Wzzard™ Sensing Platform

Network Planning and Installation

Application Note

B+B SMARTWORX®

International Headquarters

B&B Electronics Mfg. Co. Inc.
707 Dayton Road
Ottawa, IL 61350 USA
Phone (815) 433-5100 -- **General Fax** (815) 433-5105
bb-smartsensing.com
bb-smartworx.com

support@bb-smartworx.com

European Headquarters

B&B Electronics
Westlink Commercial Park
Oranmore, Co. Galway, Ireland
Phone +353 91-792444 -- **Fax** +353 91-792445

Document: Wzzard Network Planning and Installation Application Note R1_1115

CONTENTS

1.0 OVERVIEW

Planning, deploying and installing a Wzzard network does not require any special network expertise. But some simple guidelines should be followed. Let's discuss some topics that are the keys to enabling a robust network installation. These include Planning a Deployment, Verification of Network Health and Troubleshooting common problems.

2.0 PLANNING A DEPLOYMENT

While a Wzzard network is self-forming, self-managing and self-optimizing, there are a few simple, but critical, steps that the installer should take at the planning stage. If these simple steps are followed and verified after installation, the vast majority of deployments will be successful, they will produce reliable networks, and users will obtain value from Day One.

2.1 GUIDELINE #1: 3 GOOD NEIGHBORS WITHIN RANGE OF EACH DEVICE

You must provide the Wzzard Network Gateway with the building blocks it needs to build a robust network. It is vitally important that every edge node should have enough "good neighbors". What this means is that every edge node must be able to communicate with as many other nodes as possible. As a bare minimum guideline, it is critical that every device is within range of at least three (3) other devices at the moment that it is deployed. Placing nodes within range of only one other device along a maximally spaced string will result in a fragile network that will be prone to node resets and data loss.

2.2 GUIDELINE #2: NUMBER OF 1ST HOP DEVICES

The first hop nodes are the devices that will be placed within range of the network gateway, and within range of one another. As a bare minimum, at least 10% of the devices in the network should be placed within range of the gateway. This collection of devices will form the core of the system, through which all data will travel. Following this guideline greatly improves the first hop nodes' ability (and by extension, the network's ability) to support requested data rates.

2.3 ESTIMATING RANGE

Range performance of a wireless device is affected by choices made during hardware integration (e.g. antenna choice), and even more by choices made during installation. Device placement can change the effective range by orders of magnitude. At one end of the spectrum, devices placed on elevated poles or towers with clear line of sight to other nodes in the network may have a range of 1000m or more. At the other end, devices placed on the ground, or next to large metal objects, may have an effective range of 10m or less. The most accurate way to estimate range is to evaluate range in a real environment using the same placement methods that will be used in the final installation. That being said, it is convenient to use estimates (e.g. based on transmit power and receive sensitivity) as a starting point. For a typical indoor application, we recommend that customers plan on their devices working at a spacing of 50m for nodes with internal antennas, or 100m for nodes with external antenna. Analysis of the first several 'typical' deployments can guide the typical range number up or down.

2.4 MAPPING OUT A DEPLOYMENT

A site inspection may help determine if a specific site will meet the deployment guidelines. Once you have settled on a range for your environment, you can use a scale map to place nodes at all the required sense points for the network. If possible, the gateway should be located near the middle of the distribution of nodes to reduce latency and node power. Mark the gateway location on your map. If your estimated range is 50m, draw a circle with a 50m radius around the gateway. Not all nodes within this circle will be able to communicate directly with the gateway, but some nodes outside the circle will. So it should balance out. The number of nodes inside this 50m circle approximates the number of 1-hop nodes in the deployment.

Next, draw a 100m radius circle centered at the gateway. The number of nodes in the ring between 50m and 100m approximates the number of 2-hop nodes. Repeat this process with circles of increasing radius until all nodes have been encircled and note how many nodes are in each hop.
Note that if the devices are hidden from each other they should not be counted in the list of neighbors.

Check for the following-
- Each node, including the gateway, should be within the estimated range of 3 other devices.
- 10% of nodes should be within the 1st hop.
- The network should be no more than 8 hops (recommended).

