IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
MARSHALL DIVISION

STINGRAY IP SOLUTIONS, LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
AMAZON.COM, INC., AMAZON.COM SERVICES LLC, RING LLC, EERO LLC, and IMMEDIA SEMICONDUCTOR LLC,	§	**CIVIL ACTION NO. 2:21-cv-194**
	§	
Defendants.	§	
	§	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions, LLC ("Stingray") files this Complaint in this Eastern District of Texas (the "District") against Defendants Amazon.com, Inc., Amazon.com Services LLC, Ring LLC, eero LLC, and Immedia Semiconductor LLC (collectively, "Defendants" or "Amazon") for infringement of U.S. Patent No. 7,082,117 (the "'117 patent"), U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No. 7,440,572 (the "'572 patent"), and U.S. Patent No. 7,616,961 ("the "'961 patent").

THE PARTIES

1. Stingray IP Solutions, LLC ("Stingray" or "Plaintiff") is a Texas limited liability company, located at 6136 Frisco Sq. Blvd., Suite 400, Frisco, TX 75034.

2. On information and belief, Defendant Amazon.com, Inc. ("Amazon.com") is a corporation organized under the laws of the state of Delaware, with its principal place of business located at 410 Terry Avenue North, Seattle, Washington 98109. Amazon.com may be served with

process via its registered agents, including Corporation Service Company, 300 Deschutes Way SW Ste 208 MC-CSC1, Tumwater, WA, 98501 and Corporation Service Company, 251 Little Falls Dr., Wilmington, DE 19808. Amazon.com is a publicly traded company on the Nasdaq Global Select Market under the symbol "AMZN."

3. On information and belief, Defendant Amazon.com Services LLC (formerly "Amazon.com Services, Inc." and referred to herein as "Amazon Services") is a limited liability company organized under the laws of the state of Delaware, with its principal place of business at 410 Terry Avenue North, Seattle, Washington 98109. *See also Vocalife, LLC v. Amazon.com, Inc. and Amazon.com, LLC*, Case No. 2:19-cv-00123-JRG, Dkt. 14 at ¶ 3 (E.D. Tex. July 2, 2019) (Amazon admitting that Amazon.com LLC merged into Amazon.com Services, Inc., the predecessor of Defendant Amazon Services). Amazon Services is a wholly owned subsidiary of Amazon.com. Amazon Services is registered to do business in the state of Texas and may be served with process via its registered agent in Texas: Corporation Service Company d/b/a CSC-Lawyers Incorporating Service Company at 211 7th Street, Suite 620, Austin TX 78701-3218. Amazon Services may also be served via its Delaware registered agent: Corporation Service Company, 251 Little Falls Dr., Wilmington, DE 19808.

4. On information and belief, Defendant Ring LLC ("Ring") is a limited liability company organized under the laws of the state of Delaware, with its principal place of business at 410 Terry Avenue North, Seattle, Washington 98109. Ring is a wholly owned subsidiary of Defendant Amazon.com. Ring may be served with process via its registered agent in Delaware: Corporation Service Company, 251 Little Falls Dr., Wilmington, DE 19808.

5. On information and belief, Ring manufactures and sells home security products, including its home security Ring-branded of products and related services. In 2018, Amazon purchased Ring for more than $1 billion.

6. On information and belief, Defendant eero LLC (capitalization intentional, referred to herein as "eero") is a limited liability company organized under the laws of the state of Delaware, with its principal place of business at 410 Terry Avenue North, Seattle, Washington 98109. eero is a wholly owned subsidiary of Defendant Amazon.com. The company eero may be served with process via its registered agent in Delaware: Corporation Service Company, 251 Little Falls Dr., Wilmington, DE 19808.

7. On information and belief, eero manufactures and sells a line of eero-branded mesh wireless routers. In 2019, Amazon acquired eero for $97 million.

8. On information and belief, Defendant Immedia Semiconductor LLC (also known as and referred to herein as "Blink") is a limited liability company organized under the laws of the state of Delaware, with its principal place of business at 410 Terry Avenue North, Seattle, Washington, 98109. Blink is a wholly owned subsidiary of Amazon.com Services LLC, and Defendant Amazon.com is the ultimate parent of Blink. Blink is registered to do business in Texas and may be served with process via its registered agent in Delaware: Corporation Service Company, 251 Little Falls Dr., Wilmington, DE 19808.

9. On information and belief, Blink manufactures and sells Blink-branded security cameras. In 2017, Amazon acquired Blink for around $90 million.

10. Via online and physical stores, Amazon sells "hundreds of millions of unique products" by Amazon and third parties "across dozens of product categories." 2020 Annual Report, Amazon.com, Inc., at p. 3,

https://s2.q4cdn.com/299287126/files/doc_financials/2021/ar/Amazon-2020-Annual-Report.pdf (last visited May 21, 2021). Amazon also manufactures and sells "electronic devices, including Kindle, Fire tablet, Fire TV, Echo, Ring, and other devices." Id. Amazon offers delivery services for its products purchased on-line, including delivery of its electronic devices to customers for a delivery fee or via its subscription delivery services, i.e., Amazon Prime. *See More of what you love, delivered in more ways.*, AMAZON.COM, https://www.amazon.com/b?ie=UTF8&node=15247183011 (last visited May 24, 2021).

11. Among these electronic devices, Amazon makes and sells smart home devices which communicate with each other over a variety of network protocols. For instance, Amazon's Echo-branded products include smart speakers, smart displays, and smart streaming devices that when coupled with voice-controls, such as Amazon's Alexa application, allow customers to control, via at least Wi-Fi and ZigBee communication protocols, other Amazon and third-party smart home devices, including smart plugs, cameras, lights, and appliances. *See Devices & Services*, AMAZON.COM, https://www.aboutamazon.com/what-we-do/devices-services (last visited May 21, 2021). Ring-branded devices of Amazon include video doorbells, alarm systems, and smart lighting. See id. Ring's alarm systems utilize the Wi-Fi, Z-Wave, and ZigBee communication protocols to control and monitor security sensors, such as keypads, contact sensors, motion detectors, range extenders, flood and freeze sensors, smoke and CO listeners, and panic buttons. Blink-branded products of Amazon utilize Wi-Fi protocols (i.e., 802.11) to provide battery-powered wireless home security cameras and video monitoring, bringing "a watchful eye and one-click connection" to customers' homes. See id. eero-branded products of Amazon provide home Wi-Fi systems that "blanket[] customers' homes in fast, reliable Wi-Fi." *See id.* As an added feature, eero products are configured as a ZigBee smart home hub "eliminating the need for

additional ZigBee hubs around the home." *See FAQ*, EERO, AN AMAZON COMPANY, https://eero.com/shop/eero-pro-6 (scroll from top of page down to FAQ section) (last visited May 21, 2021).

12. On information and belief, Defendants, on their own and/or via subsidiaries and affiliates, maintain a corporate and commercial presence in the United States, including in Texas and this District, via at least its 1) online presence (e.g., amazon.com and woot.com) that solicits sales of its products and services; 2) its physical stores, including Amazon's 4-star stores and Whole Foods grocery store locations; 3) Amazon's retail distribution and sales of its products, including sales of its Amazon Echo, Ring, Blink, and eero products in third-party retail stores located and targeting customers in this District; 4) Amazon's home delivery of products to customers in this District; 5) Amazon's self-service package delivery service (referred to as "Amazon Locker") operating in this District; 6) Amazon's corporate and administrative offices; 7) Amazon's distribution facilities; and 8) Amazon's employment of thousands of residents of the state of Texas, who work to and/or commute for work from this District. For example, Defendants, on their own and/or via subsidiaries and affiliates, maintain a fulfillment facility located at 15201 Heritage Parkway, Fort Worth, TX 76177, among other properties identified herein. Thus, Amazon does business in the U.S., the state of Texas, and in the Eastern District of Texas.

JURISDICTION AND VENUE

13. This action arises under the patent laws of the United States, namely 35 U.S.C. §§ 271, 281, and 284-285, among others.

14. This Court has subject matter jurisdiction pursuant to 28 U.S.C. §§ 1331 and 1338(a).

A. Defendant Amazon.com

15. On information and belief, Defendant Amazon.com is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, affiliates, and/or consumers.

16. For example, Amazon.com owns and/or controls multiple subsidiaries and affiliates, including, but not limited to Defendants Amazon Services, Ring, eero, and Blink, that have a significant business presence in the U.S. and in Texas. *See, e.g., Find jobs by location*, AMAZONJOBS, https://www.amazon.jobs/en/locations/?&continent=all&cache (click "North America" to see Amazon employment locations across the U.S., including Austin, Dallas/Fort Worth Area, and San Antonio locations) (last visited May 24, 2021). Amazon.com, via its at least wholly owned subsidiary Amazon Services, operates a fulfillment center, among other properties such as warehouses, package sorting centers, physical stores, and self-service delivery locations, in at least Denton county and Collin county, i.e., in this District, at 15201 Heritage Parkway, Fort Worth, TX 76177. *See Property Search Results > 1-7 of 7 for Year 2021*, DENTON CAD https://propaccess.trueautomation.com/clientdb/SearchResults.aspx?cid=19 (search results for "Amazon" as owner) (last visited May 24, 2021); *see also Amazon to hire 6,500 people in Dallas*

area, 100,000 across the country, WFAA, https://www.wfaa.com/article/money/business/amazon-to-hire-6500-people-in-dallas-area-100000-across-the-country/287-09fb8559-deda-4d14-b256-ff432edbc410 ("Amazon also opened a new fulfillment center in Dallas earlier this year, and will have three new delivery stations in Fort Worth, Frisco and Forney, according to the spokesperson.") (last visited May 25, 2021). Denton county CAD search results show that Defendant Amazon.com Services LLC and other subsidiary Amazon Logistics own at least six properties in Denton county. These properties are Amazon facilities and employ thousands of residents of the state of Texas and this District. *See Amazon to hire 6,500 people in Dallas area, 100,000 across the country*, WFAA, https://www.wfaa.com/article/money/business/amazon-to-hire-6500-people-in-dallas-area-100000-across-the-country/287-09fb8559-deda-4d14-b256-ff432edbc410 ("Amazon said [in September 2020] that it will be hiring another 100,000 people to keep up with a surge of online orders, including 6,500 open roles in the Dallas area."). (last visited May 24, 2021).

