PATROLL Winning Submission

U.S. Patent 8,284,690

U.S. Patent 8,284,690 ("*Entropic Communications*" or the "patent-at-issue") was filed on December 10, 2009. Claim 1 of the patent-at-issue describes a method that involves receiving a probe request in a first node, which contains parameters specifying the content payload and target second node. Subsequently, a second set of parameters is determined, influencing how the probe will be generated and transmitted. The generated probe's form is primarily shaped by the parameters from the initial request, but the second set also contributes. Finally, the method concludes by transmitting the probe to the designated second node, essentially ensuring that the probe aligns with the specified parameters and reaches its intended destination within the network.

The primary reference, U.S. Patent 7,221,750 ("*Enright*"), was filed on January 20, 2006, and claims priority on May 24, 2002. The patent discloses methods, devices, and systems designed for the management of wireless node access within wireless networks. The process begins with the initialization and configuration of a sensor node, equipped with predefined connection parameter sets for association with specific wireless networks operated by access points. A crucial security feature is that the sensor node only accepts wireless frames that it can correctly decrypt using its stored encryption key. When the sensor node associates with a wireless access point, they engage in secure encrypted data exchange, such as package-related information, facilitated by an encryption key. Prior to disassociation, the wireless access point updates the sensor node with a new set of connection parameters, ensuring efficient network management.

The primary reference, U.S. Patent 8,339,991 ("*Biswas*"), was filed on February 28, 2008, and claims priority on March 1, 2007. The patent is directed to a device that executes a self-configuration procedure within a managed network, primarily aimed at assigning a network address. This process first involves evaluating whether the device will function as a network gateway; if so, it secures a network address for external communication. Additionally, the device scans for neighboring devices operating within the managed network, creating a database of these neighbors during the scanning process. Subsequently, the device's decision to operate as a network node leads to the selection of a managed network to join based on the information stored in the neighbor device database, ensuring efficient network integration and address allocation.

The secondary reference, U.S. Patent 7,929,504 ("*Wentink*"), was filed on December 21, 2005, and claims priority on December 23, 2004. The patent is directed to a system and method that revolve around the establishment and remote configuration of wireless nodes operating on a shared communication channel. In this setup, a master node possesses a processor capable of generating a frame containing crucial configuration details that define network configuration parameters. These parameters are essential for configuring a remote wireless node, enabling it to partake in network communications effectively. The master node then transmits this frame over the shared communication channel to a designated slave node, which is responsible for receiving the frame through its receiver. Subsequently, the slave node utilizes its processor to configure the wireless node, ensuring that it adheres to the network configuration parameters specified within the transmitted frame. This approach streamlines the process of setting up and configuring wireless nodes for efficient network communication on a shared channel.

The secondary reference, U.S. Patent 8,942,758 (“*Hoymann*”), was filed on August 17, 2009, and claims priority on September 26, 2008. The patent describes the determination of key characteristics associated with communication links, either from the terminal to a further access node or from a further terminal to the serving access node. These determined characteristics serve as the basis for selecting the appropriate access node to support uplink cooperative signal reception. Furthermore, the patent encompasses a computer program designed for execution by an access node's processor to implement this method and a computer-readable medium containing the said program. Additionally, a network device configured as a serving access node is detailed, featuring a processor responsible for determining link characteristics and making informed selections regarding the supporting access node for uplink cooperative signal reception based on these characteristics.

A sample claim chart comparing claim 1 of *Entropic Communications* to *Enright*, *Biswas*, *Wentink*, and *Hoymann* is provided below.

US8284690 (“*Entropic Communications*”)	**A. US7221750** (“*Enright*”) **B. US8339991** (“*Biswas*”) **C. US7929504** (“*Wentink*”) **D. US8942758** (“*Hoymann*”)
1. A method comprising: a) receiving in a first node, **a probe request specifying a first plurality of parameters associated with the generation and transmission of a probe**, wherein **the first plurality of parameters at least specify content payload of the probe and a second node**;	**A. US7221750** “Referring again to FIG. 4, after sensor node 60 c associates with wireless access point 50 c, sensor node 60 c and a network application may exchange information via wireless access point 50 c. For example, **a network application may receive or request sensor data from the sensor node** 60 c.” *Enright* at col. 9, lines 5-9 2. The wireless access point of claim 1 wherein the **first** and second **connection parameter sets each comprise one or more of network identification, one or more encryption keys, and a frequency**. *Enright* at Claim 2 1. A wireless access point operative to communicate with a sensor node in a wireless network, the wireless access point comprising: . . . **establish a wireless connection with a sensor node having a first connection parameter set**. . . . *Enright* at Claim 1 “During the initialization, business logic 20 transmits connection parameter data to sensor node 60 c. As described above, the connection parameter data enables sensor node 60 c to associate with the next wireless access point 50 c on the

