Bluetooth blog

An Intro to Bluetooth Mesh Part 2

Posted on August 01, 2017 by Martin Woolley

Chapter 2 of the Bluetooth Mesh Networking Series

Introduction

In Part 1 of this article, I introduced the new Bluetooth mesh networking technology. If you haven't read part 1, start there before reading this, the second part.

I'll complete my introductory overview of Bluetooth mesh networking here with an overview of the way messages find their way across large mesh networks, in-market device support, security and the mesh stack itself, and then we'll proceed to explore aspects of the technology in greater detail in subsequent articles.

Relaying

In Part 1, we learned that Bluetooth mesh networking devices talk to each other using messages and a publish/subscribe mechanism.

Mesh networks allow devices to be installed and to communicate with each other across a very large area. Consider how large a space a shopping mall, airport or office block occupies. With walls and other physical barriers, it may not be possible to achieve direct radio contact from a device on one side of a building, to a device installed on the far side of the same building, or in fact a device in another, adjacent building. Bluetooth mesh networking solves this problem by allowing some of the devices in the network to be designated "relays".

Relay devices retransmit messages that they receive from other devices. In doing this, they are able to communicate with devices that are not in radio range of the device which originally published the message. A message may be relayed multiple times, over what are termed "hops". A maximum of 127 hops are possible, enough to relay a message across an enormous physical area.

