

Automatika

Journal for Control, Measurement, Electronics, Computing and Communications



ISSN: 0005-1144 (Print) 1848-3380 (Online) Journal homepage: <https://www.tandfonline.com/loi/taut20>

Seamless connectivity architecture and methods for IoT and wearable devices

Luka Celic & Ratko Magjarevic

To cite this article: Luka Celic & Ratko Magjarevic (2020) Seamless connectivity architecture and methods for IoT and wearable devices, *Automatika*, 61:1, 21-34, DOI: [10.1080/00051144.2019.1660036](https://doi.org/10.1080/00051144.2019.1660036)

To link to this article: <https://doi.org/10.1080/00051144.2019.1660036>



© 2019 The Author(s). Published by Informa UK Limited, trading as Taylor & Francis Group



Published online: 07 Nov 2019.



Submit your article to this journal [↗](#)



Article views: 1698



View related articles [↗](#)




View Crossmark data [↗](#)



Citing articles: 1 View citing articles [↗](#)



Seamless connectivity architecture and methods for IoT and wearable devices

Luka Celic  and Ratko Magjarevic

Faculty of Electrical Engineering and Computing, University of Zagreb, Zagreb, Croatia

ABSTRACT

Wearable and Internet of Things (IoT) devices have the potential to improve lifestyle, personalize receiving treatments or introduce assisted living for elderly people. However, service delivery depends on maintaining and troubleshooting device connectivity to smartphones, where user engagement and technology proficiency represent a possible barrier that prevents a wider adoption, especially in the elderly and disabled population. Low-cost and low-power wearable and IoT devices face challenges when operating out of range of known home networks or paired devices. We propose an architecture and methods to provide seamless connectivity (Se-Co) between devices and wireless networks while maintaining low-power, low-cost and standards compatibility. Through Se-Co, the devices connect without user interaction both in home and in unknown roaming networks while maintaining anonymity, privacy and security. Roaming networks approve data limited connectivity to unknown devices that are able to provide a valid anonymized certificate of compliance and no harm through a home provider. Se-Co enables shifting data processing, such as pattern processing using artificial intelligence, from a wearable device or smartphone towards the cloud. The proposed Se-Co architecture could provide solutions to increase usability of wearable devices and improve their wider adoption, while keeping low the costs of devices, development and services.

ARTICLE HISTORY

Received 3 July 2019
Accepted 17 August 2019

KEYWORDS

Seamless connectivity;
Bluetooth LE; privacy;
security; anonymity; IoT;
MQTT optimization; cloud;
GLOMONET

1. Introduction

Wearable and IoT devices deliver an increasing number of benefits to their users, yet there remains a number of barriers preventing their wider adoption [1–6]. In a typical user's wearable-smartphone scenario, the user is required to manage several actions: (i) pairing and establishing connectivity between two devices, (ii) ensuring connectivity of the smartphone to the Internet (mobile plan or credit), and (iii) managing charging level of both devices. Failure of any of those three actions may cause service failure as a whole and all its linked services. Successful use of wearable devices presumes the user has a certain level of technical knowledge and dexterity to interact with wearable devices and smartphones for establishing, maintaining and troubleshooting their connectivity. Although a younger healthy population may have such skills, the latter may pose a significant barrier for the elderly, children, and populations with disabilities or insufficient technical skills. Moreover, service failure can require troubleshooting the problem remotely and/or sending a technician onsite, both resulting in increased service costs. Therefore, ensuring seamless connectivity and management without user interaction are potential prerequisites for lowering user adoption barriers and service provision operational costs. The adoption of a human-centered design approach can

facilitate in maintaining high utility value due to the interdisciplinary nature of problems and at the same time help reduce adoption barriers and certain inconveniences [7]. Products without user interfaces and hermetically enclosed electronics have additional useful features such as allowing more carefree use due to a water-resistant design and longer lasting operability since there is no display to consume power. The capability of the product to self-maintaining connectivity and enrolling in the user base without user interactions would allow the building of devices without any user interface. Further improvements can be achieved by providing usability beyond simple informative data towards more actionable data [8].

Understanding the history and forces driving the evolution of IoT can help to better understand possible directions in which wearable and IoT devices, and how to make them more user centric, will evolve. A analysis carried out by Ibarra-Esquer et al. [9] on tracking the evolution of the IoT concept across different application domains identifies two trends in the description what IoT is; extension to the existing Internet and evolution of the Internet. Although definitions may appear as diverging, authors conclude that they usually encompass the same five elements: networking, services, communications, data and things. Data and things could be bonded to the node at one end of the

system, services to the data consumer at the other end and communications and networking as the underpinning link between them. Therefore, a priority should be placed on maintaining connectivity whenever possible.

Constant connectivity and increasing number of smart devices which broadcast their presence to nearby listeners have exposed users' privacy and security vulnerabilities [10,11]. Acknowledged to be one of the crucial technology factors, trust [12,13], as well as social related factors, need to be properly addressed. As users' privacy and data-trail awareness starts to raise, a balance between user/device identifiability and privacy is needed. Information which is not needed for certain processes should not be exposed.

1.1. Privacy and security

Two important stages are present when providing connectivity; device discovery and authorization to join to a network. Both stages challenge the state of maintaining anonymity and privacy while providing reasonable security.

Device discovery can be found in smart devices which broadcast their presence to nearby listeners, such as in Bluetooth Low Energy (BLE) devices.

As devices broadcasting their presence to nearby listeners have exposed users' privacy and security vulnerabilities [10,11,14], several new features and methods have been designed to overcome those recognized vulnerabilities. Device anonymity may be achieved by hiding all identifiable data from non-authorized/paired devices/services. For example, the device could expose a pseudo-random medium access control (MAC) identity (ID), allowing only authorized/paired devices/services to resolve the pseudo-random number to a valid device MAC/ID. Resolving a pseudo-random number into a valid device MAC/ID is carried out using a previously shared secret in the authorization or pairing stage. Bluetooth natively provides an IRK (Identity Resolution Key) [15] service where the detected pseudo-random MAC is decrypted using keys from all previously paired devices, although is suitable only for identifying a limited number of known devices offline. The scalability of this approach would be impractical, time-consuming and expensive when trying to resolve the identity for a large number of devices and searching online through the database of stored keys. The inclusion of both offline and centralized identification capability is offered by Edystone Ephemeral ID (EID) [16] which has based its solution around a combination of nonce and time state-defined encryption. Similarly to pseudo-random MAC, EID has limitations in cases where there is a need to centrally precompute cryptographic states for a large number of devices [16]. The provided solution requires 6.75 GB for storing four hours of Ephemeral IDs for 30 million devices. As per Gartner [17], 318 million wearable

devices were shipped worldwide in 2017 and 2018. The prediction for shipment in 2022 alone is 453 million wearable devices which suggests more than a billion shipped devices worldwide in the period from 2019 to 2022. The Edystone solution would require the computing of 225 GB of data every 4 h without counting a 60 d time drift. Moreover, it does not provide options to support multiple service providers and distributed identity resolving. Device power failure is another limitation in EID. Since the time variable is used as an encryption secret, it will be lost in the event of a power failure and the device will not compute a valid EID resulting in the device's inability to establish a valid connection. Another service for device discovery using Bluetooth low energy (BLE) is the Microsoft Connected Device Platform (CDP) where, in addition to the discovery service, the platform also provides a message exchange service between devices: "provides a discovery system to authenticate and verify users and devices, as well as providing a message exchange between devices" [18]. It uses the cryptographic one-way SHA-256 hash function to generate a 20 B hash from 4 B salt and device thumbprint which is sent to the centralized Web server. Similarly to EID, the high likelihood for precomputing limitations may result from the use of a one-way hash function. A CDP BLE broadcast message also contains device type byte, which in an environment of only a few CDP devices can enable active tracking of device activity. Additionally, offline use capability is a limitation in this design since it requires communication with a CDP web service to obtain information on other devices signed with the same Microsoft Account.