	route. In one implementation, the business logic also provides **sensor data** to the sensor node, such as information (e.g., identification) about sensor node 60 c and/or **information (e.g., content, final destination, etc.) about the package** to which sensor node 60 c is attached." *Enright* at col. 7, lines 37-45 **B. US8339991** "A device performs its scan by scanning each channel twice (approximately 20-40 ms per channel), and performs periodic scans at predetermined intervals (such as every 10-15 seconds) thereafter. To perform a scan request, **a node broadcasts an 802.11 management probe request, with the SSID in the payload set to zero**. **The probe request packet has a message configuration that includes an 802.11 header, a type field for the managed network, a subtype field, an SSID field, and a bit rate field.** FIG. 4 shows the configuration of a probe request packet that is produced by the node device performing a scan. In the scan request packet, the message type field is set to "management", the subtype field is set to "probe request", and the SSID field is set to zero. The SSID is set to zero so that any nearby access points will respond to the probe request message." *Biswas* at col. 7, line 56 through col. 8, line 3 "Using the payload information 606, the node maintains the access point list with the following properties for each neighboring access point: MAC Address; SSID; SNR in both directions (e.g. when a **node A issues a probe request received by node B**, the node B includes the A-to-B SNR in its probe response, and when node A receives node B's probe response, node A will also know the B-to-A SNR); the IS_GW value, the IS_MERAKI value, and the gateway metric value." *Biswas* at col. 8, line 62 through col. 9, line 2 **C. US7929504** 5. The method of claim 1, wherein the first wireless node resides on a base channel, and responsive to **receiving a probe request from the second wireless node on the base channel**, **transmits the network configuration information to the second wireless node at a time when the second wireless node resides on the base channel of the access point**. *Wentink* at Claim 5

	D. US8942758 1. A method for cooperatively **receiving an uplink signal from a first terminal served by a first access node**, the method comprising: **determining at least one of: a first characteristic of a first link from the first terminal to a second access node that serves a second terminal** . . . . *Hoymann* at Claim 1
b) determining a **second plurality of parameters associated with generation and transmission of the probe**;	**A. US7221750** 1. A wireless access point operative to communicate with a sensor node in a wireless network, the wireless access point comprising: . . . **select a second connection parameter set that enables the sensor node to associate with a second wireless network**. . . . *Enright* at Claim 1 **B. US8339991** "In response to the scan message, any nearby access point will provide a management probe response message as illustrated in FIG. 5. The **response packet includes the 802.11 header field, a type field, a subtype field, and a message payload**. The type field is set to "management" and the subtype field is set to "probe response". The message payload includes information that identifies whether the responding device is a member of a network 100 that is being managed in accordance with the present invention. In particular, the **payload will include TLV (type, length, value) elements in the probe response payload that properly configured receiving devices will recognize as indicated managed network operation**. FIG. 6 shows details of the payload 602, including **data fields for timestamp 604, a beacon interval 606, capability indicator 608, respondent SSID 610, FH parameter 612, DS parameter 614 that indicates the respondent's channel of operation, and a managed network information field 616**. Additional data fields 618, 620, 622 are available for use, but currently are not used and are reserved for future use. Those skilled in the art will recognize that these data fields correspond to data fields of the 802.11 beacon frame message." *Biswas* at col. 8, lines 4-25 **C. US7929504** "The system further includes a master node including a processor configured to generate a frame that includes configuration information. The **configuration information designates network configuration parameters to remotely configure another wireless node for network communications**. The master node includes a transmitter for