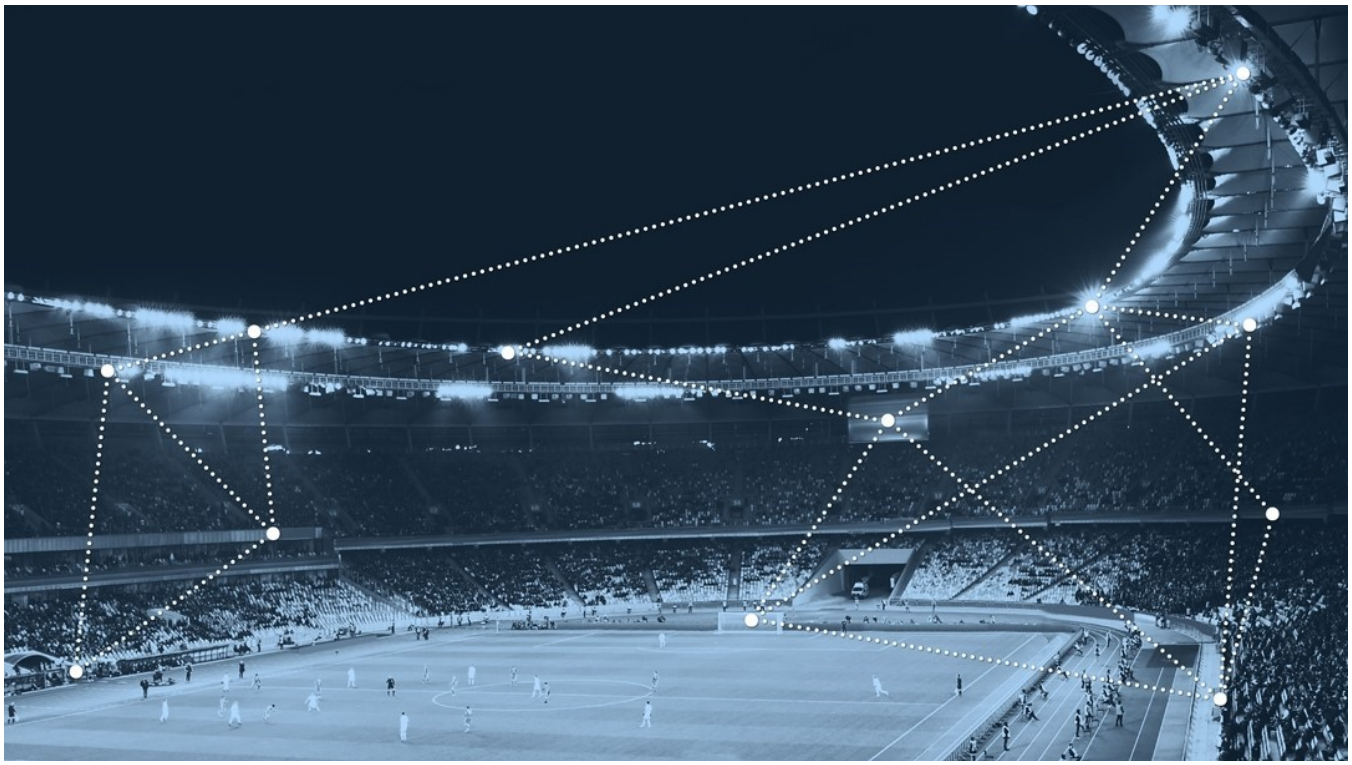

Figure 1 - Bluetooth mesh networks relay messages from node to node

Managed Flooding

Bluetooth mesh networking uses an approach known as “flooding” to publish and relay messages. This means that messages are not routed by a process which results in them being transmitted along a specific path comprising a sequence of only certain devices. Instead, all devices in range receive messages and those which are acting as relays, retransmit the message to all other devices in range.

In general terms, flooding is a technique which has strengths and weaknesses. With Bluetooth mesh networking however, we believe we’ve optimised the design to retain the strengths but at the same time, address the weaknesses.

The Strengths of the Flooding Technique

Let’s start by considering the strengths of flooding.

Flooding has the advantage that there is no need for particular devices to have special responsibility to act as centralised routers, the failure of which could render the entire network inoperable. Specific routes being unavailable could also have a catastrophic impact on the network, and this too is avoided with a flooding approach to mesh networking.

A flooding approach also means there are generally, multiple paths by which a message can arrive at its destination. This makes for a very reliable network.

Optimizing the Mesh Network

The Bluetooth approach to mesh networking includes a number of measures which allow a flooding approach to be taken, but in a way which optimizes the energy used by individual devices and the network as a whole.

All packets include a field known as the TTL. This may be used to limit the number of hops that a message takes as it is relayed. Heartbeat messages, transmitted by devices at intervals, include information which allows the network to learn about its topology and the number of hops away, each of the other devices is. This allows devices to set TTL to an optimal value, which avoids messages being relayed an unnecessary number of times.

Every device contains a message cache so that it can determine whether or not it has seen a message before and if it has, immediately discard the message, thus avoiding unnecessary processing higher up the stack.

Perhaps most interestingly, devices which are very power-constrained, such as sensors which are powered by small batteries which must last for years, may be designated “low power nodes”. Low power nodes work in conjunction with one or more devices, which are designated “friends”. Friends are not power constrained and act on behalf of the low power node, storing messages addressed to the low power node and only delivering them when the low power node asks for them. The relationship between a low power node and a friend is, not surprisingly, termed “friendship”.

Let’s consider exactly how friendship works in terms of energy conservation.

Low power devices usually spend the most significant proportion of their time transmitting data and again, sensors are a good example of this. Maybe a sensor only transmits a temperature reading whenever the temperature falls below or above a specified threshold and perhaps this only tends to happen twice a day. Such an infrequent transmission schedule in itself, keeps the energy use of this type of device very low.

But what if the sensor needs to be able to receive data occasionally? It will need to keep up to date with the security keys being used in the network, for example. And maybe those temperature thresholds need to be modified to use different values according to the season. For a sensor to be able to receive messages directly, it needs to switch the radio on so that it can receive data. Most of the time it will receive nothing, but energy will have been expended nevertheless.

Working with a friend allows the low power node to schedule its use of the radio to receive messages to whatever frequency makes sense for the device, but importantly, a much lower frequency than it would have otherwise needed to if it had to “listen” for messages all the time, just in case that rare event of one being sent to it should occur.

Friends do the heavy lifting for low power nodes. They store messages for the low power nodes they serve and deliver them when explicitly asked to by the low power node, which operates to a schedule which they control and thus, can make the most efficient use of the radio possible.

FEATURED RESOURCE

Bluetooth Mesh Networking - An Introduction for Developers

Download this comprehensive technology overview to learn more about the key concepts and terminology, system architecture, and security mechanisms, as well as the unique message publication and delivery technique behind Bluetooth mesh networking.

In-Market Bluetooth Device Support

Bluetooth mesh networking may be new, but Bluetooth Low Energy (LE) is not. So what about the billions of devices out there in the market already? What about smartphones and tablets? Is it possible for them to access a Bluetooth mesh network?