In the "node joining network" stage, reasonable security needs to be provided in order for a gateway to accept a connection request from the node. Additional interoperability needs to be provided when nodes want to connect outside of their home network. Granlund et al. [19] proposed the use of two mechanisms for enabling secure sensor mobility between different administrative domains. Authors have drawn parallels with EduRoam where academic institutions all over the world are interconnected using the RADIUS [20] Authentication, Authorization and Accounting (AAA) protocol in a tree-like structure. Users are identified using a Network Access Identifier (NAI) with route to the home AAA server. This method provides complete guarantee of the user joining the network, but it also exposes his identity. The concept of Global Mobility network (GLOMONET) where mutual (anonymous) authenticated and key agreement (MAKA) protocols was originally proposed by Zhu et al. [21], and followed by others [22–30]. These proposed protocols are evolving and are able to provide user anonymity although they rely on a preexisting relation between the connectivity provider and user where Temporary Identity (TID) is generated. Lee et al. [26] proposed the delivery of a smartcard and password to the user for a successful

authentication. Ruhul et al. [30] suggested a protocol requiring a user setup phase where user ID and hashed password are shared with a gateway node to create a shared secret. After a shared password is generated, it needs to be propagated to gateway nodes. Additionally, users are required to execute actions in order to connect and enter passwords. This action imposes the existence of a user interface on the node itself and would prevent connection to a new node. In [30], the gateway node knows the identity of both users and mobile user. Temporary identity is changed only by the gateway node after a successful login phase which makes tracking possible when the mobile user tries to connect. Kai et al. [22] proposed additional anonymity improvements in which a mobile node can choose when to generate a new random number to hide its temporary identity. Messages are encrypted using a foreign agent public key to prevent a denial of service attack on the home agent.

Even if anonymity is preserved in the discovery and authentication stage, normal communication of the node can be used for detection of activity, as noted by Das [14]. A similar de-anonymization fingerprint attack on Tor hidden services is described by Albert [31].

1.2. Seamless connectivity

The connectivity of a wireless sensor network (WSN) can be improved either by extending the working range of communication or by improving coverage/availability of interoperable/compliant infrastructure to which the node can connect.

Maintaining the low-power attribute of wearable and IoT devices prevents increasing the transmitted output power, therefore only sensitivity can be increased which is the case for a low-power wide-area network (LPWAN). Increasing sensitivity may arise at the expense of lowering effective communication data rate. An example can be found in sub-gigahertz LoRa [32] and Sigfox [33], ranging from a few kilometres in urban areas to several tens of kilometres in suburban areas. The upload is extremely limited. In the case of Sigfox, it is up to 12 bytes per upload and limited to 140 bytes daily which is impractical for wearable and IoT use cases.

Improving coverage/availability of interoperable/compliant infrastructure can be achieved using several approaches; using devices with multichannel capability, deploying new infrastructure or reuse of technology already present/deployed. In [34], hyper connectivity is seen as a way to ensure evolution towards distributed IoT architectures with better efficiency, scalability, end-to-end security, privacy and resilience. Pramanik et al. [35] concluded that wireless body area networks (WBAN) are autonomous and capable of finding a suitable communication network opportunistically. Jamil et al. [36] proposed a WBAN solution

to overcome connectivity limitations by using nodes capable of communicating over multiple channels and opportunistically connecting. This approach increases size and cost since there is a need to add active and passive components for multiple communication channels. Lei et al. proposed the creation of community networks [37]. In this scenario, a service provider such as a hospital is responsible for providing a service in a specific region. This approach requires the setting up of a suitable infrastructure. Examples of interoperable wireless neighbour area networks like Wi-SUN or JupiterMesh are highlighted in [34]. Rohokale et al. [38] proposed a cooperative IoT model where a mobile device would act as a gateway. Consideration of the same approach can be found in Dutta [39] where firstly leveraging smartphones as a temporary gateway used as a router, or secondly as a Bluetooth profile proxy when interacting with a Bluetooth device, are envisaged. The router option offers better flexibility while the BLE profile proxy is better suited to the power and processing constraints of the device.

1.3. Solution proposal

The aim of Se-Co is to provide lower wearable and IoT adoption boundaries by providing architecture and methods for seamless experience across a user's multiple environments present during the day as shown in Figure 1. These challenges were experienced during our previous research [40,41]. Using Se-Co ensures seamless connectivity by connecting either to home or to previously unknown roaming networks without a need for user intervention and without taking over the tasks of establishing and maintaining connection. Chain of trust guarantees that gateways share resources only with genuine devices without degrading gateway's or peripheral device's privacy. They are both secure and motivated to share a part of their Internet bandwidth with nearby devices holding anonymous certification of ethical usage and no harm for the network.

Providing seamless connectivity requires overcoming contradictory requirements:

- broadcasting device presence to initiate the connection process while preventing device profiling and maintaining of device privacy,
- connecting to unknown anonymous devices while maintaining security, and
- ensuring connectivity in home and roaming networks while maintaining communication uniformity.

The Se-Co architecture, methods and procedures support programmatically (without user intervention) establishing connectivity of IoT and wearable devices with gateways both in home (known) networks and in roaming networks (unknown private phone or

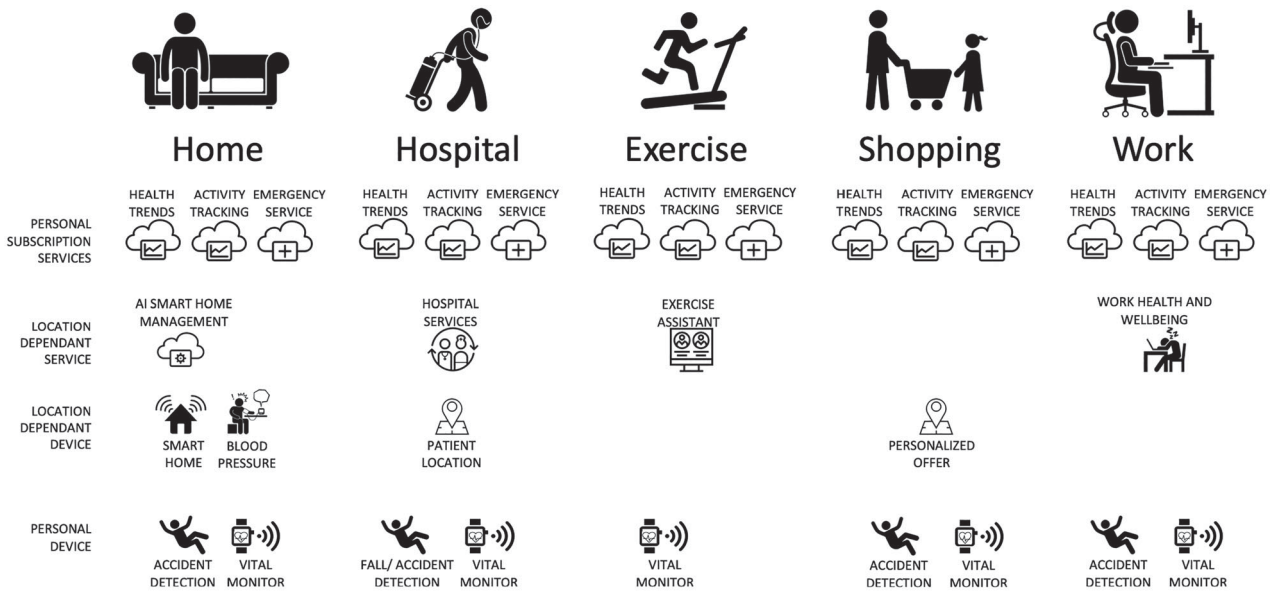


Figure 1. Services across user's daily activities.

infrastructure gateways). Se-Co methods are used to maintain the privacy and security of peripheral devices and gateways, with options to disclose a granular layer of identification and certification. Improvements to a Message Queuing Telemetry Transport (MQTT) protocol are used to provide both addressable and publishing/subscription capabilities. In this paper, we elaborate Se-Co implementation using a BLE wireless protocol, although another wireless protocol may also be used. Attributes defining Se-Co are:

- (1) seamless anonymous connectivity based on opportunistic Internet connectivity from known and unknown networks while keeping both privacy and security intact,
- (2) autonomous connectivity management without user input,
- (3) flash anonymous device discovery methods to determine if the device is a part of the same home network without a call to the home provider,
- (4) incentivize provision of Se-Co services through ethical use and no harm certification of device's hardware, firmware and application scope,
- (5) adaptation of Bluetooth LE broadcasting packets to support Se-Co methods for advertising and resolving pseudo-random ID to device ID by the home on-premises/cloud provider at the predicted scale of a billion active devices,
- (6) home and roaming network application agnostic messages routing,
- (7) optimization and reduction of the MQTT header size while maintaining support for large descriptive topics,
- (8) optimization of the MQTT header to support both topic messages and addressable messages.

2. Seamless connectivity architecture and methods

The architecture of the proposed Se-Co solution consists of: certification authorities, providers, gateways and nodes. Providers and gateways can have attributes of home or roaming. If gateways and providers are part of the same network relative to the node, they have a home attribute and if not, they have a roaming attribute. The solution architecture is shown in Figure 2.