17. On information and belief, Amazon.com also owns and operates Whole Foods Market grocery stores in Texas and in this District. *See Amazon to Buy Whole Foods for $13.4 Billion*, THE NEW YORK TIMES (June 16, 2007), https://www.nytimes.com/2017/06/16/business/dealbook/amazon-whole-foods.html (last visited May 25, 2021). which not only sell grocery products to and employ residents of the District, but also serve as delivery locations, i.e., Amazon Hub lockers, that provide "a secure, self-service kiosk that allow you to pick up your package at a place and time that's convenient for you — even evenings and weekends." See Everything you need to know about Amazon Hub Locker, Amazon.com, https://www.amazon.com/primeinsider/tips/amazon-locker-qa.html (last visited May 24, 2021). For example, an Amazon Hub Locker is located in the Plano Whole Foods Market

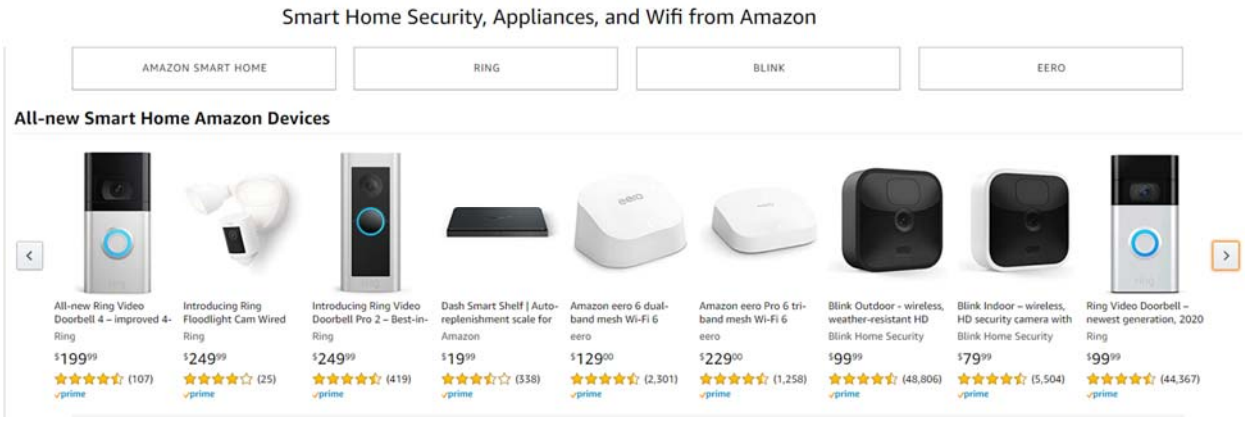
located at 2201 Preston Rd., Plano, TX 75093. See Plano – Store Amenities, Whole Foods Market, https://www.wholefoodsmarket.com/stores/plano (click "Store Amenities" to scroll to amenities description) (last visited May 25, 2021). Customers, including residents, shopping within this District may, therefore, purchase and have Amazon's smart home devices delivered to Whole Foods locations that contain Amazon Hub Lockers.

18. Such a corporate and commercial presence by Defendant Amazon.com furthers the development, design, manufacture, importation, distribution, and sale of Amazon's infringing electronic devices in Texas, including in this District. Through direction and control of its subsidiaries and affiliates, Amazon.com has committed acts of direct and/or indirect patent infringement within Texas, this District, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Amazon.com would not offend traditional notions of fair play and substantial justice.

19. On information and belief, Amazon.com controls or otherwise directs and authorizes all activities of its subsidiaries and affiliates, including, but not limited to Defendants Amazon Services, Ring, eero, and Blink, which, significantly, have substantial business operations in Texas. Directly and via at least these subsidiaries and/or affiliates and via intermediaries, such as distributors and customers, Amazon.com has placed and continues to place infringing electronic devices, including Amazon.com's smart home devices, such as Echo, Ring, eero, and Blink devices, into the U.S. stream of commerce. Amazon.com has placed such products into the stream of commerce with the knowledge and understanding that such products are, will be, and continue to be sold, offered for sale, and/or imported into this District and the State of Texas. *See Litecubes, LLC v. Northern Light Products, Inc.*, 523 F.3d 1353, 1369-70 (Fed. Cir. 2008) ("[T]he sale [for purposes of § 271] occurred at the location of the buyer."); *see also Semcon IP Inc. v. Kyocera*

Corporation, No. 2:18-cv-00197-JRG, 2019 WL 1979930, at *3 (E.D. Tex. May 3, 2019) (denying accused infringer's motion to dismiss because plaintiff sufficiently plead that purchases of infringing products outside of the United States for importation into and sales to end users in the U.S. may constitute an offer to sell under § 271(a)).

20. Defendant Amazon.com utilizes established distribution channels to distribute, market, offer for sale, sell, service, and warrant infringing products directly to consumers, including offering such smart home products, including Echo, Ring, Blink, and eero products, for sale under its overarching house brand "Amazon" via its own website, as shown below.



See Smart Home Security, Appliances, and Wifi from Amazon, AMAZON.COM, https://www.amazon.com/b?ie=UTF8&node=17386948011 (showing Amazon smart home devices from Ring, eero, and Blink brands sold on Amazon's flagship website) (last visited May 24, 2021).

21. Moreover, Defendant Amazon.com utilizes its subsidiaries, affiliates, and intermediaries, such as Defendants Amazon Services, Ring, eero, and Blink, to design, develop, import, distribute, and service infringing products, such as Amazon Echo, Blink, Ring, and eero-branded products. Such Amazon products have been sold in retail stores, both brick and mortar and online, in Texas and within this District. *See., e.g., Amazon - Echo Show 10 (3rd Gen) HD smart display with motion and Alexa*, BEST BUY, https://www.bestbuy.com/site/amazon-echo-show-10-3rd-gen-hd-smart-display-with-motion-and-alexa-charcoal/6430066.p?skuId=6430066

(showing that Amazon's Echo Show 10 (3rd) is available for purchase and pick up from Best Buy store at 1800 S Loop 288, Ste 102 Bldg 1, Denton, TX 76205, i.e., in this District) (last visited May 24, 2021).

22. On information and belief, Defendant Amazon.com also purposefully places infringing smart home devices in established distribution channels in the stream of commerce by contracting with national retailers who sell Amazon's products in the U.S., including in Texas and this District. Amazon contracts with these companies with the knowledge and expectation that Amazon's smart home devices will be imported, distributed, advertised, offered for sale, and sold in the U.S. market. For example, at least BestBuy, Costco, Home Depot, Lowes, Target, and Bed, Bath, and Beyond offer for sale and sell Amazon electronic devices, such as the Echo, Ring, eero, and/or Blink brands, in and specifically for the U.S. market, via their own websites or retail stores located in and selling their products to consumers in Texas and this District. *See, e.g., Purchasing Ring Products*, RING, https://support.ring.com/hc/en-us/articles/204755524-Purchasing-Ring-Products (showing where the Amazon's Ring products) (last visited May 24, 2021). Amazon.com also provides its application software, the "Alexa App," for download and use in conjunction with and as a part of its Alexa-enabled devices. *See Alexa Devices Help*, AMAZON.COM, https://www.amazon.com/gp/help/customer/display.html?nodeId=202009680 (listing some Amazon devices that are compatible with Alexa) (last visited May 24, 2021). The Alexa App is available via digital distribution platforms by Apple Inc. and Google.

23. Based on Defendant Amazon.com's connections and relationship with its U.S.-based national retailers, package delivery services (e.g., UPS, USPS, and Fed Ex), and digital distribution platforms, Amazon.com knows that Texas is a termination point of the established distribution channel, namely sales to customers via online and brick and mortar stores offering Amazon smart

home products and related software to consumers in Texas and direct delivery to customers via Amazon's Prime Delivery service and the Amazon Hub Locker service. Amazon.com, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis. *See Icon Health & Fitness, Inc. v. Horizon Fitness, Inc.*, 2009 WL 1025467, at (E.D. Tex. 2009) (finding that "[a]s a result of contracting to manufacture products for sale in" national retailers' stores, the defendant "could have expected that it could be brought into court in the states where [the national retailers] are located").

24. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Amazon.com has committed acts of infringement in this District. As further alleged herein, Defendant Amazon.com, via its own operations and employees located there and via ratification of Defendant Amazon Services' presence, has a regular and established place of business, in this District at least at a fulfillment facility located at 15201 Heritage Parkway, Fort Worth, TX 76177, among other Amazon locations owned and operated in this District including those identified herein in Collin and Denton counties. Accordingly, Amazon.com may be sued in this district under 28 U.S.C. § 1400(b).

