protocols.

Industrial networks also extend to multiple sites. The enterprise services will reside in the cloud or edges, while factory floors or plants are at remote locations. Structurally, ISA architecture (Figure 1) can be expressed as IETF's Limited Domain Networks [LDN] framework. Thus, L4 and L5 levels in enterprise zone are one site, connected via global Internet to L3-L0 levels at factory floors or plants. Using LDN model, we get break down the framework requirements systematically:

- \* Inside Network Requirements (manufacturing zone) Inside networks support OT specific protocols and maybe combination of IP and non-IP solutions. This may utilize encapsulations in IP, compression of headers in IP or new native-short header approaches.
- \* Outside Network Requirements (global or public Internet) External public networks will interconnect different sites using IETF technologies of the Internet. These may utilize pure IPv6, NAT, VPNS or similar technologies.

- \* Boundary Network Requirements - for translations between inside to outside protocols.

Note: LDN is a methodology that helps in defining deployment boundaries (how, what, where) between the use specific protocols in a network-zone. it is specifically interesting here because of 2 reasons - as virtualized components move from one site to other security, safety and data-privacy perimeter changes. We need to make sure proper security profiles get applied. Secondly, it especially aligns well with the border protocols mapping to the IDMZ definition in Purdue model. There is one problem though - instinctively, we see edge services located in boundary protocols (or in IDMZ) not as a separate site. So RFC8799 needs to say more than translations about the border protocols.

### 3.3. Alignment with stakeholders

The paradigms of networking in OT are quite different than IP based best-effort networking protocols. Yet, IETF protocols are extensively used in OT applications. Often, it is not possible to get contributors directly from the OT sectors, then it would make more sense to coordinate with well-established consortia where OT scenarios and requirements are discussed may be utilized. Two well established foundations are IIC [IIC] and OPC-UA [OPC]. For example, a [IIC\_TALK] provided overview of IIC activities.

Industrial IoT Consortium (IIC) provides use cases, scenarios, and best-practice frameworks to solve specific problems and solution pain points. It is a rich resources of case studies and demonstrations of different test beds. The IIC itself is not involved in standards development, but may help in formalizing requirements, further insights into solutions developed in IETF, and potentially help adoption of those solutions.

Open Platform Communications-Unified Architecture (OPC-UA) provides interoperability across different hardware platforms using a standard data model. It standardizes various information models, corresponding client-server architecture and defines necessary access mechanisms to those information models. The OPC-UA is an abstraction layer to provide common interface to different data look-up and event notifications. A number of information models are provided by OPC-UA can be found here [OPC\_INFO]. For example, OPC has a specification on PLCs. It abstracts PLC specific protocols (such as Modbus, Profibus, etc.) into a standardized interface allowing HMI/SCADA systems to interface with a middleware that converts generic-OPC read/write requests into device-specific requests and vice-versa.

Note: OPC-UA information model similar to YANG?

IETF solutions will focus on leveraging or extending IETF technologies for IT and OT integration which is at the infrastructure or communication layer. Thus, providing protocols that could potentially benefit higher-level OPC-UA work.

Both IIC and OPC could provide guidance to the lower level work.

- \* For Discussion: assuming there is an IIN framework – how does it fit in the OPC-UA architecture and facilitate adoption of existing information models.

#### 4. IIoT New Requirements

Traditionally, OT and IT experts have focussed on different concerns. On a production floor or with OT, the focus is generally on no-congestion, lossless reliable transmission, and real-time or deterministic communication. Quality of manufactured goods, and efficiency of processes is also an important concern for OT experts.

With Industry 4.0 initiatives (such as smart factory and smart manufacturing), these concerns are beginning to overlap, i.e. OT networks are also required to be concerned with scalability, security, operations and maintenance from remote locations.

The fundamental requirement for industrial networks is to support legacy devices (even when the network infrastructure is upgraded) while enabling emerging applications.

- \* Requirements from legacy device support:

1. Support for protocol formats and their core capabilities.
2. Support for traffic profiles for different types of services
3. Support for security and separation as designed in OT systems.

- \* Requirements from Emerging Trends:

1. Support device to cloud communication (remote operations)
2. Virtualization (virtual PLCs, digital twins)
3. High-volume data emission (analytics and surveillance)
4. Explicit location awareness (to determine edge networks, latency sensitive controls, safety operations).

5. Enhanced Industry data and device security (movement of sensitive data and remote control)

#### 4.1. Device to Cloud Mechanisms

Perimeter of device control is expanding from factory floors to the cloud. It is anticipated that Industrial IoT controls when extended to the cloud or edge compute platforms will offer better integration with sophisticated business logic application architectures.

With adoption of virtualization several of supervisory or management equipment could transition to IT infrastructure. It may or may not remain on-premises. All scenarios are possible - moving L1,L2, L3 to separate IT network on the same floor, to the edge or to the cloud. Now extending the communication to the edge and cloud nodes increases the distance requiring adoption of layer 3 network designs.