Se-Co certification authority provides certificates to devices/nodes which are hardware, firmware and application scope compliant. The provider is a central body which can create a virtual private network (VPN) and associate gateways and nodes with it. In a provisioning stage, the home provider and nodes exchange certificates and public keys. Once the device provisioning is completed, connectivity between devices associated with the same home network can be established, with or without Internet connectivity. Connection between the node and the gateway is established autonomously without user actions when the node is a part of the same VPN as a gateway or when a roaming gateway receives certification from the home gateway that the node is Se-Co certified. Certification is given upon successful pseudo-random identity resolution which the anonymous node broadcasts. The cloud providers are able to resolve device pseudo-random identity efficiently "on the fly" and cost-efficiently for any large number of associated devices. In a home network, all devices are interconnected and capable of exchanging data across that VPN using all available bandwidth.

When a node is out of reach of the home network, a connection to a roaming network can be achieved only if the roaming provider has Internet connectivity to the node's home provider. This is aligned with

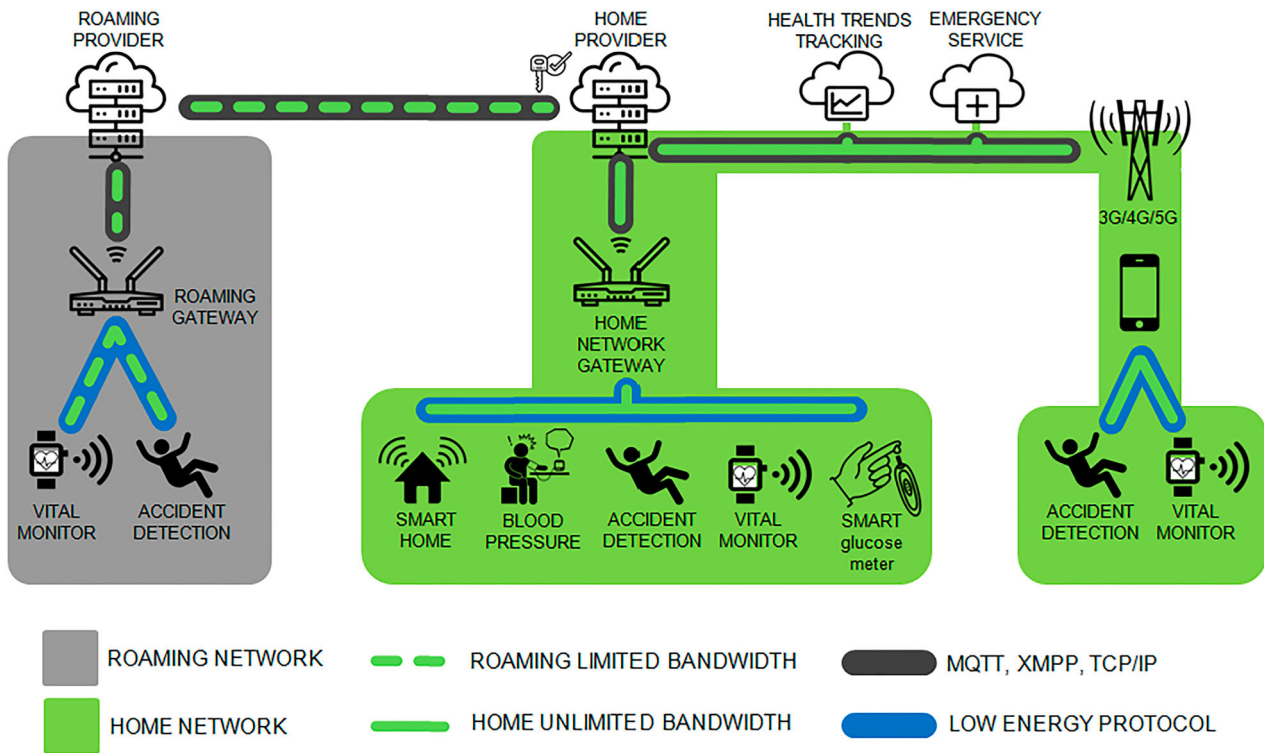


Figure 2. Solution architecture.

the scope of the node connectivity aim through roaming network communication with the home network. In the roaming network, all traffic coming from roaming providers outside of the VPN is forwarded to the home provider. Through roaming provider, the devices have the ability to send to, and receive from, the home network provider bandwidth-limited encrypted packets. The home provider is responsible for decrypting and ingesting packets into the home network and also to encrypt packets from the home network being sent to the devices currently in a roaming network. Roaming network gateways provide a bandwidth-limited access (at their discretion). Gateways connected to broadband Internet and having constant power supply may be willing to provide higher bandwidth to a larger number of devices. In contrast, a smartphone gateway has a limited bandwidth and a limited energy supply with the aim of preventing degradation of usable smartphone time of use. Therefore, the smartphone acting as a gateway is willing to provide access to only a few devices providing very limited bandwidth.

2.1. Se-Co chain of trust and privacy

Chain of trust is the basis for the GLOBONET concept and MAKa protocol. Proposals from [21–30] provide device identity confirmation through a home agent. This identity does not provide device scope, therefore, identity of a device which is a BLE sniffer and profiler can be validated. Adding a specific scope attribute to the certification could enable device profiling. As an example, where 20 devices are near a gateway, adding a scope

attribute would potentially isolate single nodes by their specific scope and enable device tracing and profiling.

Se-Co compliant devices do not disclose their scope to the roaming gateway/provider, but provide certification that the device does not pose a threat to the roaming network. Both the device and firmware are certified. If the device is programmable or customizable, certification will be extended to prevent post-sale harmful modification. Chain of trust across different device stages is shown in Figure 3. Communication between providers uses standard WEB secure channels and X.509 certificates.

2.2. User privacy and device identifiability

The developed architecture supports two identification methods based on modern cryptography functions. The node broadcasts a pseudo-random advertisement to nearby listeners which carry out the following identity resolution methods:

- resolving an advertised pseudo-random ID to a device ID efficiently and “on the fly” for any number of devices using public-key cryptography,
- high probability determination of whether the observed peripheral device is a part of the same home network to support fast connection regardless of online or offline status.

The solution maintains device privacy and anonymity against nearby listening devices, gateways or providers which are not a part of the same home

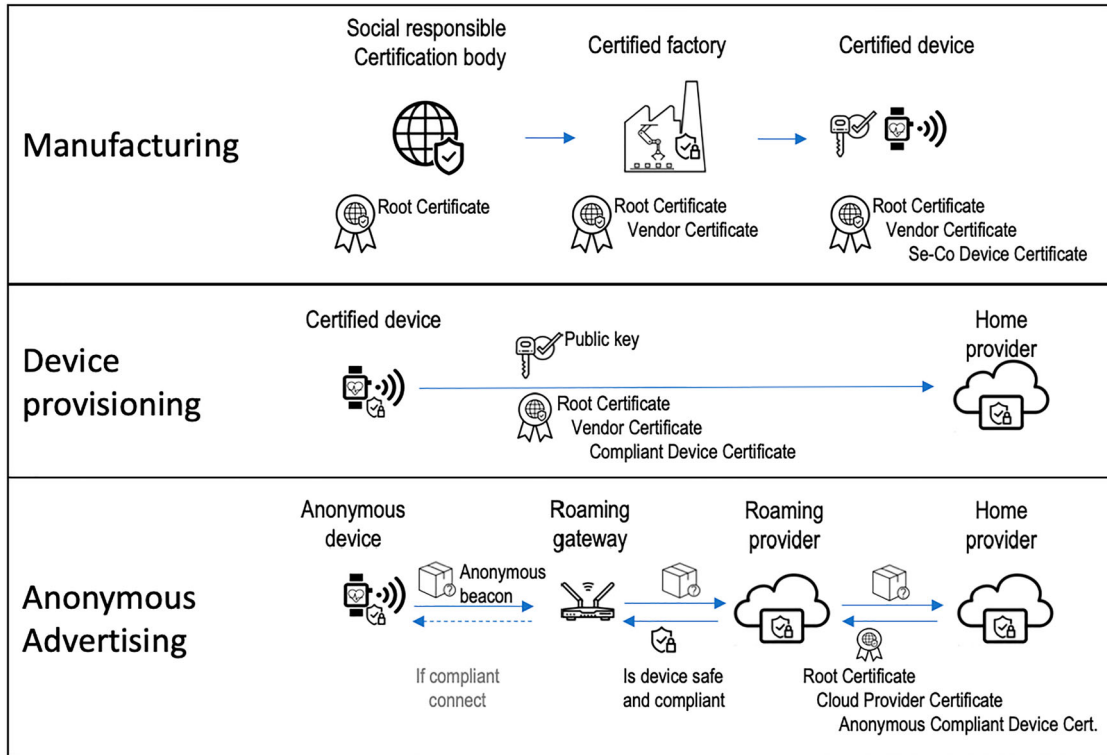


Figure 3. Chain of trust across different device stages.

network by frequently generating new pseudo-random IDs. At the same time generation of new pseudo-random IDs does not impact on the method to identify devices which are a part of the same network or cloud providers. Disabling of reverse IP address tracking and profiling of the gateway by the node is achieved by hiding the gateway’s address behind the cloud provider. All traffic between two different networks is routed and exchanged centrally between the two cloud providers. To an external observer, the cloud provider is a single visible address/entity entry point for multiple associated networks. A node trying to profile and track the gateway’s physical location and IP address will always receive a response from a single cloud provider when connecting/connected to different roaming networks, thus preventing effective profiling.