Figure 2 - Bluetooth Low Energy devices and mesh support

Happily, the answer is YES.

Bluetooth mesh networking specifies a device role known as the Proxy Node. Proxy nodes include a standard, Bluetooth Low Energy GATT service which has two GATT characteristics. The characteristics are called Mesh Proxy Data In and Mesh Proxy Data Out. Bluetooth LE devices like smartphones can use these characteristics to send and receive data to and from the mesh network.

The mesh specification defines a protocol called the Proxy Protocol and the data exchanged via the two GATT characteristics provided by a Proxy Node consists of Proxy Protocol PDUs.

We'll dedicate an article later in this series to the role of the Proxy Node.

Security

Security is at the heart of the design of Bluetooth mesh networking and its use is mandatory.

Figure 3 - Security is mandatory in Bluetooth mesh networking

Every packet is encrypted and authenticated. Replay attacks are prevented by judicious use of sequence numbers. Man-in-the-middle attacks are protected against by using asymmetrical cryptography during important procedures. Protection against trash-can attacks, which exploit discarded devices, is provided for. Security keys get refreshed when necessary.

“Separation of Concerns” is an important principle which is reflected in the security of Bluetooth mesh networking. Security of the network and security of individual applications such as lighting, heating or physical building security are independent of each other. Different security keys are used for securing network layer operations such as relaying vs securing the application-specific content of messages. The result of this is, for example, that a light bulb has full access to data in messages transmitted by light switches, because they have the same application key. But whilst the same light bulb is able to relay messages from the Bluetooth physical access token to the lock in the front door, it is not able to see the application layer content of those messages.

We'll explore security in detail later in this series. We'll also look closely at the secure procedure known as "provisioning", which results in a device becoming a member of a Bluetooth mesh network, how devices are securely removed from the network and how security keys get refreshed when required.

The Stack

Bluetooth mesh networking introduces a new protocol stack, which as was described above, sits on top of Bluetooth low energy. Figure 4 depicts the layers of the stack.

Figure 4 - The Bluetooth mesh networking stack

The specification is the best place to thoroughly learn about the responsibilities of the various layers. Briefly though, to give you a flavour of how the stack works, the layers of the stack are each responsible for the following key functions:

bearer layer: The bearer layer defines how PDUs are transported using an underlying LE stack. Currently, two bearers are defined, the Advertising Bearer and the GATT Bearer.

network layer: The network layer defines various message address types and a network message format. The relay and proxy behaviours are implemented by the network layer.

lower transport layer: Where required, the lower transport layer handles segmentation and reassembly of PDUs.

upper transport layer: responsible for the encryption, decryption and authentication of application data passing to and from the access layer. It also has responsibility for special messages known as transport control messages. These include heartbeats and messages related to the "friendship" relationship.

access layer: responsible for the format of application data, defining and controlling the encryption and decryption process which is performed in the upper transport layer and verifying that data received from it is for the right network and application, before forwarding the data up the stack.

foundation models: The foundation model layer is responsible for the implementation of those models concerned with the configuration and management of a mesh network.

models: The model layer is concerned with the implementation of models and as such, the implementation of behaviours, messages, states and so on.

The Future of Bluetooth Mesh Networking

We expect Bluetooth mesh networking to be adopted across a broad range of industry sectors and applications. But in the first instance, we anticipate it being adopted for applications such as building automation, commercial lighting and sensor networks in particular. Commercial lighting is an especially exciting application for Bluetooth mesh networking. Think about it. With the right firmware, a lighting system can offer more than just wireless light control. It can become a platform for all manner of Bluetooth services to the building, such as asset tracking and location!

Conclusions

This was the second and final part of the first in a series of articles introducing Bluetooth mesh networking. I hope it whetted your appetite for more. In the next part, we'll introduce some of the formal terms and concepts used.

ON-DEMAND WEBINAR

What Makes Bluetooth Mesh so Disruptive?

The behind-the-scenes story of the making of Bluetooth mesh

Watch our free on-demand webinar to discover how Bluetooth mesh is disrupting building automation, wireless sensor networks, asset tracking, and more.