#### 4.2. Preserving Performance and Deterministic Behavior

Shorter addresses are inherent to industry control systems to provide implicit determinism. For this purpose, the industrial networks use fieldbus interface with the controllers.

#### 4.3. Preserving Safety and Task outcomes

#### 4.4. Interoperability with IP-world machines

To develop further on different type of address format support. From smaller address of legacy devices to IT based applications with IP address.

(OT-Address)--->(Industry Control)--->(IP-Address)  
(control dev)            ( network )            (application)

Preferably allow OT devices to understand IP-addresses for the servers they connect to.

#### 4.5. Digital Twin

Note: Should we include this. A digital twin is a virtual 3D representation of the real world. It can show physical objects, processes, relationships, and behaviors - and it can represent them as they are now, as they were in the past or will be in the years ahead. Some discussions have already begun, for example [I-D.draft-zhou-nmrg-digitaltwin-network-concepts].

## 5. IIN Framework

Above mentioned emerging trends such as virtualization of PLCs or moving MES or HMI into the cloud will have a significant impact on the framework. It moves functions from manufacturing zone to the cloud which not only influences how latency, safety and resiliency can be assured but also moves the security zones.

### 5.1. Distributed Architecture

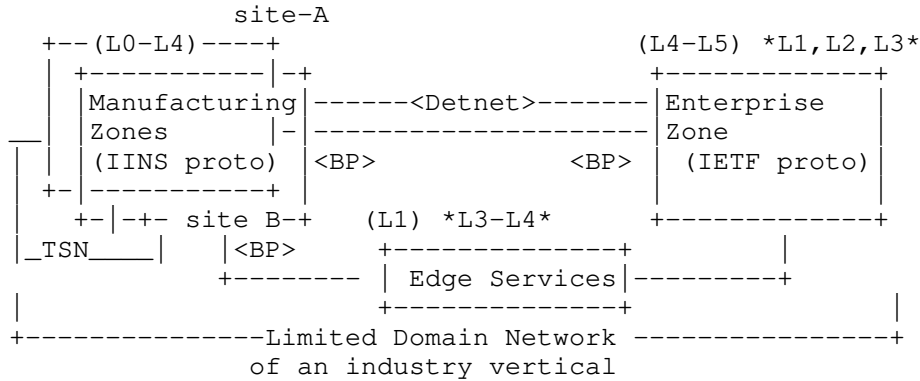


Figure 2: Integrated Framework with new placements for ISA 95 levels

In Figure 2, LDN taxonomy of internal, external and boundary protocols is used. The round brackets represent current Purdue model levels. Note that both Manufacturing and Enterprise zones are 'inside protocols' in LDN terminology but can (or may) run different protocol stacks. Each zone may deploy either custom or standard protocols. They interact using outside protocols i.e., public Internet technologies. The translation from inside to outside protocol happens through boundary protocols (shown as <BP> in the figure).

- \* IINS (Integrated Industrial Network Stack) Protocols: A set of inside protocols that are used in traditional manufacturing zones. These are expected to support and extend existing industry protocols or may even be new extensions. Note that as a level component moves to cloud, those IINS will have to be supported in the cloud as well.

### 5.2. Interfaces

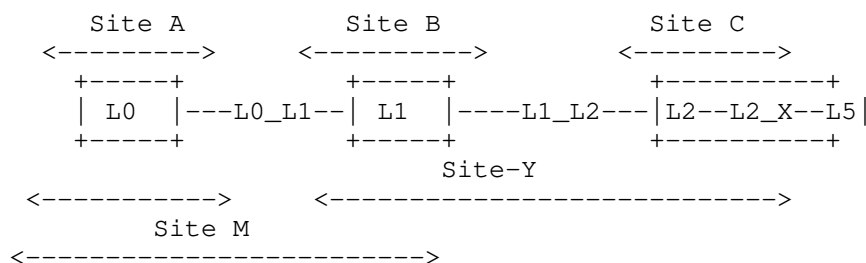


Figure 3: Interfaces dependent on the levels

Figure 3 above depicts that in IIN framework, boundaries between the interfaces should not be crossed. Moreover, equipment or functions from different levels may be placed at different sites, but in this framework direct communication from higher levels to devices is not permitted.

- \* L0\_L1 interface decides the communication channel between the process and basic control levels even when there may be a number network devices. These network devices are typically IIoT gateways that perform protocol translations (such as Modbus to Profibus).
- \* L1\_L2 interface serves as communication between supervisory control devices and PLCs.
- \* L2\_X interface is very likely IP interface for levels beyond L2, not sure if need to define an interface. it will be used for IT enterprise applications. however, it will still need to participate in functional requirements of data security and operational safety (meeting latency, resiliency targets).

Note: later add network device details in between.

Each interface has at least three attributes associated - whether a particular request is authorized, the service level guarantees (latency, data rate, frequency, etc), security profile.

In Figure 3, a level based hierarchical co-location is shown to be preserved.

- \* L0 is site A, L1 is site B and above L2 in site C.
- \* L0 is site A, L1 above in Site Y.
- \* L0, L1 in site M and above L2 in site C.