2.2.1. Resolving pseudo-random advertisement into ID at scale

Se-Co provides improvements from solutions presented in section 1.1 which have either scalability or offline constraints. Se-Co provides a pseudo-random architecture and methods which ensure device privacy and anonymity while retaining efficient “on the fly” decoding of a device’s pseudo-random ID using an integrated cryptography model: Elliptic Curve Diffie-Hellman key exchange, Advanced Encryption Standard (AES) symmetric encryption and one way hash cryptographic functions. Cryptography used in BLE 4.2 relies on ECC and AES with 256 and 128 bit key sizes, respectively [42]. Security reports [43,44] estimate that

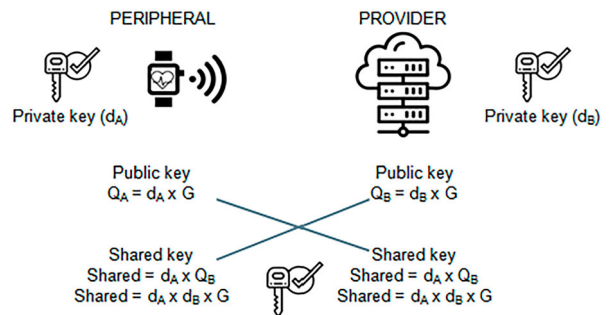


Figure 4. Elliptic curve Diffie-Hellman key exchange.

the ECC with a 256 bit key size is secure to use for another few decades, along with projections of a RSA key becoming impractically large and consuming more power [45].

In order to resolve pseudo-random identity, we decided to use the public–private key pair method. Since an AES key is derived from a shared secret between the provider and the peripheral devices using Elliptic Curve Diffie-Hellman key exchange (Figure 4), only the provider can decode the device’s ID using its private key. The same principle is used in Transport Layer Security (TLS) and sequentially in Hypertext Transport Protocol Secure (HTTPS), both used today worldwide. Although using AES 256 and ECC 512 bit keys would provide longer lifespan of the security, we decided to use 256 bit ECC key size because of the payload limitation in broadcasting packets. The public compressed key for 256 bit ECC is a 257 bit key which

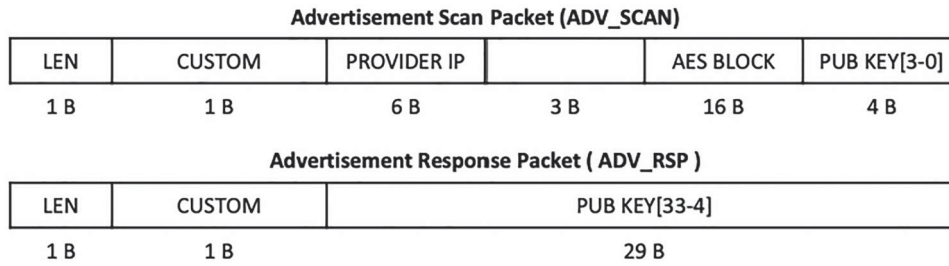


Figure 5. Advertising and request response packets.

may be divided between two broadcast packets. Larger ECC keys would not be possible to broadcast with BLE specification 4.2. The major future adoption of devices with BLE revision 5 will allow the use of ECC with a 512 bit key size.

In the device provisioning stage, peripheral devices store the provider's public key and IP address. For every session, the peripheral device generates a random public/private key pair. Using the provider's public key, the device computes a shared key which is used to derive the symmetric AES key. The AES symmetric key is used to encrypt the device's ID into a 16 B block. By broadcasting a random peripheral device's public key and AES block, the provider and only him, is able to decrypt the AES block and access the device ID. This approach allows using standard server-side public-key cryptography found in TLS to retrieve the device ID. Due to use of public-key cryptography, problem space is reduced from:

$$\text{Total computations} = N_{\text{DEVICE NUMBER}} * (X_{\text{WINDOW SIZE}} + Y_{\text{TIME ERROR}})$$

for EID example, down to

$$\text{Total computations} = 1 * \text{Packet decryption}$$

eliminating long running and expensive (pre) computation, making it viable for resolving requests for any number of devices and providing support for billions of predicted active devices.

BLE 4.2 advertisement packet limits user defined bytes to a size of 29 B which is not sufficient to transmit a compressed ECC public key (33 B) and AES block (16 B). To overcome this limitation, an ECC public key is split between a BLE scan and response packet, as shown in Figure 5.

A Table 1 compares properties of different identification methods used with low power devices in terms of: offline address resolution, online address resolution, scaling impact and multi provider support. Current

methods in use fail in at least one category and this was the initial motivation to development Se-Co.

2.2.2. Determining peripheral devices belonging to a home network

In a worst case scenario, the roaming networks may provide only a restricted bandwidth connectivity service. Therefore, in terms of power consumption and communication channel congestion, it is crucial to efficiently detect the probability that the observed peripheral device and the gateway are a part of the same network. This detection is achieved using a highly efficient method capable of resolving in real time and in congested areas where thousands of peripherals advertise their presence.

In section 1.1 (Security and Privacy), Microsoft's CDP service approach was outlined. The service uses a one-way hash function which meets the requirements for privacy and network identification. The Se-Co architecture and methods use the same one-way model, where hash is generated from nonce (advertised payload) and home network key. Our design challenge was to find space for the hash result since the advertisement packet payload is already full as it contains the peripheral device's public key and AES block. Since the output of the hash is pseudo-random, it is suitable for use as a replacement for the dummy advertised device random access address. This approach provides the same device tracking protection but with an added functionality to detect the device belonging to a home network. For that purpose, the 32 B result of the hash function will be trimmed to 9 B of which 6 B is used as a random address and the remaining 3 B in the advertisement packet. Final assembly of the advertisement packet is shown in Figure 6.

As the nonce and hash result is available in the advertisement packet, the proposed method saves the peripheral's power and prevents communication channel congestion since the gateway can act as a passive

Table 1. Comparison of different identification method used in low power devices.

	Offline resolution	Online resolution	Scaling impact	Multi provider
Bluetooth IRK	Supported	Not supported	Resource intensive	Not supported
EID	Supported	Supported	Resource intensive	Not supported
Microsoft CDP	Not supported	Supported	Unknown	Not supported
Se-Co	Supported	Supported	No impact	Supported