B. Defendant Amazon Services

25. On information and belief, Defendant Amazon Services is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents

and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, Amazon Services, including as an alter ego of parent company Amazon.com, owns and operates several Amazon fulfillment facilities, warehouses, self-service delivery locations, and physical stores throughout the District. Amazon Services is the owner of at least the following Amazon facilities in Collin county:

- An Amazon delivery station located at 16399 Gateway Dr., Frisco, TX 75033 (*see Amazon to open delivery station in Frisco, offer hundreds of local job opportunities*, COMMUNITY IMPACT NEWSPAPER (June 26, 2020), https://communityimpact.com/dallas-fort-worth/frisco/impacts/2020/06/26/amazon-to-open-delivery-station-in-frisco-offer-hundreds-of-local-job-opportunities/) (last visited May 25, 2021); and
- An Amazon 4-star store located at 2601 Preston Rd. Frisco, TX 75034 (*see Amazon 4-star - Stonebriar Centre*, AMAZON.COM, https://www.amazon.com/Amazon-4-star-Frisco-Stonebriar-Centre/b?ie=UTF8&node=20017628011 (last visited May 25, 2021).

26. A further detailed listing of Amazon Services' properties in Collin county is found at https://www.collincad.org/propertysearch by searching using "Amazon" as part of the owner name.

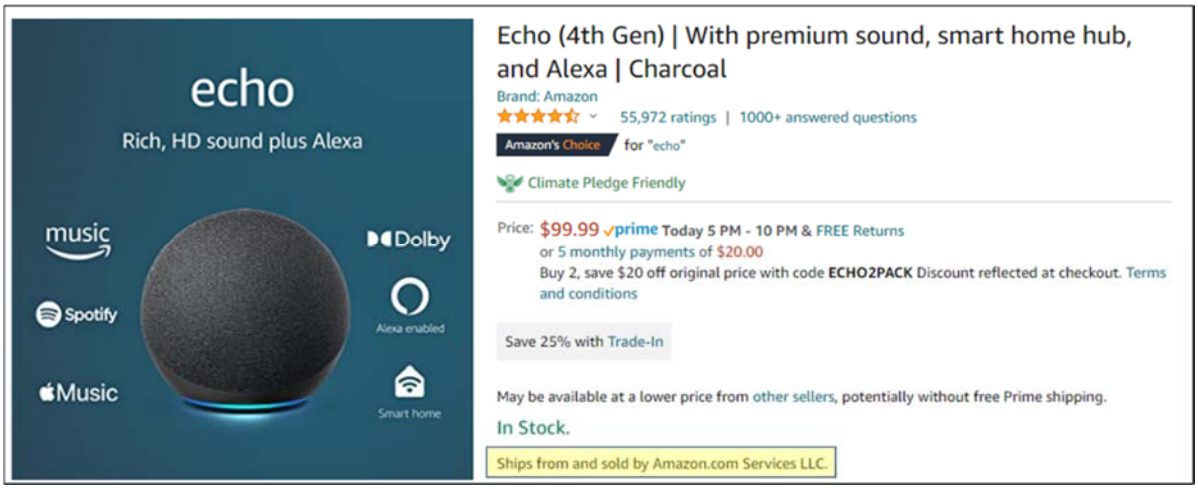
27. Amazon Services is the owner of at least the following Amazon facilities in Denton county:

- An Amazon fulfillment center ("FTW3/ FTW4") located at 15201 Heritage Pkwy, Fort Worth, TX 76177;
- An Amazon distribution facility ("DDF1") located at 1550 Lakeway Dr Lewisville, TX;
- An Amazon distribution facility ("DDF1") 1303 Ridgeview Dr., Lewisville, TX 75057;

- An Amazon Hub located in a BBVA bank at 3640 N Josey Ln, Carrollton, TX 75007 (*see Find pickup locations near:*, Amazon.com, https://www.amazon.com/ulp/pickup-points (search using zip code "75007" and scroll to Amazon Hub Locker - Charisma) (last visited May 25, 2021)); and
- An Amazon Woot! corporate office located at 4121 International Pkwy, Carrollton TX, 75007-1907 (*see Woot LLC, Company Profile*, https://www.dnb.com/business-directory/company-profiles.woot_llc.d0a61f3586186285d22505f5d5beef5a.html (last visited May 25, 2021)).

28. A further detailed listing of Amazon Services' properties in Denton county is found at https://propaccess.trueautomation.com/clientdb/?cid=19by searching using "Amazon" as part of the owner name.

29. Defendant Amazon Services further is responsible for shipping, selling, and delivering Amazon's smart home devices, including Echo, Ring, Blink and eero branded products, from the Amazon.com website and purposefully placing infringing smart home devices in established distribution channels in the stream of commerce in the U.S., including in Texas and this District. As shown below, consumers in this District are notified each time they browse for Amazon smart home products that the product, such as the Amazon Echo (4th Gen), "[s]hips from and [is] sold by Amazon.com Services LLC." Amazon Services, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court.



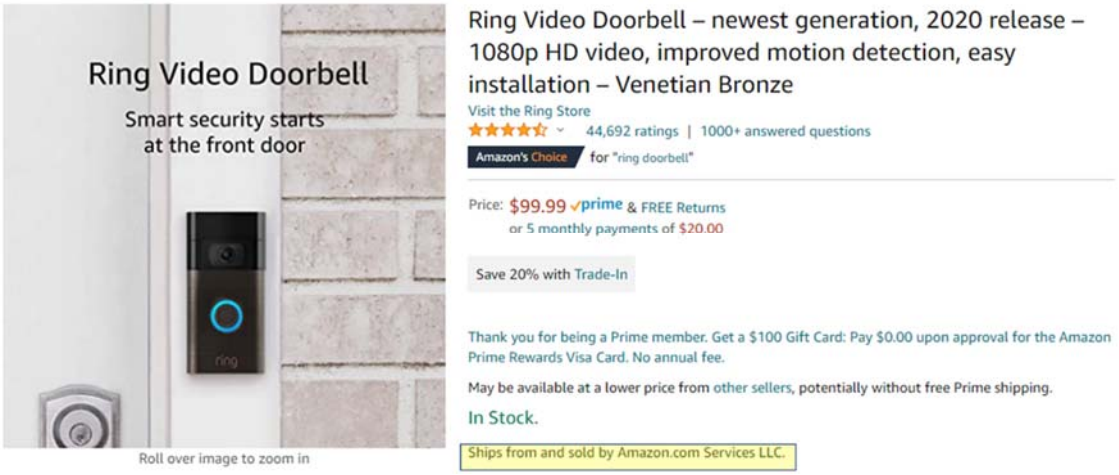
See Echo (4th Gen) | With premium sound, smart home hub, and Alexa, AMAZON.COM, https://www.amazon.com/dp/B085HK4KL6?ref=MarsFS_AUCC_lr (last visited May 25, 2021).

30. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). Defendant Amazon Services has committed acts of infringement in this district and has one or more regular and established places of business in this District, including those listed above in Collin and Denton counties, and by one example at least at 15201 Heritage Pkwy, Fort Worth, TX 76177. Accordingly, Amazon Services may be sued in this district under 28 U.S.C. § 1400(b).

C. Defendant Ring

31. On information and belief, Defendant Ring is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers.

32. For example, Ring distributes, sells, and delivers its Ring-branded products to consumers in this District via its parent companies Defendants Amazon.com and Amazon Services. Consumers, for example, are notified each time they browse for Ring-branded smart home products of Amazon that the product, such as the Ring Video Doorbell, "[s]hips from and [is] sold by Amazon.com Services LLC," as shown below.



33. By working in concert with its parent companies Defendants Amazon.com and Amazon Services to store, distribute, sell, and deliver its products to Texas residents, including those of this District, Ring purposefully places infringing smart home devices in established distribution channels in the stream of commerce. Ring also distributes its products to residents of Texas and this District, via national retailers, such as Best Buy, Costco, Home Depot, Lowes, Target, and Bed, Bath and Beyond. *See Purchasing Ring Products*, RING, https://support.ring.com/hc/en-us/articles/204755524-Purchasing-Ring-Products (last visited May 25, 2021). Ring, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court.

34. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Ring has committed acts of infringement in this District and has one or more regular and established places of business in this District. The regular and established

places of business of Ring's ultimate parent Defendant Amazon.com and of Defendant Amazon Services, including those listed above in Collin and Denton counties, are also regular and established places of business of Defendant Ring. One such regular and established place of business is an Amazon fulfillment facility located at 15201 Heritage Pkwy, Fort Worth, TX 76177, among others. As an affiliate, subsidiary, and alter ego of Amazon.com and Amazon Services, Ring utilizes these facilities located in this District to store inventory of Ring products and deliver such products to consumers living and working in the District. Employees and agents of Defendants Amazon.com and Amazon Services working at these facilities of Amazon, therefore, act as agents of Ring to which Ring exercises some degree of control in managing said inventory, completing deliveries, and handling returns. Accordingly, Ring may be sued in this district under 28 U.S.C. § 1400(b).