2.5 BEST PRACTICE SUGGESTIONS

- It is better to place a device at its final location and then have it join than to form your network ahead of time and subsequently scatter nodes around the site
- Have a field procedure to guarantee that the device hardware is working. Do this before it is mounted in its intended location by checking the LED status.
- Install the gateway first, then the devices at the 1st hop, and so on.
- If you have pre-planned for each node to have multiple neighbors, it is not necessary to wait for a node to join before proceeding to installing the next node. It is more important to verify that each device is on, and then to verify that all devices have joined at the gateway.
- It is better to not install devices close to ground. It is preferable to install them at least 1m above ground.
- It is better to have devices placed away from a flat metal object (at least 12 inches away if possible).

2.6 COMMISSIONING- NETWORK ID, JOIN KEY

To join the network, the node must be configured with the correct Network ID and Join Key. These parameters are persistent and may be set once prior to installation.

A node’s Network ID must match the Network ID of the gateway of the intended network. If multiple networks are operating on the site, additional care should be taken to ensure that the nodes’ Network IDs are set correctly. Similarly, if a node moves from one location to another in the deployment space, it may be out of range of its intended network. It will have the wrong Network ID for the alternative network that is now within range, and it will not be able to rejoin.

Nodes use a Join Key to encrypt the initial join request when joining a network. If the node’s join key does not match the gateway's join key the gateway will not be able to decrypt the join message and will not allow the node to join the network. For ease of use, we recommend using a single deployment-specific Join Key shared by all nodes, but unique to the customer. This will prevent malicious devices from joining the network. To join the network, a node need only be configured with the secure common Join Key.

3.0 VERIFYING THE HEALTH OF A DEPLOYED NETWORK

Evaluating the health of a network is important. You want to ensure that long-term performance targets are achievable. Network health verification is simple and is based on interpreting readily available information.

During initial installation, use the network health indicators listed below to know when it is safe to move on. In the rare case that a properly installed network does have problems, these steps will help to identify the source of problems. Often, adding more nodes in key locations will remedy the problem.

3.1 VERIFICATION PROCESS

Ask yourself these two questions:

1. Are the nodes positioned well? Does the network LOOK like it should function well?
2. Are there enough network nodes? Does the network have the building blocks it needs?

If the answer is YES to both these questions, the network should run well for the foreseeable future.

3.2 DOES THE NETWORK LOOK GOOD?

1. Is the data reliability high? In any good deployment, the data delivery rate in the network should be close to 100%. The reliability of a Wzzard network is expected to be at least four nines (>99.99%), and five nines (>99.999%) is common. It is highly unlikely that you would lose data. Confirm that this is the case.

2. Is the joining behavior correct? Have all of your devices joined? Only the installer knows how many devices were deployed. If 50 nodes were deployed, the installer must confirm that 50 nodes have joined.

It is easy to determine if a node has joined. Its LED will stop blinking.

Have all the nodes joined just once? If a node joined more than once, has it been continuously live in the network long enough to make you confident it is not constantly dropping out and rejoining?

A device that dropped out and rejoined once while the network was building is not as ominous as one that resets long after the installation is complete.

3. Does it look like a mesh? Check that all nodes have two parents in the mesh. There should be only one node in the one hop ring that has only one parent. That is OK and expected.

3.3 DOES THE NETWORK HAVE THE BUILDING BLOCKS TO BE GOOD THROUGHOUT THE LIFE OF THE NETWORK?

Ask yourself three quantitative questions about the details of connectivity in the mesh.

1. Are there enough nodes in the one-hop ring? Remember that all traffic in the network converges at the gateway node, and that the one hop nodes connect it to the rest of the network. The hardest working nodes in the mesh will be in the one-hop ring.

The more one-hop nodes, the better. They give the network more opportunity to balance the traffic and to survive a single node reset. You never want to build a system in which the removing one node will cause the loss of many nodes' data. As a rule of thumb, there should be at least 5 nodes or 10% of the total, whichever is larger, in the one-hop ring.