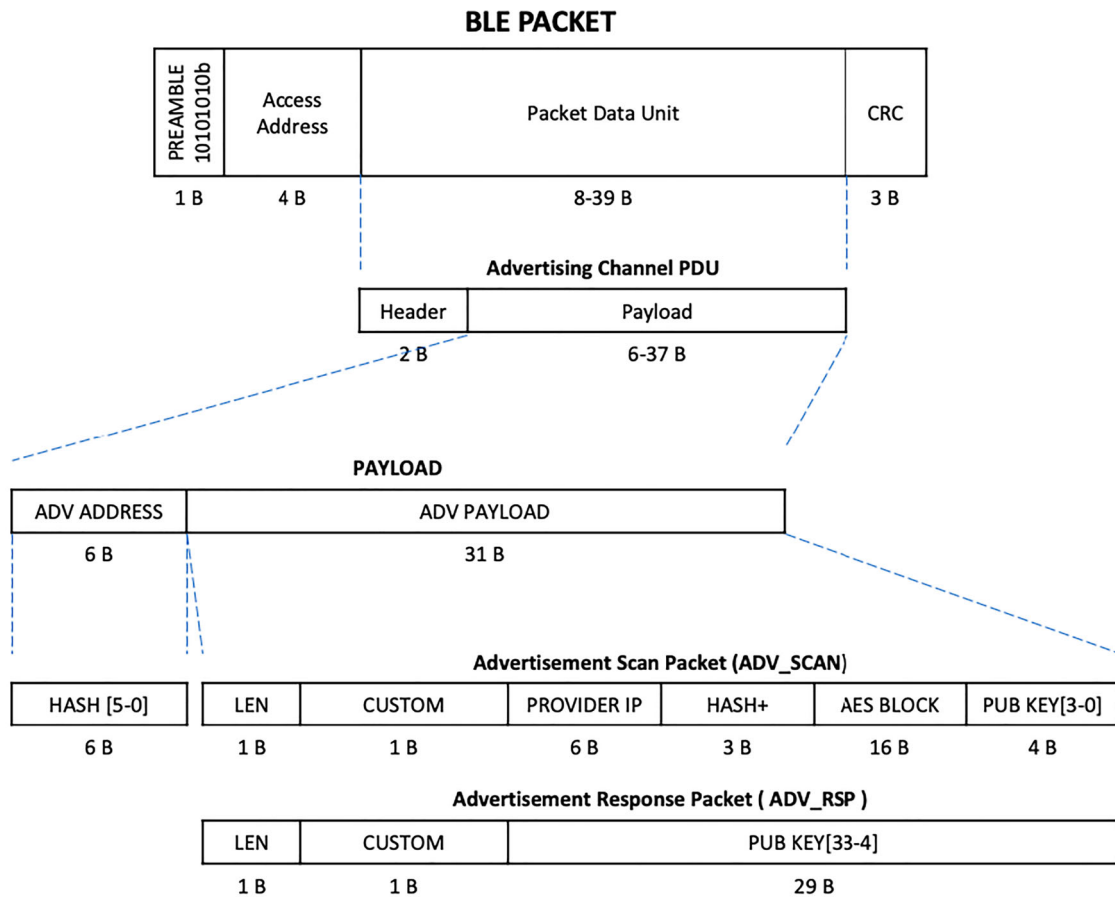


Figure 6. Complete Bluetooth LE packet including advertising packet with address.

observer and does not need to actively ping peripheral devices for response packet information.

2.3. Connection establishment and certifications

As noted in the Introduction, the goal of this solution and methods is to provide the required uninterrupted connectivity service to peripheral devices, both in home and roaming network environments. The designed solution provides power efficient and anonymous methods for establishing a connection between any two anonymous devices. Power efficiency is achieved by minimizing events with data exchange and by pushing computation to devices with higher energy availability. Minimizing data exchange events is achieved by using cryptography models. This connection process is shown in Figure 7.

The connection establishment process was designed to remove delays, allow caching and preserve the peripheral device's power, the latter of which is achieved by pushing power extensive pre-computation towards the gateway and providers.

2.3.1. Connection establishment – roaming

The connection process starts with the gateway (home/roaming) receiving the peripheral device's non-connectable advertisement. As described in 2.2.1 and

2.2.2, from the initial advertisement packet, the gateway can determine:

- whether the observed peripheral device is a part of a home network (either real-time or offline), and
- which is the provider's IP address.

After determining the provider's trustworthiness, certificate or confirmation of whitelisted status, the gateway sends a scan request to the peripheral device (a scan request is interpreted by the peripheral device as a connectivity offer and it adds the offer to a list for subsequently making a choice on connection).

Upon receiving the scan response, the gateway forwards the received packets to its provider. The gateway's provider makes a request to the device's provider requesting a connection token/packet, which is further used when the connection with the peripheral device is established. The response is then returned back to the gateway's provider and if the preset policy is met, it forwards a positive reply and connection token/packet to the gateway. We chose that method to maintain the gateway's anonymity and privacy by hiding the gateway's local IP or other traceable information behind the gateway's provider.

Regarding the peripheral device's decision to connect with the selected gateway, the device will start to broadcast a connectable advertisement with the

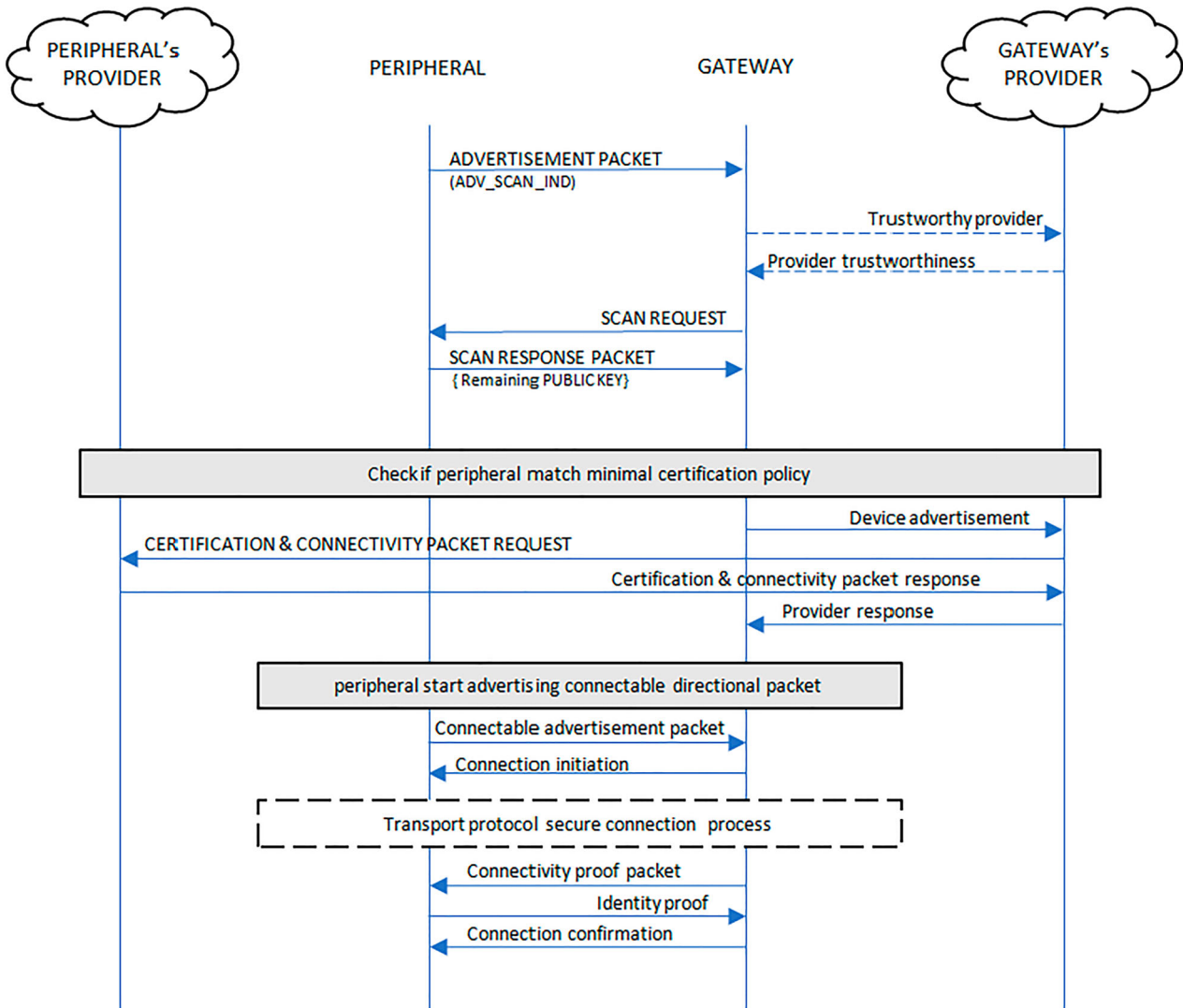


Figure 7. Connection process using Bluetooth LE 4-transport layer.

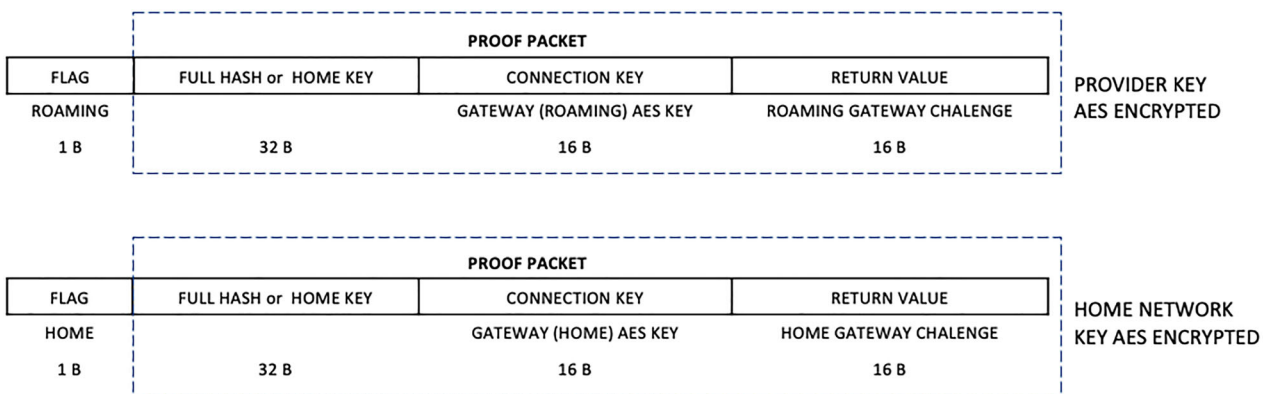


Figure 8. Connection establishment packet.

selected gateway’s address (ADV_DIRECT_IND). If the security policy of the peripheral device matches the predefined policy, the gateway will respond with a connection request and the Bluetooth LE connection process will start, thus establishing the transport layer. In the response from the peripheral device’s provider, data to instruct the gateway to connect using a “Just

Works” or OOB (Out Of Bound) method with provided passcode are included.