D. Defendant eero

35. On information and belief, Defendant eero is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers.

36. For example, eero distributes, sells, and delivers its eero-branded products to consumers in this District via its parent companies Defendants Amazon.com and Amazon

Services. Consumers, for example, are notified each time they browse for eero-branded smart home products of Amazon that the product, such as the eero mesh Wi-Fi system, "[s]hips from and [is] sold by Amazon.com Services LLC," as shown below.

37. By working in concert with its parent companies Defendants Amazon.com and Amazon Services to store, distribute, sell, and deliver its products to Texas residents, including those of this District, eero purposefully places infringing smart home devices in established distribution channels in the stream of commerce. eero also distributes its products to residents of Texas and this District, via national retailers, such as Best Buy, Crutchfield, newegg.com, and Dell. *See Where to Buy*, RING, https://eero.com/where-to-buy (last visited May 25, 2021). Eero, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court.

38. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant eero has committed acts of infringement in this District and has one or more regular and established places of business in this District. The regular and established places of business of eero's ultimate parent Defendant Amazon.com and of Defendant Amazon Services, including those listed above in Collin and Denton counties, are also regular and established places

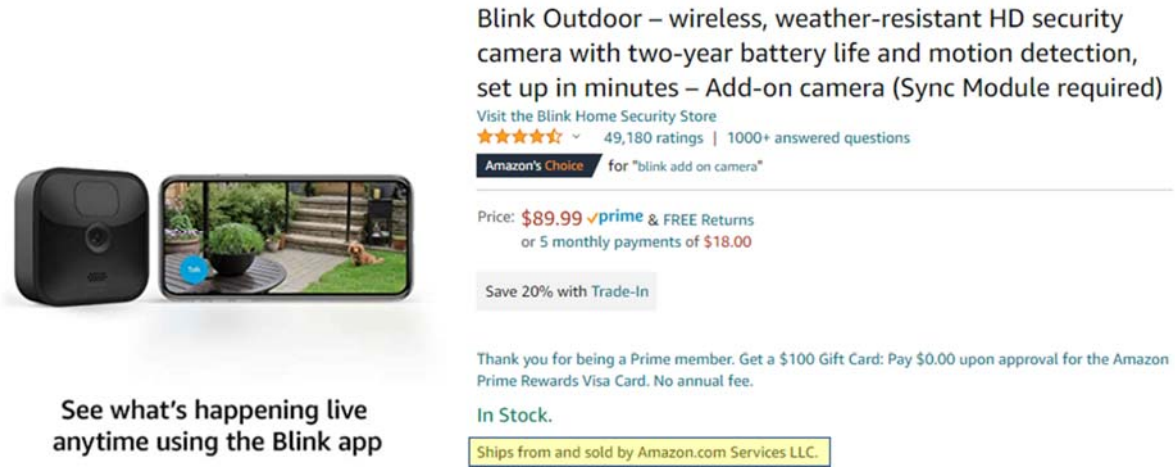
of business of Defendant eero. One such regular and established place of business is an Amazon fulfillment facility located at 15201 Heritage Pkwy, Fort Worth, TX 76177, among others. As an affiliate, subsidiary, and alter ego of Amazon.com and Amazon Services, eero works in concert with its parent companies to store inventory of eero products at these facilities and deliver such products to consumers from these facilities. Employees and agents of Defendants Amazon.com and Amazon Services working at these facilities, therefore, act as agents of eero to which eero exercises some degree of control in managing said inventory, completing deliveries, and handling returns. Accordingly, eero may be sued in this district under 28 U.S.C. § 1400(b).

E. Defendant Blink

39. On information and belief, Defendant Blink is subject to this Court's specific and general personal jurisdiction pursuant to due process and/or the Texas Long Arm Statute, due at least to its substantial business in this State and this District, including: (A) at least part of its infringing activities alleged herein which purposefully avail the Defendant of the privilege of conducting those activities in this state and this District and, thus, submits itself to the jurisdiction of this court; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this District, and/or deriving substantial revenue from infringing goods offered for sale, sold, and imported and services provided to and targeting Texas residents and residents of this District vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers.

40. For example, Blink distributes, sells, and delivers its Blink-branded products to consumers in this District via its parent companies Defendants Amazon.com and Amazon Services. Consumers, for example, are notified each time they browse for eero-branded smart

home products of Amazon that the product, such as the Blink Outdoor camera, "[s]hips from and [is] sold by Amazon.com Services LLC," as shown below.



41. By working in concert with its parent companies Defendants Amazon.com and Amazon Services to store, distribute, sell, and deliver its products to Texas residents, including those of this District, Blink purposefully places infringing smart home devices in established distribution channels in the stream of commerce. eero also distributes its products to residents of Texas and this District, via national retailers, such as Best Buy, The Home Depot, Target, Kohl's, and Staples. *See Select Your Country – United States*, BLINK, https://blinkforhome.com/select-country (last visited May 25, 2021). Blink, therefore, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court.

42. Venue is proper in this District pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). As alleged herein, Defendant Blink has committed acts of infringement in this District and has one or more regular and established places of business in this District. The regular and established places of business of Blink's ultimate parent Defendant Amazon.com and of Defendant Amazon Services, including those listed above in Collin and Denton counties, are also regular and established places of business of Defendant Blink. One such regular and established place of business is an Amazon fulfillment facility located at 15201 Heritage Pkwy, Fort Worth, TX 76177,

among others. As an affiliate, subsidiary, and alter ego of Amazon.com and Amazon Services, Blink works in concert with its parent companies to store inventory of Blink products at these facilities and deliver such products to consumers from these facilities. Employees and agents of Defendants Amazon.com and Amazon Services working at these facilities, therefore, act as agents of Blink to which Blink exercises some degree of control in managing said inventory, completing deliveries, and handling returns. Accordingly, Blink may be sued in this district under 28 U.S.C. § 1400(b).

43. On information and belief, Amazon.com, Amazon Services, Ring, eero, and Blink each have significant ties to, and presence in, the State of Texas and the Eastern District of Texas, making venue in this District both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

44. The Asserted Patents cover various aspects of monitoring, detecting intrusions, and encrypting and decrypting wireless communications networks, including networks created between Defendants' smart home devices.

45. The '117 patent involves detecting intrusions into a wireless communication network by monitoring transmissions among nodes of the network. The disclosed intrusion detection techniques of the '117 patent include monitoring, by a policing node, transmissions among a plurality of nodes of a mobile ad-hoc network (MANET). Such nodes of the MANET intermittently operate in a contention-free mode during a contention-free period. The policing node detects intrusions by monitoring the transmissions between the MANET nodes to detect contention-free mode operation outside of a contention-free period. Based on such a detection, an intrusion alert may be generated.

46. The '678 patent involves detecting intrusions into a wireless local or metropolitan area network. The disclosed intrusion detection techniques include monitoring transmission

between stations of the network, where each station has its own media access layer (MAC) address. The monitoring is done to detect failed attempts to authenticate the MAC addresses. Upon detection of a number of failed attempts to authenticate, an intrusion alert may be generated.

47. The '961 patent involves allocating channels in mobile ad hoc networks. The patent describes dynamic channel allocation in such networks to efficiently make use of a plurality of channels. In such networks, wireless communication links connect wireless mobile nodes over multiple separate channels at different frequencies. The disclosed techniques for channel allocation include monitoring link performance on one channel based on a quality of service (QoS) threshold. When the monitored link performance falls below the QoS threshold, other available separate channels are scouted. Scouting may include switching to a second separate channel at a different frequency. A channel activity query may be broadcast to determine link performance of the second separate channel. Replies to the query are processed to determine the link performance, and channel activity may be updated for each separate channel based on the replies.

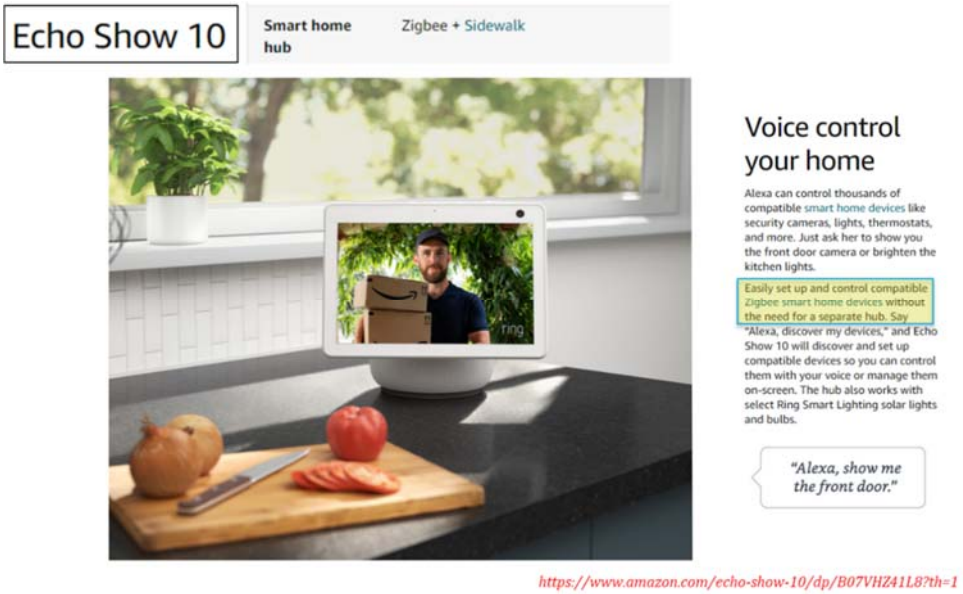
48. The '572 patent involves providing secure wireless local area networks (LAN). A device for securing such a LAN may include a housing with a wireless transceiver carried by the housing. A medium access controller (MAC) also carried by the housing. A cryptography circuit may be connected to the MAC controller and the transceiver. The circuit may encrypt both address and data information by at least adding a plurality of encrypting bits to be transmitted. And the cryptography circuit may decrypt both address and data information upon reception.

