Spintly
Amplify the Simplicity

www.spintly.com

BLUETOOTH MESH FOR ACCESS CONTROL

Technology Overview

Abstract

Bluetooth Mesh Technology Developed For Smart Lighting And Other IoT Applications Can Be Adapted For Other Interesting Use Cases. Access Control Being One Of Them. Bluetooth Is Seemingly Becoming A Part Of All Access Control Hardware And Using That To Create A Mesh Network Create A Disruptive Technology Platform Which Changes The Way Access Control Systems Are Used And Deployed.

Rohin Parkar

rohin@spintly.com

sales@spintly.com
support@spintly.com

+1 408 214 5962
+91 87668 12888

691 S Milpitas Blvd Suite 217
Milpitas, CA 95035, United States

BLUETOOTH LOW ENERGY (BLE) MESH FOR ACCESS CONTROL

1. Introduction

Bluetooth Mesh Technology Developed For Smart Lighting And Other IoT Applications Can Be Adapted For Other Interesting Use Cases. Access Control Being One Of Them. Bluetooth Is Seemingly Becoming A Part Of All Access Control Hardware And Using That To Create A Mesh Network Create A Disruptive Technology Platform Which Changes The Way Access Control Systems Are Used And Deployed.

2. History Of Access Control Systems

If You Look Back Into History The First Access Control Systems Were In The Form Of Lock And Keys. Pre Historic Ages Used Complex Set Of Keys And Locks To Ensure Secure Entry To Barriers. In Around 1950s And 1960s Modern Access Control Systems Which Allowed The Use Keypads To Allow Access To Users. Users Entered A Unique Key Known Only To The Authorized Users To Gain Access. This System Provided Almost No Security But Solved The Problem Of Managing Keys For The Doors.
Card Readers Came Into Existence To Solve The Problems Faced By Keypad-Based Access. Magnetic Cards And Readers Became A Very Popular Means Of Access Control. This System Gradually Evolved Into RFID Based Card Readers Which Worked Based On Proximity. This Is The System Most Of Us Are Currently Familiar With. One Thing Which Remained Constant Throughout The Evolution Of Access Control Systems Was The Weigand Interface Which Became Popular In 1980s. Since Then By Far Majority Of The Access Control Readers Support The Weigand Standard. IP Door Readers Also Became Quite Popular Once LAN Started Getting Utilized In Offices. However, Wifi Based Access Control Readers Never Took-Off For Obvious Reasons Of Poor Security And Reliability. An Improved Standard For Access Control Networking Called OSDP (Open Supervised Device Protocol) Has Started Seeing Adoption Recently. OSDP Addresses The Security Vulnerabilities Of Weigand And Also Helps Reduce The Amount Of Wiring, Thanks To Its Multi Drop Capability.
The Modern Access Control Systems Have Evolved To A Point Where Now Other Methods Of Authorizations Are Widely Used. Mifare Cards, Fingerprint IDs, Face Recognition-Based IDs And Now The Latest Trend Of Smartphone Credentials Are Being Used As A Means Of Access. Mobile Based Access Control Is One Of The Fastest Growing Trends In The Market Since 2012.
We Are Now At A Point Where A Radical Shift In Access Control Systems And Technology Is Imminent.

sales@spintly.com
support@spintly.com
+1 408 214 5962
+91 87668 12888
691 S Milpitas Blvd Suite 217
Milpitas, CA 95035, United States

3. IoT-Fication Of Access Control

I Am Sure By Now Some Of You Have Started To Wonder On The Fact That If We Are Using Wifi (Wireless Communication) To Stream Videos, Or Receive E-Mails Or Do Most Of Our Work While In Office, Why Are These Access Control Systems Still Using A Wired Networks For Communication. That Is Exactly What We Wondered At Spintly And Resulted Into We Working Towards Building A Wireless Solution For Access Control. With The Goal Of Getting Rid Of Wires From Access Control Systems Various Wireless Technologies Were Evaluated. Wifi Was The Immediate First Choice Because Of Its Ubiquitous Nature. But Quickly We Realized That Typically, Wifi Networks In Offices Are Maintained By The IT Infrastructure Department And Cannot Act As A Reliable Network For Access Control System. Wifi Being An IP Based System Configuration Of Devices Through Firewalls Posed Challenges. Zigbee As A Very Strong Candidate For A Wireless Access Control Network. Zigbee Even Supports Mesh Topology. But Look At The Way The Market Was Moving Bluetooth Was Already Being Used As A Credential To Authenticate Users. Now Adding Zigbee Hardware Into Each Reader Seemed Like A Dumb Choice. Why Use 2 Wireless Technologies In The Same Device And Increase The Cost Of The Readers. Just Around 2017 The BLE (Bluetooth Low Energy) Mesh Standard Was Getting Defined. This Created Exciting Opportunities For The Access Control World And Spintly Was Quick To Jump Onto This Opportunity. Figure1 Shows How BLE-Mesh Has The Potential To Change The Way Access Control Systems Are Deployed And Set-Up.
This Is The Age Of IoT (Internet Of Things) Where Every Device Or Appliance We Use Or Will Use In Future Will Have Some Form Of Connectivity Embedded Into It. Access Control Readers Are Devices Which Need To Be Connected To The Internet And Yet Need To Very Secure. Thus, The Choice Of Wireless Connectivity Used In Access Control Readers Is Critical.