Upon establishing the Bluetooth LE transport layer, the gateway will forward an Internet connectivity proof packet to the peripheral device. The peripheral device replies with an identity proof packet to which the gateway replies with an acknowledgement.

2.3.2. Internet connectivity and identity proof

Since the peripheral device seeks connection to a roaming gateway to establish Internet connectivity, it needs to be able to determine whether that roaming gateway is a genuine provider. This is achieved by sending a connectivity proof packet upon establishing a connection on the transport layer and with periodical pings as shown in Figure 8. The connectivity proof was designed to be consistent for both connection scenarios to minimize code footprint:

- connecting to a roaming network, and
- connecting to a home network (offline capable).

In the roaming scenario, Internet connectivity and access to the peripheral device's provider is verified. The proof packet is encrypted using an AES key derived from a shared secret between the peripheral device and its provider. Since a valid packet can be generated only by the provider, providing a valid packet with a full calculated hash is sufficient proof to a peripheral device that the gateway has access to the peripheral device's provider. Since the public key is randomly generated per session, false gateway reply attacks are not possible outside the current key pair session.

In the second scenario, connectivity to a valid home network is verified. Since connectivity between the peripheral device and the gateway needs to support the capability to connect between, for example, a user's smartwatch and smartphone in an offline environment, the home network AES key is used for packet encryption.

In both scenarios, master keys are used only once to limit the exposure of static keys and to prevent attacks. The proof packet contains the AES key to be used in all subsequent communication.

The peripheral device proves its identity to the gateway by replying with a packet containing the previously sent gateway's challenge encrypted with the gateway provided AES key. False peripheral reply attacks are prevented since the gateway is using a new random key in each proof packet sent.

2.3.3. Anonymous chain of trust and ID certifications

Since Se-Co aims to provide connectivity access to genuine peripherals and non-harmful devices while devices want to protect their anonymity, there may be a need to efficiently establish a chain of trust between anonymous devices. Three levels of identification are designed to offer balance between full anonymous certification and use case where domain or ID need to be exposed:

- anonymous – Se-Co/ethical compliant consumer device (W/o category certification),
- domain certification and

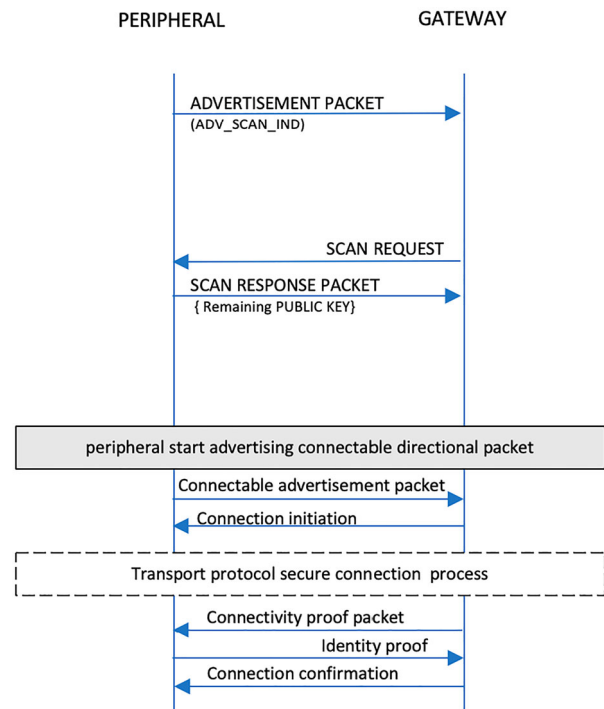


Figure 9. Fast offline connection process.

- ID certification.

A cloud provider, depending on manufacturer's certification, will issue the certificate to a roaming network provider proving that the device, as observed by the roaming gateway, is not harmful and can be offered connectivity.

Combination of Internet connectivity proof and the device anonymous certification provides enough information for roaming and for the peripheral device's cloud provider to programmatically decide, based on previously set rules, whether they want to exchange connection information, thereby allowing connection between the gateway and peripheral.

2.3.4. Fast offline home network connection

An important solution design feature is the supporting of fast offline connection capability, currently found in examples of connecting smartwatches to smartphones, or IoT sensors to local networks (Figure 9). Upon receiving an advertisement packet from the peripheral device, the gateway can determine whether there is a high probability that two devices belong to the same home network. If that is the case, the gateway can skip all calls to the device provider, offer connectivity and try to connect using the home key. If the connection attempt is unsuccessful, the gateway may repeat the process using the roaming connection process.

2.3.5. Switching to a home network in a multi-network environment

A particularly interesting scenario happens when a peripheral device is within range of multiple gateways

and randomly chooses a roaming gateway. Since a peripheral device is broadcasting only its presence and not listening to the radio in order to conserve power, it cannot detect whether there is a home network in range. To overcome that obstacle, Se-Co uses providers as proxies.

After the home gateway receives an advertisement packet where the hash result matches the gateway's computation using the home network key, it sends a message to the provider to request the peripheral device to disconnect from the current roaming gateway, compute a new random session key (and address) and reconnect to a specific address of the home network gateway. Since the peripheral device has a new pseudo-random address, the privacy is protected from nearby listening devices.

2.3.6. Easy key revocation and access management

Since the proposed solution provides connectivity to anonymous certified devices, the provider can single-sidedly revoke a home network key. That simplifies key/access management/distribution. As an example, when there is a need to revoke access to devices which previously were a part of the home network, the provider can invalidate the current home network key and trigger reissuing of new keys to all remaining devices in the network. Roaming will be approved by the provider since the provider has insight into which devices are a part of the same network.

3. Wearable/IoT optimized messaging protocol – MQTT header optimization

In recent years, the MQTT protocol has grown through adoption in the IoT community and has started to be used as a backbone for cloud services such as Amazon Web Services AppSync notifications due to its simplicity, versatility and human readable topics. Due to wide support from different cloud providers and platforms, it has been chosen as the messaging protocol for the presented solution.

Since the overhead of the header and the topic can easily be several times larger than the useful payload, research on header optimization was focused in two directions: compatibility with existing protocols and maximal optimization. Optimization is crucial to the link between the edge node and the gateway since there are constraints in available bandwidth and power. Common wearable devices and IoT nodes are repetitive in posting data of the same type. This means that certain topics will be used over and over again when data are broadcasted/published. Since topics are human readable text, which from the development and maintenance perspective is better to be longer and descriptive, their representation is not optimized. For example, in the case of the topic:

IoT “house_08f34ab/living_room/smart_sensor” and a useful payload “Temperature:22.4”

or a wearable topic:

“net_8a56bc72/user_723bf8ac/left_arm/heart_rate” and the payload “hr:67”,

the header is 8 times larger than the actual data payload.

To overcome this inefficiency and to maintain a descriptive character of the topic, first level optimization with replacement of text sections was tested. After the connection was established, the device sent a packet (type “publish”) with the text to be replaced between two wildcards.

```
MESSAGE TYPE 0 × 30 (PUBLISH, topic “optimisation/”)
```

```
DATA: 0 × 81, “house_08f34ab/living_room/smart_sensor”, 0 × 81
```

```
MESSAGE TYPE 0 × 30 (PUBLISH, Topic: 0 × 81)
```

```
DATA [ 16 Byte ]: “Temperature:22.4”
```

Wildcards are characters with a starting value of 0×81 and, for the example above, the topic may be replaced with a single character 0×81 . In the development stage, the developer can determine which sections of text are repetitive and notify this to the MQTT gateway. The node can concatenate a list of text replacements with wildcards in the optimization packet and the receiver node, based on storage capacity, will confirm which wildcards are accepted. Whenever a packet is received and a wildcard is present in the topic, the wildcard will be replaced by a full text hence maintaining standard message processing.