49. On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture and sale of smart home devices. For example, Defendant Amazon.com utilizes its subsidiaries, including Defendants Amazon Services, Ring, eero, and Blink, distributors, customers, partners, and retailers to provide smart home devices to

consumers. Amazon's worldwide net sales of its products via online and physical stores in 2020 was $213 billion. *See 2020 Annual Report*, 66.

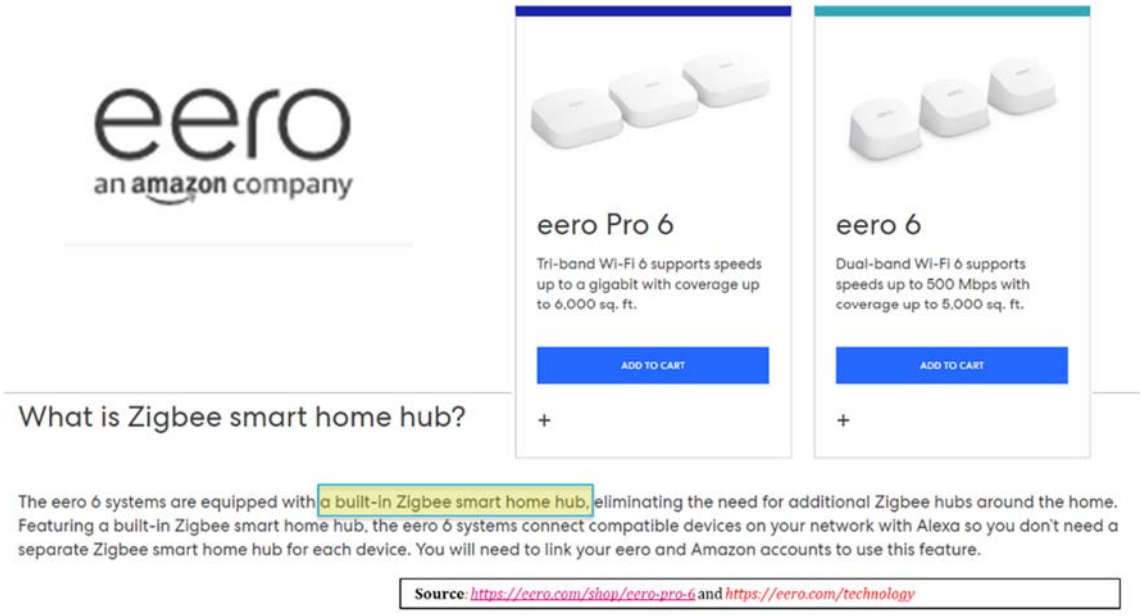
50. Amazon's smart home devices use Wi-Fi, ZigBee, and Z-Wave protocols to enable communication between Amazon smart home devices, and other compatible third-party devices. Amazon further provides software to users, e.g., the Alexa app, to allow users to control such devices across platforms. *See Amazon Echo & Alexa Devices*, AMAZON.COM, https://www.amazon.com/smart-home-devices/b?ie=UTF8&node=9818047011 (last visited May 25, 2021).

51. The Asserted Patents cover wireless communication methods that are incorporated into ZigBee, Wi-Fi, and Z-Wave protocols and the products that utilize them, such as Amazon's smart home devices, their components, and processes related to the same (the "Accused Products"). For example, Amazon's smart home products utilize Wi-Fi, ZigBee and/or Z-Wave protocols. The Accused Products include at least Defendants' Echo, Ring, eero, and Blink brand of devices. Examples of Echo brand devices the utilize the ZigBee protocol include the Echo Show 10 product are shown below:

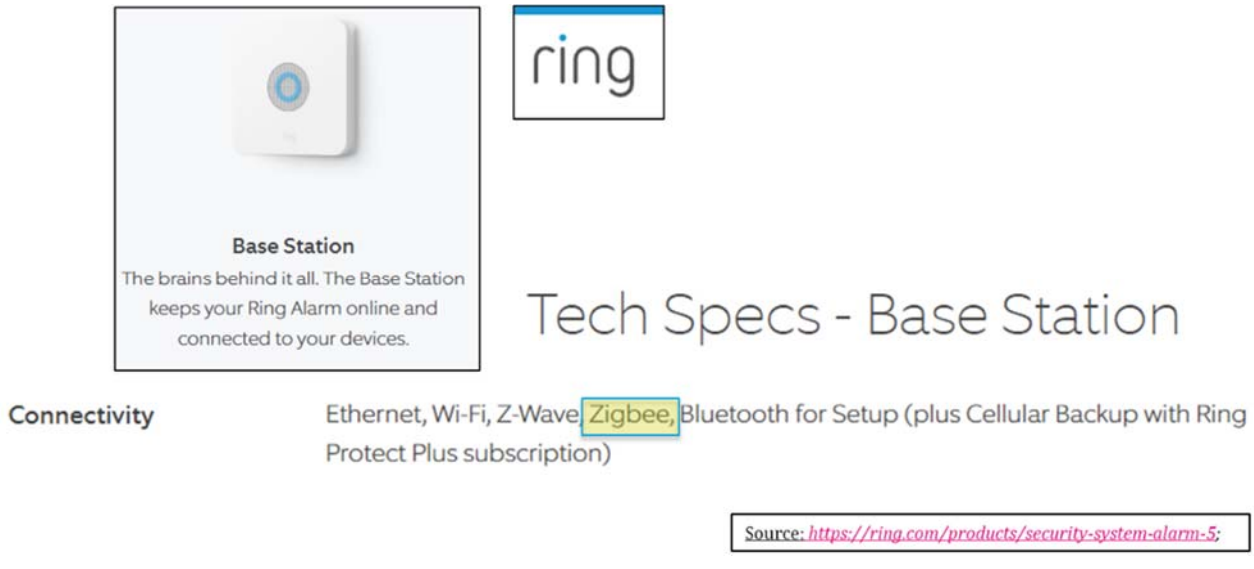


https://www.amazon.com/echo-show-10/dp/B07VHZ41L8?th=1

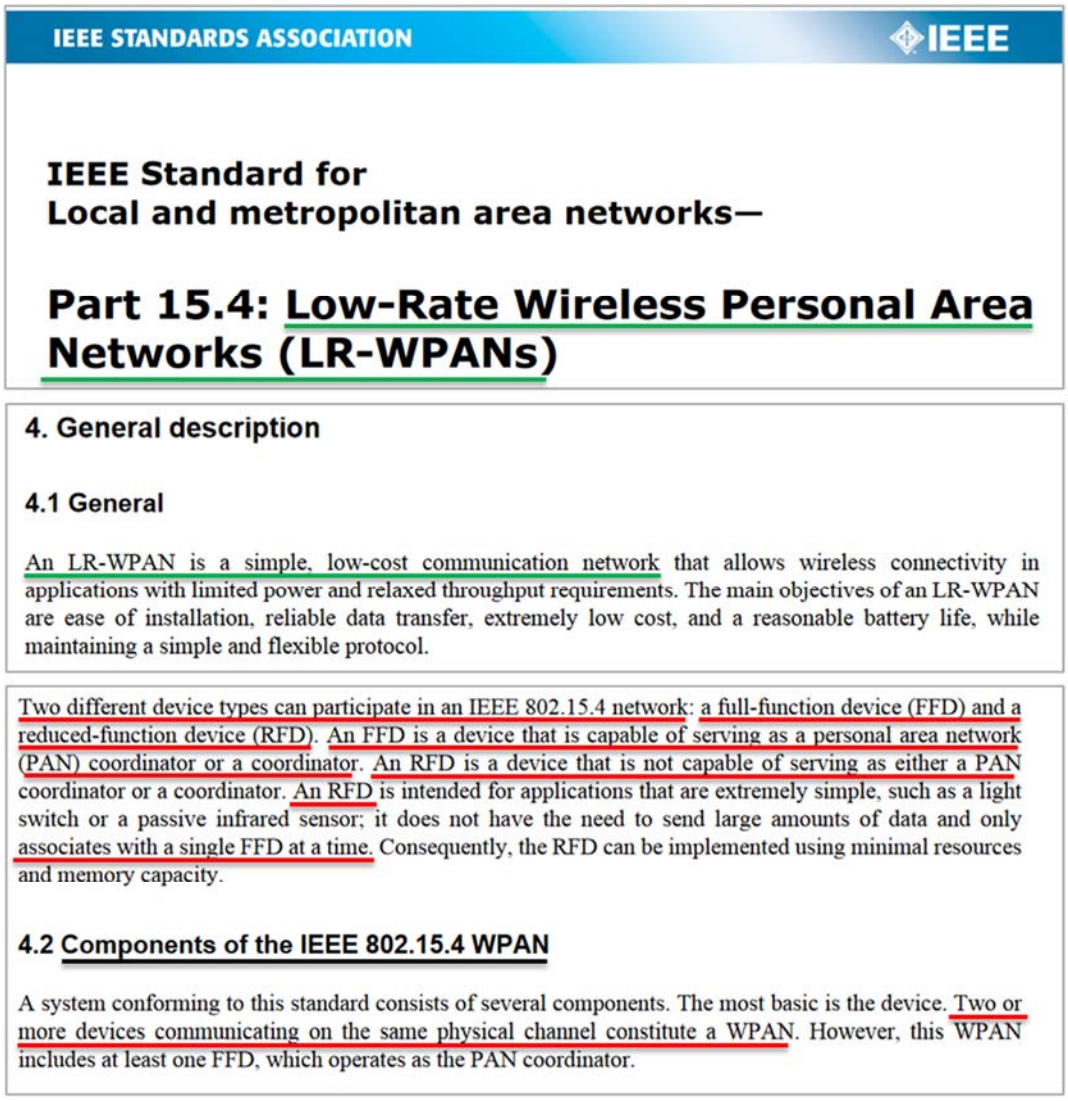
52. Examples of eero-branded products that utilize the ZigBee protocol include the eero Pro 6 and eero 6, as shown below:



53. An example of the Ring-branded products that utilizes the ZigBee protocol includes the Ring Base Station, as shown below:



54. The IEEE 802.15.4 standard based mobile ad-hoc network, utilized by the Accused Products, is a type of Low-Rate Wireless Personal Area Network (LR-WPAN) that allows transmission of data between plurality of network nodes.



IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for
Local and metropolitan area networks—

Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)

4. General description

4.1 General

An LR-WPAN is a simple, low-cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements. The main objectives of an LR-WPAN are ease of installation, reliable data transfer, extremely low cost, and a reasonable battery life, while maintaining a simple and flexible protocol.

Two different device types can participate in an IEEE 802.15.4 network: a full-function device (FFD) and a reduced-function device (RFD). An FFD is a device that is capable of serving as a personal area network (PAN) coordinator or a coordinator. An RFD is a device that is not capable of serving as either a PAN coordinator or a coordinator. An RFD is intended for applications that are extremely simple, such as a light switch or a passive infrared sensor; it does not have the need to send large amounts of data and only associates with a single FFD at a time. Consequently, the RFD can be implemented using minimal resources and memory capacity.

4.2 Components of the IEEE 802.15.4 WPAN

A system conforming to this standard consists of several components. The most basic is the device. Two or more devices communicating on the same physical channel constitute a WPAN. However, this WPAN includes at least one FFD, which operates as the PAN coordinator.

Page 8, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

55. LR-WPAN network allows use of a superframe structure. A superframe is bounded by network beacons sent by the coordinator node and is divided into 16 slots of equal duration. The superframe includes a contention access period (CAP) and a contention free period (CFP), together accounting for the 16 superframe time slots. By default, the network nodes use CAP for data/frame transmission.

4.5 Functional overview

A brief overview of the general functions of a LR-WPAN is given in this subclause.

4.5.1 Superframe structure

This standard allows the optional use of a superframe structure. The format of the superframe is defined by the coordinator. The superframe is bounded by network beacons sent by the coordinator, as illustrated in Figure 4a), and is divided into 16 slots of equal duration. Optionally, the superframe can have an active and an inactive portion, as illustrated in Figure 4b). During the inactive portion, the coordinator is able to enter a low-power mode. The beacon frame transmission starts at the beginning of the first slot of each superframe.

5.1.1.1.1 Contention access period (CAP)

The CAP shall start immediately following the beacon and complete before the beginning of the CFP on a superframe slot boundary. If the CFP is zero length, the CAP shall complete at the end of the active portion of the superframe. The CAP shall be at least *aMinCAPLength*, unless additional space is needed to

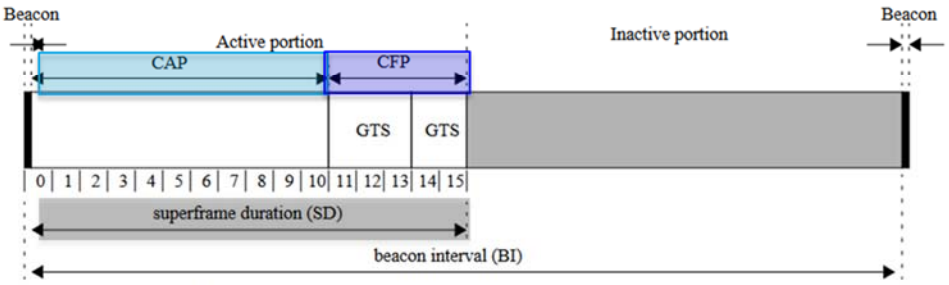


Figure 8—An example of the superframe structure

temporarily accommodate the increase in the beacon frame length needed to perform GTS maintenance, as described in 5.2.2.1.3, and shall shrink or grow dynamically to accommodate the size of the CFP.

All frames, except acknowledgment frames and any data frame that quickly follows the acknowledgment of a data request command, as described in 5.1.6.3, transmitted in the CAP shall use a slotted CSMA-CA mechanism to access the channel. A device transmitting within the CAP shall ensure that its transaction is complete (i.e., including the reception of any acknowledgment) one interframe spacing (IFS) period, as

contention access period: The period of time immediately following a beacon frame during which devices wishing to transmit will compete for channel access using a slotted carrier sense multiple access with collision avoidance mechanism.

Page 12, 19, 20, 4, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

56. In the superframe, the length of the CAP is required to be at least equal to – aMinCAPLength. The PAN coordinator monitors, i.e., a policing node, if a device's request to add a new GTS (e.g., to an existing CFS in the superframe) would result in reduction of the aMinCAPlength. A newly requested GTS lies outside an existing CFP and will be used for transmission by the requesting device.

5.1.7.2 GTS allocation

A device is instructed to request the allocation of a new GTS through the MLME-GTS.request primitive, as described in 6.2.6.1, with GTS characteristics set according to the requirements of the intended application.

On receipt of a GTS request command indicating a GTS allocation request, the PAN coordinator shall first check if there is available capacity in the current superframe, based on the remaining length of the CAP and the desired length of the requested GTS. The superframe shall have available capacity if the maximum number of GTSs has not been reached and allocating a GTS of the desired length would not reduce the length of the CAP to less than *aMinCAPLength*. GTSs shall be allocated on a first-come-first-served basis by the PAN coordinator provided there is sufficient bandwidth available. The PAN coordinator shall make

5.2.2.1.2 Superframe Specification field

The Superframe Specification field shall be formatted as illustrated in Figure 41.

Bits: 0–3	4–7	8–11	12	13	14	15
Beacon Order	Superframe Order	Final CAP Slot	Battery Life Extension (BLE)	Reserved	PAN Coordinator	Association Permit

Figure 41—Format of the Superframe Specification field

The Final CAP Slot field specifies the final superframe slot utilized by the CAP. The duration of the CAP, as implied by this field, shall be greater than or equal to the value specified by *aMinCAPLength*. However, an

aMinCAPLength	The minimum number of symbols forming the CAP. This ensures that MAC commands can still be transferred to devices when GTSs are being used. An exception to this minimum shall be allowed for the accommodation of the temporary increase in the beacon frame length needed to perform GTS maintenance, as described in 5.2.2.1.3.	440

5.1.7.1 CAP maintenance

The PAN coordinator shall preserve the minimum CAP length of *aMinCAPLength* and take preventative action if the minimum CAP is not satisfied. However, an exception shall be allowed for the accommodation

Page 49, 62, 125, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

57. If the new GTS (lying outside the existing CFP) reduces the minimum CAP length of aMinCAPLength, a next higher layer of the coordinator is notified, i.e., generates and intrusion alert, which then takes preventative actions to deallocate one or more of the existing GTSs (forming the existing CFP) in the superframe.

5.1.7.1 CAP maintenance

The PAN coordinator shall preserve the minimum CAP length of *aMinCAPLength* and take preventative action if the minimum CAP is not satisfied. However, an exception shall be allowed for the accommodation of the temporary increase in the beacon frame length needed to perform GTS maintenance. If preventative action becomes necessary, the action chosen is left up to the implementation but may include one or more of the following:

— Limiting the number of pending addresses included in the beacon.
— Not including a payload field in the beacon frame.
— Deallocating one or more of the GTSs.

Figure 32 depicts the message flow for the cases in which a GTS deallocation is initiated by the PAN coordinator.

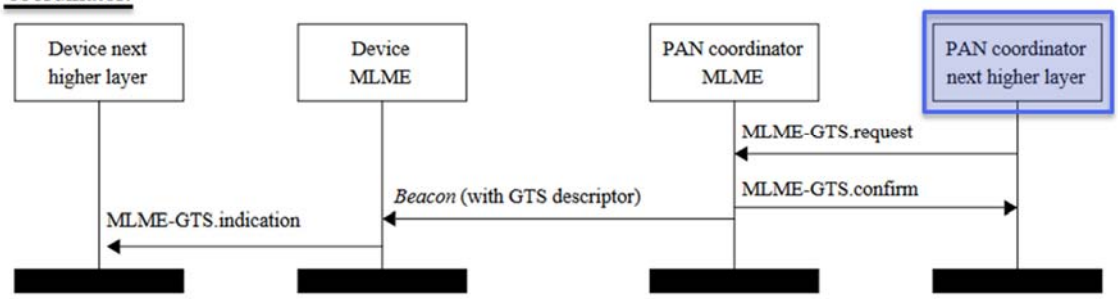


Figure 32—Message sequence chart for GTS deallocation initiated by the PAN coordinator

Page 49, 52, http://ecee.colorado.edu/~liue/teaching/comm_standards/2015S_zigbee/802.15.4-2011.pdf

58. The Accused Products, including Amazon's smart home devices utilizing the ZigBee protocol identified above, also practice a method for dynamic channel allocation in a mobile ad hoc network. As indicated below, "[a] single device can become the Network Channel Manager."