4. Why Bluetooth Mesh

Bluetooth Mesh As A Standard Was Announced By Bluetooth SIG In November-2017 And Was Mainly Focused On Lighting Applications. However, It Was Defined In Such A Way That A Model Layer Was Defined Which Allowed Exchange Of Application Specific Messages. These Allowed Adopters To Define Custom Models Based On Their Use Case. In This Case These Models Could Be Used For Access Control Use Case.
Some Of The Key Features Of Bluetooth And Bluetooth Mesh Which Make It Suitable For Access Control Applications Are Listed Below.

- **Bluetooth Is Ubiquitous:** Bluetooth Is One Of The Most Widely Used Wireless Technologies In The World. Bluetooth Is Present In Your Smartphone, Every Portable Computing Device, Cars And Bluetooth Headsets. This Has Resulted Into High Volume Production Of Bluetooth Chips Sets And Which Has Driven Their Prices To A Level That Bluetooth Devices Tend To Be Very Cost Effective. Bluetooth Is Already Getting Accepted As A Very Secure Credential For Access Control And Is Already Present In Many Access Control Readers And Thus It Just Makes Sense To Use Bluetooth As A Networking Medium.
- **Bluetooth Mesh Is Robust Wireless Standard:** Bluetooth Mesh Uses BLE Advertising Signals. BLE Advertising Happens On Channels Which Fall In The Inter-Band Regions Of The 2.4GHz (ISM) Spectrum. Hence These Signals Are Very Less Susceptible To Effects Of Noise Caused By Wifi And Bluetooth Classic. This Makes BLE Mesh Robust In Presence Of Other 2.4GHz Signals. Bluetooth Mesh Also Has Features Like TTL (Time To Live) And Caching Which Ensures The Messages Take The Optimum Number Of Hops To Reach Their Destination.

- **Bluetooth Mesh Is Highly Secure:** BLE Mesh Uses Various Levels Of Encryption Using AES-128 But Encryption To Secure The Messages. This Makes The Network One Of The Most Secure IoT Networks For Data Communication.
- **Bluetooth Mesh Is Self-Healing:** Bluetooth Mesh Is Self-Healing In Nature Which Means That It Allows Adding And Removing Of Devices In The Network On The Go. Even If A Device In The Network Goes Down The Network Automatically Reconfigures Itself And The Messages Continue To Flow Without Any Down-Time.

One Can Learn More About Bluetooth Mesh By Visiting The Resources Page On The Bluetooth Website

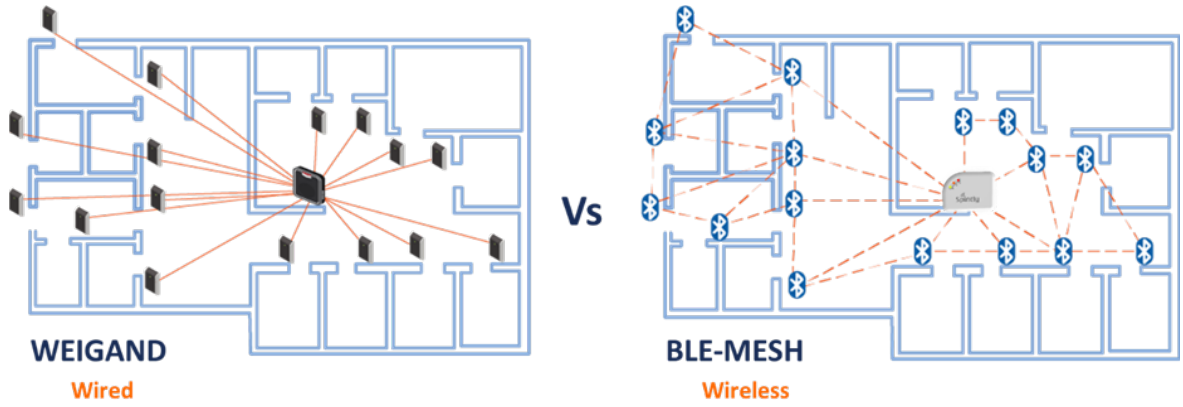

Figure 1. Weigand Vs BLE-Mesh For Access Control

5. Conclusion

In Conclusion, The Future Of Access Control Is Very Exciting And Is At A Stage Where A Big Shift In The Way Of Doing Things In The Access Control World Is Expected. Various Standards And Technologies Will Be Proposed And Experimented With. But Bluetooth Seems To Be Front Runner Mainly Due To The Fact That Companies Like Silvair Are Already Building A Robust Smart Lighting Networks Using BLE-Mesh And The Ecosystem Is Shaping Up Towards An Interoperable BLE Mesh Enabled Smart Buildings Infrastructure.