Deeper second level optimization strips out completely the topic content from the header, thus removing the current requirement of minimal 3 B (2 B length + topic “/”) which is achieved by introducing the $0 \times 0A$ (new line) character as a delimiter between the topic and the payload. In order to allow further optimization and combining of wildcards between topics and payloads, the 0×03 (end of text) character is placed at the end of the text. To prevent packet misinterpretation, a new publish message type 0×00 is selected to be introduced for the second level optimized publish packet. For the example above, we can achieve overhead of a single byte and reduce total data (topic + payload) length to 5 B from 56 B.

```
MESSAGE TYPE 0 × 30 (PUBLISH, topic “optimisation/”)
```

```
DATA [ Byte ]: 0 × 81 + “house_08f34ab/living room/smart_sensor” + 0 × 0A “Temperature:” + 0 × 81
```

```
MESSAGE TYPE 0 × 00 (PUBLISH)
```

```
DATA [ 5 Byte ]: 0 × 81 + “22.4”
```

An overview of packet content difference for different levels of optimization is illustrated in Figure 10. The proposed optimization of the MQTT variable header

results in a protocol efficiency found in strict byte-oriented protocols like BLE profiles while maintaining complete descriptiveness, packet processing and human readability of MQTT. The provided example resulted in a reduction of overall packet size by more than six times. Improved efficiency directly reflects on either extending battery life or increasing the quantity of application data which is possible to be sent through a communication channel.

4. Results and validation

Although general Se-Co paradigm is applicable to range of protocols like BLE, Wi-Fi, ZigBee, Thread etc., validation using BLE wireless protocol was tested. Validation of Se-Co architecture and methods started with validation of individual sub components. In the BLE Se-Co implementation shown on Figure 2, it is crucial to validate wireless low power layer as is the layer with the biggest number of constrains. Expressify ESP32-based boards were chosen to simulate smart device. Gateway was simulated by both ESP32 based board and application running on Android phone. Two platforms were chosen as they are inexpensive and available featuring large community support suitable for students and researchers should they want to validate results themselves. Available Arduino libraries were used to perform ECDH key exchange, compute hash, perform AES encryption/decryption and setup required BLE and Wi-Fi functionality.

Connection activities from Figures 7 and 9 were successfully tested with implementing custom payload and address within boundaries of BLE, as per Se-Co specification. Behaviour of underpinning key methods were validate to be equal to the theoretical described; generating of the pseudorandom ID, resolving of pseudorandom ID using public-private model and determining if a observed device is part of same home network. Cryptographic SHA-256 hash calculation required on average 153 μ s to execute. Elliptic curve calculation, required for ECHD where executed on average in 36 ms. Achieved performance allowed smart device to efficiently compute and change it's advertisement pseudorandom ID signature and perform required cryptographic functions during connection establishment. Performance ensured gateway's ability to determine in μ s if observed devices are part of same home network. Empirical test were conducted to determine impact of trimming hash function digest from 32 bytes to 9 bytes. Particular attention was given to determine false positive occurrence where lower trimmed 9 bytes are equal to computed hash with different upper 23 bytes. In the empirical test computing 4 millions hashes there were no false positive and no true positive occurrence. This is in line with expectations as 9 bytes provide still large combination universe.

Positive validation of ability to create Se-Co gateways on existing consumer devices like smartphones was confirmed. Although peripheral's advertisement packet payload content is completely customized, it is still within BLE standard and therefore visible to BLE compliant devices. Both Android application and ESP32 based gateway connected to Node.js servers acting as home or roaming provider. Home provider's ability to resolve pseudorandom ID using its private key was successfully confirmed.

During testing BLE advertised device address using ESP32 supported setting up of user provided pseudorandom ID address except for the last 4 bits, therefore lower 8 bytes were used instead of 9 bytes to compare hash digest output when determining if two devices are part of same home network.

5. Conclusion

The proposed Se-Co solution defines the architecture and methods for providing anonymous seamless connectivity for wearable and IoT devices across known and unknown networks. The proposed solution provides network-agnostic routing to the application irrespective of whether the node is in a home or roaming network. Management of the connectivity is autonomous, without user input or management. Certification methods and nodes certification scope was proposed to incentivize unknown networks to provide Internet connectivity as certified devices do not pose a security threat for the network. The device discovery and certification methods developed herein retain user anonymity while supporting efficient fast offline and online functionality. Implementation optimization of the BLE broadcast beacon, which is compliant with the BLE standard capable of supporting the Se-Co connection setup process, is described. Optimization of the MQTT messages header is proposed for minimizing message size for frequently sent topics, while keeping the descriptive nature of the topic.

6. Discussion and future work

It should be noted that Se-Co aims primarily to provide opportunistic connectivity to smart devices like wearable and IoT. Seamless connectivity is primarily focused on granting connectivity and connection management across known and unknown networks while preserving both parties privacy and security. In order for a user to experience seamless connectivity, sufficient number of Se-Co gateways should be around the user. This implies that sufficient adoption rate is required. A key design feature to achieve high adoption rate was to maintain neutral impact for the connectivity donor, in form of power consumption, security, privacy, additional broadband cost or required user management.

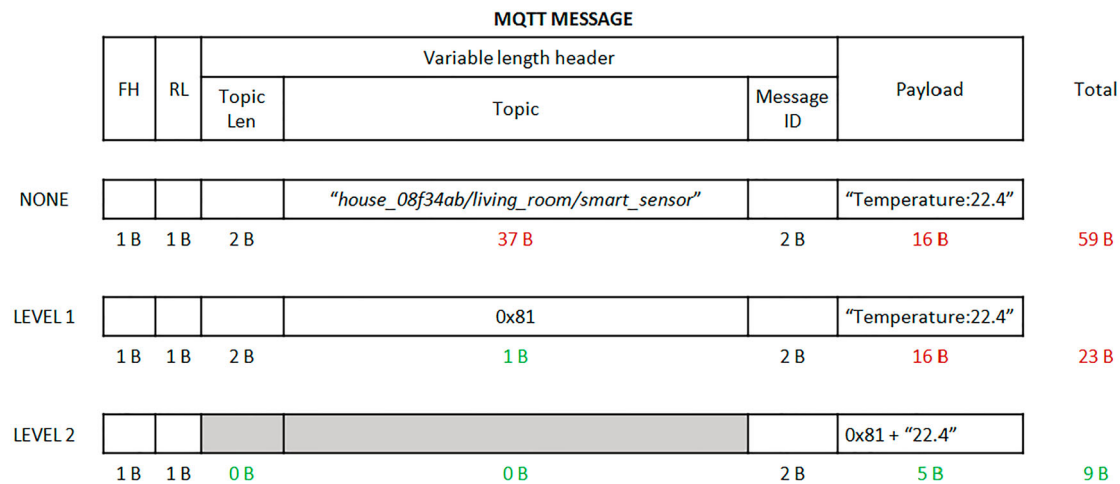


Figure 10. MQTT publish message with no optimization, level 1 and level 2 optimization.

It is not envisioned for Se-Co to guaranty connectivity and provide telemetry for life threat detection devices.

It is worth to mention that in the current solution two providers need to trust each other. Home provider is issuing to the roaming provider an anonymous certificate for a device in roaming network. Future work should be conduct to enable zero trust paradigms, where two providers do not need to trust each other. A method where the home provider is able to issue certificate to the roaming provider, which only device can confirm without disclosing any privacy data to the roaming provider would be desired.

Disclosure statement

No potential conflict of interest was reported by the authors.