ANNEX E

OPERATING NETWORK MANAGER AS NETWORK CHANNEL MANAGER FOR INTERFERENCE REPORTING AND RESOLUTION

ZigBee Control your world

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

59. As shown below, in different ZigBee Network topologies of the Accused Products, a plurality of network nodes is connected together via a respective plurality communication links.

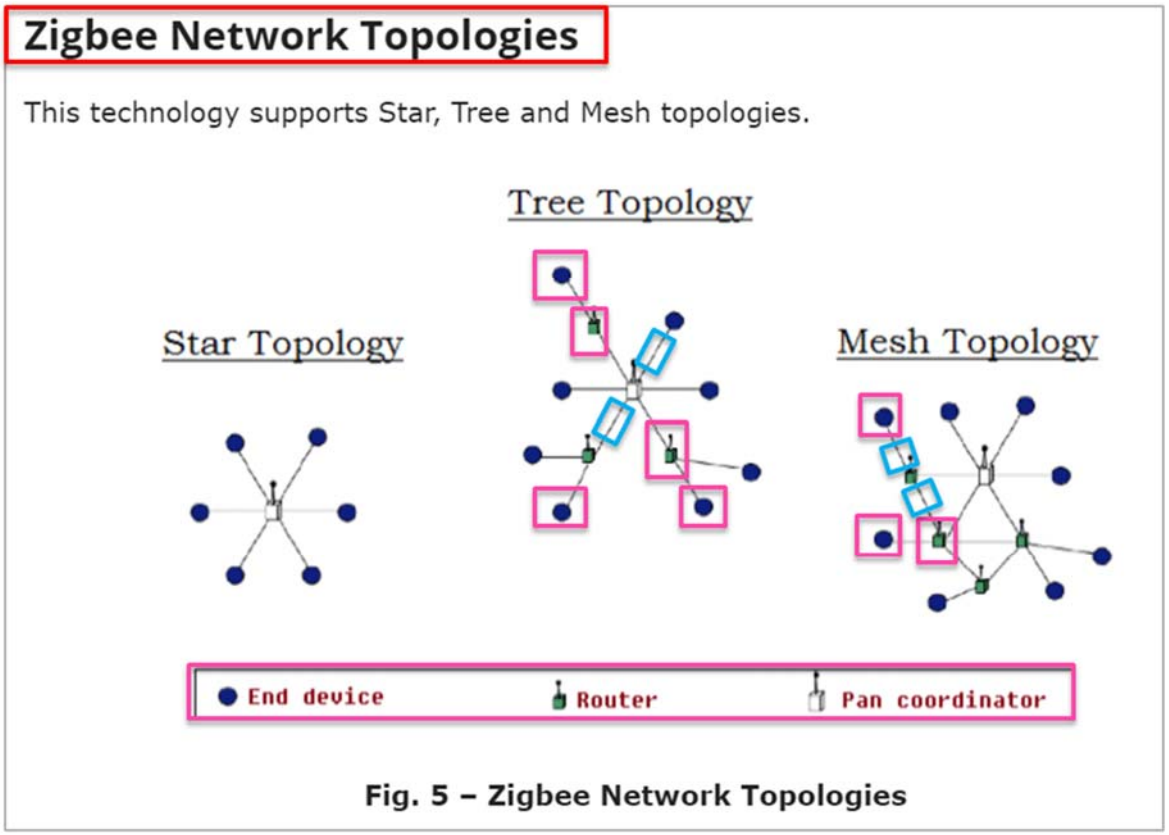
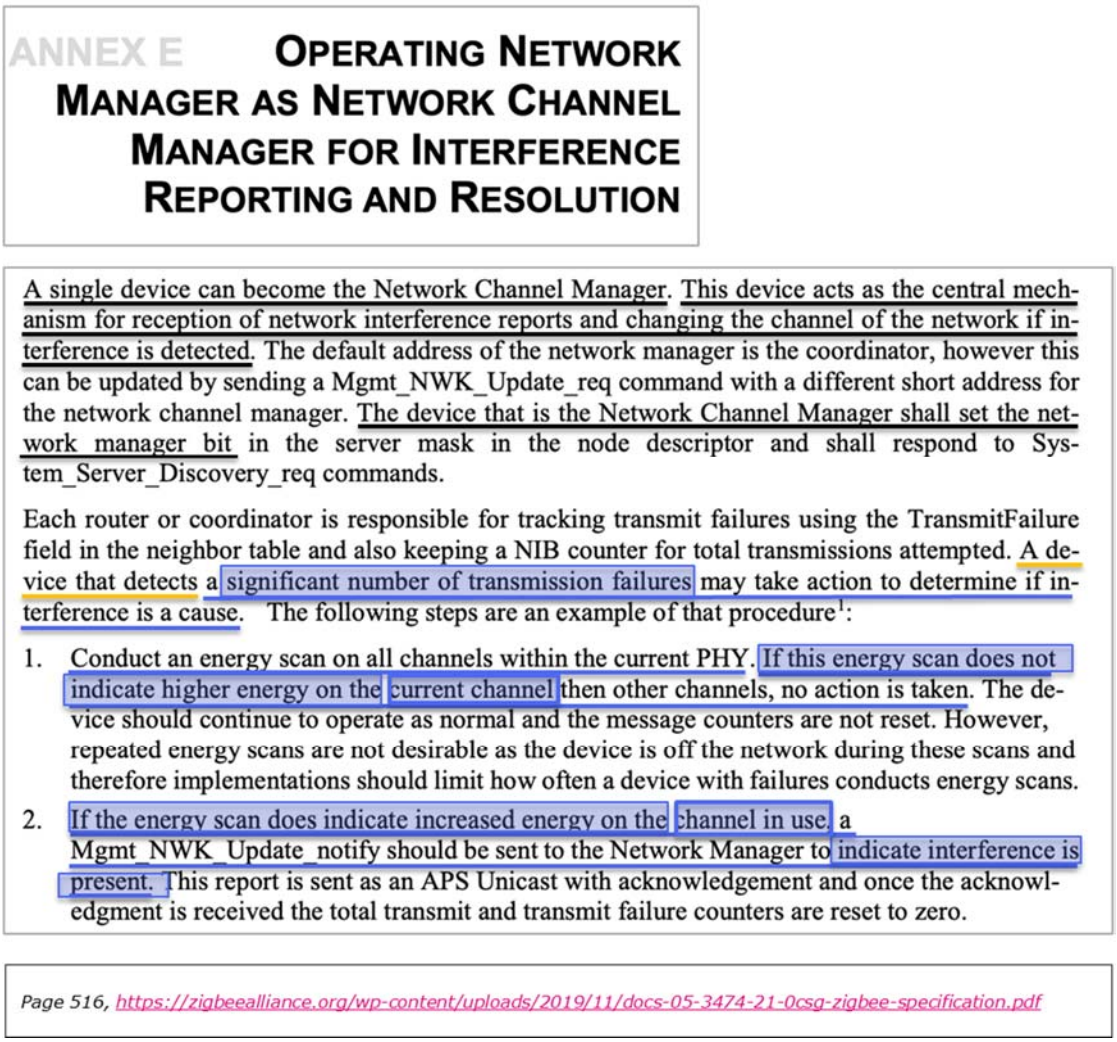


Fig. 5 – Zigbee Network Topologies

https://electricalfundablog.com/zigbee-technology-architecture/

60. In the ZigBee network of the Accused Products, a network device/node is configured to monitor the performance of a channel-in-use based on its energy measurement. As described

below, if the measurement value is higher than the value on other channels (threshold), it indicates interference is present on the channel, consequently resulting in transmission failures.



ANNEX E

OPERATING NETWORK MANAGER AS NETWORK CHANNEL MANAGER FOR INTERFERENCE REPORTING AND RESOLUTION

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network manager bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