### 5.3. IIN Device Functions

These functions apply to end nodes as well as network nodes or other gateways in the network.

The topologies in the manufacturing zones do not change very frequently and devices are also designed for long-term use with minimal time between the failures. Such design considerations may be used to simplify network operations and configurations.

Assuming this is a layer 3 network architecture, there should be an assignment and association between the network address and end devices' physical addresses. Note that legacy devices are either on serial bus or their information is carried over Ethernet media.

Further motivation and analysis for adapting to OT/IT asymmetric address formats is covered in [I-D.draft-km-industrial-internet-requirements].

Additionally, adapting these devices to network layer requires support for the following mechanisms:

#### 5.3.1. Device Specific functions

- \* discovery and on-boarding
- \* Device identification and authentication
- \* Device addresses and their assignment and management

#### 5.3.2. Transmission (Transport) Mechanisms

Currently, L0 and L1 devices do not use any transport protocol. The data is embedded after control header. With a network layer solution, TCP maybe too heavy for field-bus devices. Some other means of assuring device delivery will be needed.

#### 5.3.3. Routing considerations to provide safety & security

Routing protocols will be necessary as the scale of the devices grow at the same time it should be kept simple. Possibly, Interior Gateway Protocol (IGP) will be deployed. Here it may be useful to provide guidelines on IGP features that provide distribution of routes (for different devices), path information.

#### 5.3.4. Traffic Profiles for different type of data

Differentiating traffic and assigning priorities is required so that important data is not dropped. This is in addition to use of Detnet for time-sensitive services.

Different type of data can include - process data (high priority), monitoring data (low priority), fault, alarms, signals data (high), health-check sensors data (medium), etc.

Todo: Also discuss Detnet [DETNET] here.

#### 6. IANA Considerations

This document requires no actions from IANA.

#### 7. Security Considerations

This document introduces no new security issues.

#### 8. Acknowledgements

#### 9. Informative References

- [DETNET] Finn, N., Thubert, P., Varga, B., and J. Farkas, "Deterministic Networking Architecture", RFC 8655, DOI 10.17487/RFC8655, October 2019, <<https://www.rfc-editor.org/info/rfc8655>>.
- [I-D.draft-km-industrial-internet-requirements] Makhijani, K. and L. Dong, "Requirements and Scenarios for Industry Internet Addressing", Work in Progress, Internet-Draft, draft-km-industrial-internet-requirements-00, 10 June 2021, <<https://www.ietf.org/archive/id/draft-km-industrial-internet-requirements-00.txt>>.
- [I-D.draft-zhou-nmrg-digitaltwin-network-concepts] Zhou, C., Yang, H., Duan, X., Lopez, D., Pastor, A., Wu, Q., Boucadair, M., and C. Jacquenet, "Digital Twin Network: Concepts and Reference Architecture", Work in Progress, Internet-Draft, draft-zhou-nmrg-digitaltwin-network-concepts-05, 25 October 2021, <<https://www.ietf.org/archive/id/draft-zhou-nmrg-digitaltwin-network-concepts-05.txt>>.
- [IIC] "Industry IoT Consortium", n.d., <<https://www.iiconsortium.org>>.

- [IIC\_TALK] William Diab, W., "Overview of IIC Building the IIoT Ecosystem", 12 October 2021, <[https://github.com/iiot-dir/Meetings/blob/main/20211012/slides/Diab\\_IIC\\_Overview\\_for\\_IETF\\_1021\\_rev2.pdf](https://github.com/iiot-dir/Meetings/blob/main/20211012/slides/Diab_IIC_Overview_for_IETF_1021_rev2.pdf)>.
- [ISA95] "ANSI/ISA-95.00.01-2010 (IEC 62264-1 Mod) Enterprise-Control System Integration - Part 1: Models and Terminology", n.d., <<https://www.isa.org/standards-and-publications/isa-standards/isa-standards-committees/isa95>>.
- [LDN] Carpenter, B. and B. Liu, "Limited Domains and Internet Protocols", RFC 8799, DOI 10.17487/RFC8799, July 2020, <<https://www.rfc-editor.org/info/rfc8799>>.
- [OPC] "Open Platform Communications", n.d., <<https://opcfoundation.org>>.
- [OPC\_INFO] "OPC-UA Information Model Specifications", n.d., <<https://opcfoundation.org/developer-tools/specifications-opc-ua-information-models>>.
- [SURV] Galloway, B. and G. Hancke, "Introduction to Industrial Control Networks", IEEE Communications Surveys & Tutorials Vol. 15, pp. 860-880, DOI 10.1109/surv.2012.071812.00124, 2013, <<https://doi.org/10.1109/surv.2012.071812.00124>>.

#### Authors' Addresses

Kiran Makhijani  
Futurewei  
Santa Clara, CA 95050,  
United States of America  
  
Email: [kiran.ietf@gmail.com](mailto:kiran.ietf@gmail.com)

Lijun Dong  
Futurewei  
Santa Clara, CA 95050,  
United States of America  
  
Email: [lijun.dong@futurewei.com](mailto:lijun.dong@futurewei.com)