2. Does every node have enough "good neighbors"? (A good neighbor is a one that the node can hear at >-75dBm or has >50% path stability.) To find out, wait 15 minutes after the last node has joined, look at all the discovered paths in the network, and make sure that every node has enough good neighbors. Every node should have at least three good neighbors, at the bare minimum. The paths do not have to be currently in use, they just have to be discovered and reported by the network.

3. Are any nodes at or near their link limit? In all current products, nodes with 90 links or more indicate a risk of bandwidth issues in the network.

4.0 TROUBLESHOOTING- COMMON PROBLEMS AND SOLUTIONS

Networks are built with the goal of providing reliable performance, while keeping power usage as low as possible on the wireless devices. Links use energy, so nodes are given as few links as possible, but enough to ensure that there is sufficient bandwidth to carry the expected traffic through the node. To maintain this balance of low power and sufficient bandwidth, the gateway depends on the nodes to report their service requirements accurately, with each path averaging better than 50% stability. If there is a bottleneck, meaning that any node has run out of links, there may not be enough bandwidth to carry all the traffic from the descendants of this node.

Symptoms of a low-performing network are:
- Slow formation time
- Node resets
- Large variation in packet latency
- The gateway reports lost packets from any node

One or more of these issues will typically be the causes of poor performance:
- Poor connectivity - Nodes do not have enough neighbors with good quality paths
- Interference - In-band Wi-Fi or Bluetooth is present or a strong out-of-band interferer is nearby to lower path stability
- Oversubscription - Nodes are reporting more than their accepted service requests allow, causing congestion

To begin troubleshooting, start with these key indicators/statistics:

1. Path stability statistics of poorly connected nodes - Nodes periodically report their internal and path statistics in Health Report packets to the gateway. Check the reported path stability values on the paths that are currently being used by the node.
2. Node packet queue size - The node reports the maximum and average size of its internal packet queue. Wzzard nodes are provisioned so that they will rarely have more than one packet at any node at any time. So a nonzero average queue length usually indicates a problem.
3. Node link limits - The gateway keeps track of the network topology and the link assignments at every node in the network. This data can tell you if any nodes have run into link limits or have skipped a sequence number, which indicates a lost packet.
4. Node alarms -The gateway issues an alarm when a node resets. This may point to poor connectivity or issues observed with the children of the node.
5. Interference with Co-Located Wzzard Mesh Networks – Wzzard wireless networks are designed to coexist with both other Wzzard wireless mesh networks and other wireless devices. If there are many Wzzard networks operating in largely overlapping radio space, it is possible to see overall path stability drop if the total combined amount of traffic starts to saturate the frequency band. However, lower path stability may not necessarily translate into lower data reliability. Interference must be very severe before it can affect data reliability.

4.1 NO NODES JOIN

If no nodes have joined the gateway it will be because:
- The gateway is not running.
- There is no antenna connected to the gateway.
- The network ID and/or join key of the gateway do not match the security credentials of the nodes.
- The Access Control List (ACL) on the gateway does not include any of the nodes.
- The nodes have been placed too far away and none are within range of the gateway.
- The nodes are not powered on or batteries not installed.
- The sensor firmware on the nodes is not sending the join command correctly.

4.2 A COLLECTION OF NODES DOESN’T JOIN

If some nodes join and others do not, you have at least established that the gateway is functional.

Reasons that some nodes won't join can include:
- Some nodes are placed too far away and are not within range (Check for blinking LED).
- The maximum number of nodes that can connect to the gateway has been reached.
- Some of the nodes do not have the correct security credentials to join this gateway (network ID, join key, ACL entry).
- The nodes that are within range have been configured as leaf nodes (i.e. they are not allowed to route).

4.3 ONE NODE DOESN’T JOIN

If the number of nodes that fail to join is small relative to network size (e.g. 1 in 100), then potential reasons include:
- That node has an RF problem (It is non-functional, for example, or the antenna is not attached).
- That node has the wrong security credentials.
- That node is not powered up or has no batteries installed.

- The maximum number of nodes that can connect to the gateway has been reached.
- That node is placed too far away and is out of range of the rest of the network.