ORCID

Luka Celic  <http://orcid.org/0000-0002-7556-3284>

References

- [1] Piwek L, Ellis DA, Andrews S, et al. The rise of consumer health wearables: promises and barriers. *PLoS Med.* 2016;13(2):1001953.
- [2] Mercer K, Giangregorio L, Schneider E, et al. Acceptance of Commercially available wearable activity trackers among adults aged over 50 and with chronic illness: a mixed-methods evaluation. *JMIR Mhealth Uhealth.* 2016;4(1):e7. DOI:10.2196/mhealth.4225
- [3] Salifu Y, Jeffrey S, Abdul HB. Older people, assistive technologies, and the barriers to adoption: a systematic review. *Int J Med Inform.* 2016;94:112–116.
- [4] Lee C, Coughlin JF. Older adults' adoption of technology. *J Prod Innov Manag.* 2015;32:747–759. DOI:10.1111/jpim.12176
- [5] Baig MM, GholamHosseini H, Moqem AA, et al. A systematic review of wearable patient monitoring systems – current challenges and opportunities for clinical adoption. *J Med Syst.* 2017;41:115. DOI:10.1007/s10916-017-0760-1
- [6] Peek STM, Aarts S, Wouters EJM. Can smart home technology deliver on the promise of independent living? Health care and well-being 2017, handbook of smart homes. DOI:10.1007/978-3-319-01583-5_41
- [7] The wearable revolution that has arrived ... sort of [cited 2019 April 20]. Available from: <http://designinteractive.net/6790/>
- [8] AlHogail A. Improving IoT technology adoption through improving consumer trust. *Technologies.* 2018; 6:64.
- [9] Ibarra-Esquer J, González-Navarro F, Flores-Rios B, et al. Tracking the evolution of the Internet of things concept across different application domains. *Sensors.* 2017;17(6):1379. DOI:10.3390/s17061379
- [10] Pham V, Hagen JM. Bluetooth security and threats 2015 [cited 2019 April 20]. Available from: <https://pdfs.semanticscholar.org/a41b/3c341fb6ddd16528eb2e558532258a35ea90.pdf>
- [11] Weis SA, Sarma SE, Rivest RL, et al. Security and privacy aspects of low-cost radio frequency identification systems. In: Hutter D, Müller G, Stephan W, et al. editors. *Security in pervasive computing. Lecture Notes in Computer Science, Vol. 2802.* Berlin, Heidelberg: Springer; 2004. p. 201–212.
- [12] Schall MC, Sesek RF, Cavuoto LA. Barriers to the adoption of wearable sensors in the workplace: a survey of occupational safety and health professionals. *Hum Factors.* 2018;60(3):351–362. DOI:10.1177/0018720817753907
- [13] Kalantari M. Consumers' adoption of wearable technologies: literature review, synthesis, and future research agenda. *Int J Technol Market.* 2017;12:274–307. DOI:10.1504/IJTMKT.2017.10008634
- [14] Das AK, Pathak PH, Chuah C-N, et al. Uncovering privacy leakage in BLE network traffic of wearable fitness trackers. *Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications (HotMobile).* New York, NY: ACM, 2016, pp. 99–104. DOI:10.1145/2873587.2873594
- [15] Bluetooth SIG. Specification of the Bluetooth system. Version 4.2. 2014.
- [16] Hassidim A, Yossi M, Moti Y. Ephemeral identifiers: mitigating tracking & spoofing threats to BLE beacons. 2016. [cited 2019 April 20]. Available from: <https://pdfs.semanticscholar.org/338c/de818bdeff25c4d1f4894bfc8f60805248d.pdf>
- [17] [cited 2019 April 20]. Available from: <https://www.gartner.com/en/newsroom/press-releases/2018-11-29-gartner-says-worldwide-wearable-device-sales-to-grow>

- [18] Microsoft openspec, Bluetooth: advertising Beacon [cited 2019 April 20]. Available from: https://docs.microsoft.com/en-us/openspecs/windows_protocols/ms-cdp/77b446d0-8cea-4821-ad21-fabdf4d9a569
- [19] Granlund D, Holmlund P, Åhlund C. Opportunistic mobility support for resource constrained sensor devices in smart cities. *Sensors*. 2015;15(3):5112–5135. DOI:10.3390/s150305112
- [20] Rigney C. Remote authentication dial in user service (RADIUS). Pleasanton (CA): IETF, RFC2865; 2000.
- [21] Zhu J, Ma J. A new authentication scheme with anonymity for wireless environments. *IEEE Trans Consum Electron*. 2004;50(1):231–235. DOI:10.1109/tce.2004.1277867
- [22] Chain K, Kuo W-C, Cheng J-C. A novel mobile communications authentication scheme with roaming service and user anonymity. *Appl Sci*. 2016;6:393.
- [23] Xu G, Liu J, Lu Y, et al. A novel efficient MAKKA protocol with desynchronization for anonymous roaming service in global mobility networks. *J Netw Comput Appl*. 2018;107:83–92. DOI:10.1016/j.jnca.2018.02.003
- [24] Gope P, Hwang T. An efficient mutual authentication and key agreement scheme preserving strong anonymity of the mobile user in global mobility networks. *J Netw Comput Appl*. 2016;62:1–8.
- [25] Kai C, Kuo WC, Cheng JC. A novel mobile communications authentication scheme with roaming service and user anonymity. *Appl Sci*. 2016;6:393.
- [26] Lee CC, Hwang MS, Liao IE. Security enhancement on a new authentication scheme with anonymity for wireless environments. *IEEE Trans Ind Electron*. 2006;53(5):1683–1687.
- [27] Mun H, Han K, Yan SL, et al. Enhanced secure anonymous authentication scheme for roaming service in global mobility networks. *Math Comput Model*. 2012;55(1):214–222.
- [28] Yoon EJ, Yoo KY, Ha KS. A user friendly authentication scheme with anonymity for wireless communications. *Comput Electr Eng*. 2011;37(3):356–364.
- [29] Zhou T, Xu J. Provable secure authentication protocol with anonymity for roaming service in global mobility networks. *Comput Netw*. 2011;55(1):205–213.
- [30] Amin R, Islam SH, Biswas GP, et al. A robust and anonymous patient monitoring system using wireless medical sensor networks. *Future Gener Comput Syst*. 2018;80:483–495. DOI:10.1016/j.future.2016.05.032
- [31] Albert K, Mashaal A, David L, et al. Circuit fingerprinting attacks: Passive deanonymization of tor hidden services. 24th USENIX Security Symposium (USENIX Security 15). 2015: 287–302.
- [32] LoRaWAN™ 1.1 specification. Available from: https://lora-alliance.org/sites/default/files/2018-04/lorawan_specification_v1.1.pdf
- [33] Sigfox connected objects: radio specifications. Available from: <https://build.sigfox.com/sigfox-device-radio-specifications>
- [34] Vermesan O, Eisenhauer M, Serrano M, et al. Next generation internet of things - Distributed intelligence at the edge and human machine-to-machine cooperation, River Publishers Series in Communications, 2018, pp. 19–102. ISBN: 9788770220088. The next generation internet of things – hyperconnectivity and embedded intelligence at the edge.
- [35] Pramanik PKD, Nayyar A, Pareek G. WBAN: driving e-healthcare beyond telemedicine to remote health monitoring. *Telemed Technol*. 2019: 89–119. DOI:10.1016/b978-0-12-816948-3.00007-6
- [36] Jamil Y, Mehmet R. Wireless body area network (WBAN) for medical applications. *New Develop Biomed Eng*. 2010. DOI:10.5772/7598
- [37] You L, Liu C, Tong S. Community medical network (CMN): architecture and implementation. 2011 Global Mobile Congress, Shanghai, 2011, p. 1–6. DOI:10.1109/GMC.2011.6103930
- [38] V. M. Rohokale, N. R. Prasad, R. Prasad. 2011 2nd International Conference on Wireless Communication, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless VITAE). A cooperative internet of things (IoT) for rural healthcare monitoring and control.
- [39] Dutta P. The internet of things has a gateway problem. Proceedings of the 16th International Workshop on Mobile Computing Systems and Applications (HotMobile). New York (NY): ACM, 2015, p. 27–32. [Online]. Available: <http://doi.acm.org/10.1145/2699343.343.2699344>
- [40] Celić L, Varga M, Pozaić T, et al. WBAN for physical activity monitoring in health care and wellness. IFMBE Proceedings 2013, Vol. 39.
- [41] Džaja D, Varga M, Šeketa G, et al. System for assisted exercising and qualitative exercise assessment. IFMBE Proceedings 2015, Vol. 45, p. 682–686.
- [42] Padgette J, Bahr J, Batra M, et al. Guide to Bluetooth security. NIST 2017, NIST.SP.800-121r2 [cited 2019 April 20]. Available from: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-121r2.pdf>
- [43] ECRYPT II yearly report on algorithms and key sizes (2011–2012). ECRYPT 2012 [cited 2019 April 20]. Available from: <https://cordis.europa.eu/docs/projects/cnect/6/216676/080/deliverables/002-DSPA20.pdf>
- [44] Algorithms, key size and protocols report, ECRYPT 2018 [cited 2019 April 20]. Available from: <http://www.ecrypt.eu.org/csa/documents/D5.4-FinalAlgKeySizeProt.pdf>
- [45] Suárez-Albela M, Fraga-Lamas P, Fernández-Caramés TM. A practical evaluation on RSA and ECC-based cipher suites for IoT high-security energy-efficient fog and mist computing devices. *Sensors*. 2018;18:3868.