	sending the configuration information over the at least one shared communication channel. The system further includes a slave node. The **slave node includes a receiver for receiving the frame including the configuration information from the master node on the at least one shared communication channel**. The slave node further includes a processor configured to configure the slave node to communicate according to the network configuration parameters.” *Wentink* at col. 2, lines 39-52 **D. US8942758** 1. A method for cooperatively receiving an uplink signal from a first terminal served by a first access node, the method comprising: determining at least one of: . . . **a second characteristic of a second link from the second terminal to the first access node**; . . . **selecting the second access node to support cooperative reception of the uplink signal**, based on a comparison of the third characteristic with at least one of the first characteristic and the second characteristic. . . . *Hoymann* at Claim 1
c) **generating the probe in accordance with the first plurality of parameters and the second plurality of parameters**, **wherein the probe has a form dictated by the first plurality of parameters**; and	**A. US7221750** “As described in more detail below, **a sensor node is initialized and configured with one or more connection parameter sets** allowing it to associate with a given wireless network implemented by one or more access points. In one implementation, the connection parameter set includes 1) security credentials, which may include, for example, a network pass-phrase for authentication, and/or a network identification (network ID) that identifies the wireless network to which the sensor node may associate, 2) an encryption key that enables the sensor node and the wireless access point to establish a security association and exchange encrypted information, and 3) **a frequency identifier corresponding to the frequency channel enabling the sensor node and the wireless access point to communicate**.” *Enright* at col. 3, lines 2-15 **B. US8339991** “In response to the scan message, **any nearby access point will provide a management probe response message** as illustrated in FIG. 5. The response packet **includes the 802.11 header field, a type field, a subtype field, and a message payload**. The type field is set to “management” and the

	subtype field is set to “probe response”. The message payload includes information that identifies whether the responding device is a member of a network 100 that is being managed in accordance with the present invention. In particular, the **payload will include TLV (type, length, value) elements in the probe response payload that properly configured receiving devices will recognize as indicated managed network operation**. FIG. 6 shows details of the payload 602, including **data fields for timestamp 604, a beacon interval 606, capability indicator 608, respondent SSID 610, FH parameter 612, DS parameter 614 that indicates the respondent's channel of operation, and a managed network information field 616**. Additional data fields 618, 620, 622 are available for use, but currently are not used and are reserved for future use. Those skilled in the art will recognize that these data fields correspond to data fields of the 802.11 beacon frame message.” *Biswas* at col. 8, lines 4-25 **C. US7929504** 13. The method of claim 12, further including: the **second wireless node accepting the network configuration information and configuring the second wireless node according to the designated network configuration parameters**; and *Wentink* at Claim 13 **D. US8942758** . . . **selecting the second access node to support cooperative reception of the uplink signal**, **based on a comparison of the third characteristic with at least one of the first characteristic and the second characteristic**. *Hoymann* at Claim 1
d) **transmitting the probe from the first node to the second node**.	**A. US7221750** “During the initialization, business logic 20 **transmits connection parameter data to sensor node** 60 c. As described above, the connection parameter data enables sensor node 60 c to associate with the next wireless access point 50 c on the route. In one implementation, the business logic also provides sensor data to the sensor node, such as information (e.g., identification) about sensor node 60 c and/or information (e.g., content, final destination, etc.) about the package to which sensor node 60 c is attached.” *Enright* at col. 7, lines 37-45

	B. US8339991 "With the **received payload information**, the node devices build a list of access points that make up the mesh network 110. A node device builds a list of nearby access points with an identifier corresponding to the network as a result of its wireless scans on each channel. FIG. 7 shows details of the Managed Network Information field 616 in **the response payload** 602." *Biswas* at col. 8, lines 26-32 "Using the **payload information** 606, the node maintains the access point list with the following properties for each neighboring access point: MAC Address; SSID; SNR in both directions (e.g. when a node A issues a probe request received by node B, the node B includes the A-to-B SNR in its probe response, and when node A receives node B's probe response, node A will also know the B-to-A SNR); the IS_GW value, the IS_MERAKI value, and the gateway metric value." *Biswas* at col. 8, line 62 through line 9, line 2 **C. US7929504** 37. The first wireless node of claim 32, wherein the first wireless node resides on a base channel, and the first wireless node further comprises: means for receiving a probe request from the second wireless node on the base channel; and means for **transmitting the network configuration information to the second wireless node at a time when the second wireless node is residing on the base channel of the first wireless node in response to receiving the probe request**. *Wentink* at Claim 37 **D. US8942758** 7. The method according to claim 1, further comprising **transmitting, from the first access node to the second access node**, scheduling information for a reference signal transmitted by the terminal. *Hoymann* at Claim 7