4.4 ONE NODE GETS LOST AND REJOINS REPEATEDLY

Nodes should stay connected to the network indefinitely. If a single node joins the network, drops off and rejoins again, reasons can include:
- A power supply problem on the node is causing it to reset.
- The RF connectivity to neighbors is marginal.
- The RF connectivity to neighbors is highly transient and unstable.
- The node is in a location where RF connectivity can be severed and then re-established (like in an enclosure or behind a large obstacle).

4.5 DEVICES WITH IN OPERATING RANGE HAVE BAD PATH STABILITY

It's probably interference. Place them closer together to boost connectivity.

4.6 NEED TO INSTALL A REPEATER BUT ALREADY AT MAX NODES

Repeater is needed for connectivity: Remove one node and place the repeater, or rearrange nodes to shorten paths.

Repeater needed for 1st hop bandwidth: Cut back on reporting rate, or move a node from farther out into the 1st hop ring.

4.7 DATA LATENCY IS HIGHER THAN EXPECTED

Data latency can be lowered on an individual device at the expense of battery life (for the node and its ancestors) by shortening the service period in a request but keeping publish rate unchanged. Network-wide latency can also be improved by increasing the base bandwidth.

4.8 THE NETWORK IS USING PATHS THAT DON'T LOOK OPTIMAL

The network continually tries to optimize for lowest power - part of which includes trying new paths periodically. There are other considerations besides path stability that come into play.

5.0 WZZARD GLOSSARY

Bandwidth - The capacity of a node to transmit data, usually expressed in packets/s.
Base Bandwidth - The bandwidth each node in a network gets without having to request a service.
Child - A device that receives time information from another node is its child. A child forwards data through its parent.

Commissioning - The act of configuring nodes for use in a deployment, typically by setting Network ID, join key, and other joining parameters.

Downstream - The direction away from the gateway or wired-side gateway application and into the mesh network.

Gateway - The device or process responsible for establishing and maintaining the network.

Health report - A packet sent by a node conveying its internal state and the quality of its neighbor paths. Health reports are used by the gateway in optimization and diagnostics.

Joining - The sequence of handshakes between a new node and a gateway to bring the node into the network. It begins with a node presenting an encrypted request and ends with link and run-time security credential assignment.

Latency - The time difference between packet generation and arrival at its final destination.

Mesh - A network topology where each node may be connected to one or more nodes.

Multi-hop - A network where one or more nodes has no direct path to the access point. Data packets may sometimes take multiple hops across multiple nodes to go from the source to the destination.

Neighbor - A node in range of the node in question.

Node - A device which provides wireless communications for a field device to transmit sensor or other data. The basic building block of a network.

Non-routing - A node that has been configured to not advertise. A non-routing node never forwards packets along.

Optimization - The gateway process of taking health report information and using it to modify the network to minimize energy consumption and latency.

Packet - Also called a frame. The variable sized unit of data exchange.

Parent - A device that serves as a source of time synchronization. In Dust networks, a node's parent is one hop closer to the gateway. A parent forwards a child's data towards the gateway.

Path - The potential connection between two nodes. A path that has assigned links is a used path. One that has been discovered but has no links is an unused path.

Path stability - The ratio of acknowledged packets to sent packets between two nodes. Each of the two nodes keeps a separate count of the path stability denoted by A->B and B->A. A path where the two nodes have significantly different counts of path stability is called an asymmetric path.

Provisioning - The number of links assigned by the gateway per packet generated by the node to allow for imperfect stability. Default provisioning is 3x, meaning that on average each packet has three chances to be successfully transmitted before the node starts to accumulate packets.

Publishing rate - The rate at which a node application transmits upstream data.

Reliability - The percentage of unique packets received relative to the number generated.

Route - The nodes that a packet passes through between source and destination, e.g. a packet from node 3 might use the route 3-2-6-GATEWAY. Because of the graph routing used upstream, packets originating at the same node randomly take a variety of routes.

Services - The process of requesting and receiving (or not) task-specific bandwidth.

Statistics - The aggregated information about network topology and performance constructed from the raw node health reports.

Upstream - The direction towards the gateway or wired-side application from the mesh network.