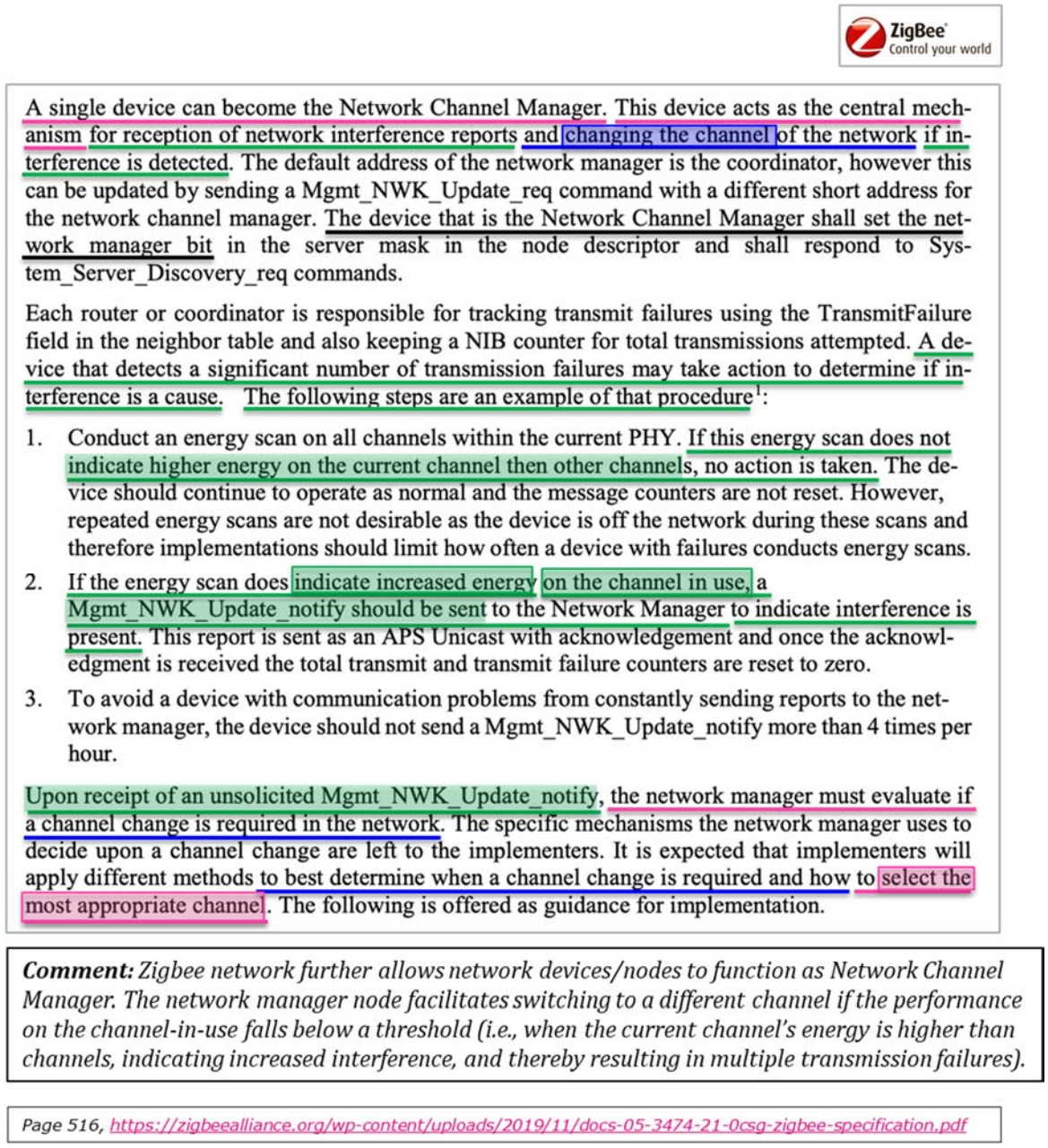
Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

61. As described below, the network manager node facilitates switching to a different channel, i.e., scouting available separate channels, if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating

increased interference, and thereby resulting in multiple transmission failures). The network nodes switch to a new (second) channel whose energy level is lowest or below an acceptable threshold.



ZigBee Control your world

A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated by sending a Mgmt_NWK_Update_req command with a different short address for the network channel manager. The device that is the Network Channel Manager shall set the network_manager_bit in the server mask in the node descriptor and shall respond to System_Server_Discovery_req commands.

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure[1]:

1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans are not desirable as the device is off the network during these scans and therefore implementations should limit how often a device with failures conducts energy scans.
2. If the energy scan does indicate increased energy on the channel in use, a Mgmt_NWK_Update_notify should be sent to the Network Manager to indicate interference is present. This report is sent as an APS Unicast with acknowledgement and once the acknowledgment is received the total transmit and transmit failure counters are reset to zero.
3. To avoid a device with communication problems from constantly sending reports to the network manager, the device should not send a Mgmt_NWK_Update_notify more than 4 times per hour.

Upon receipt of an unsolicited Mgmt_NWK_Update_notify, the network manager must evaluate if a channel change is required in the network. The specific mechanisms the network manager uses to decide upon a channel change are left to the implementers. It is expected that implementers will apply different methods to best determine when a channel change is required and how to select the most appropriate channel. The following is offered as guidance for implementation.

Comment: *Zigbee network further allows network devices/nodes to function as Network Channel Manager. The network manager node facilitates switching to a different channel if the performance on the channel-in-use falls below a threshold (i.e., when the current channel's energy is higher than channels, indicating increased interference, and thereby resulting in multiple transmission failures).*

Page 516, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

62. With reference to the above graphic and as further described below, the ZigBee network of the Accused Products further allows using the command to request interference reports, i.e., broadcasts a channel activity query, from the network nodes, which involves scanning the energy level on all the channels including the newly switched (second) channel. The interference

report will represent determining the performance for the second channel. In addition, the most recent energy level value and failure rate (indicative of the channel performance/activity) corresponding to the channels is stored, i.e., the channel activity is updated.

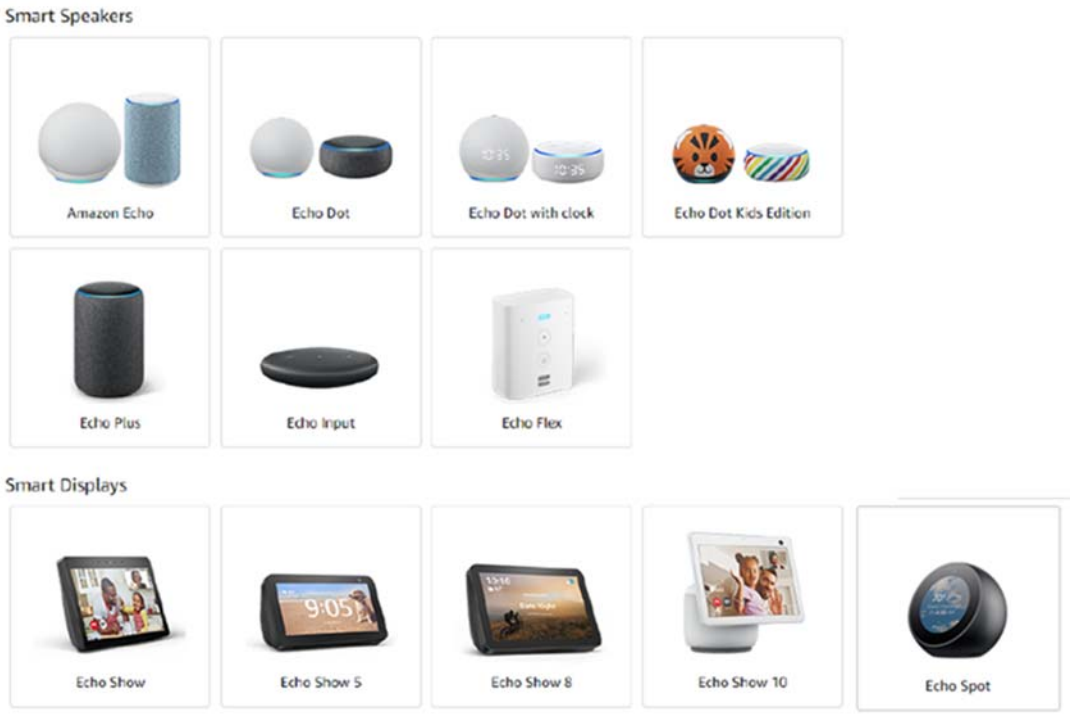
The network manager may do the following:

1. Wait and evaluate if other reports from other devices are received. This may be appropriate if there are no other failures reported. In this case the network manager should add the reporting device to a list of devices that have reported interference. The number of devices on such a list would depend on the size of the network. The network manager can age devices out of this list.
2. Request other interference reports using the Mgmt_NWK_Update_req command. This may be done if other failures have been reported or the network manager device itself has failures and a channel change may be desired. The network manager may request data from the list of devices that have reported interference plus other randomly selected routers in the network. The network manager should not request an update from the device that has just reported interference since this data is fresh already.
3. Upon receipt of the Mgmt_NWK_Update_notify, the network manager shall determine if a channel change is required using whatever implementation specific mechanisms are considered appropriate. The network manager device with just one channel allowed in the *apsChannelMask* parameter must not issue the Mgmt_Nwk_Update_Req command to request other devices to change the current channel. However, the network manager may report channel quality issues to the application.
4. If the above data indicate a channel change should be considered, the network manager completed the following:
   a. Select a single channel based on the Mgmt_NWK_Update_notify based on the lowest energy. This is the proposed new channel. If this new channel does not have an energy level below an acceptable threshold, a channel change should not be done. Additionally, a new channel shall not belong to a PHY different from the one on which a network manager is operating now.
5. Prior to changing channels, the network manager should store the energy scan value as the last energy scan value and the failure rate from the existing channel as the last failure rate. These values are useful to allow comparison of the failure rate and energy level on the previous channel to evaluate if the network is causing its own interference.
6. The network manager should broadcast a Mgmt_NWK_Update_req notifying devices of the new channel. The broadcast shall be to all devices with RxOnWhenIdle equal to TRUE. The network manager is responsible for incrementing the *nwkUpdateId* parameter from the NIB and including it in the Mgmt_NWK_Update_req. The network manager shall set a timer based on the value of *apsChannelTimer* upon issue of a Mgmt_NWK_Update_req that changes channels and shall not issue another such command until this timer expires. However, during this period, the network manager can complete the above analysis. However, instead of changing channels, the network manager would report to the local application using Mgmt_NWK_Update_notify and the application can force a channel change using the Mgmt_NWK_Update_req.

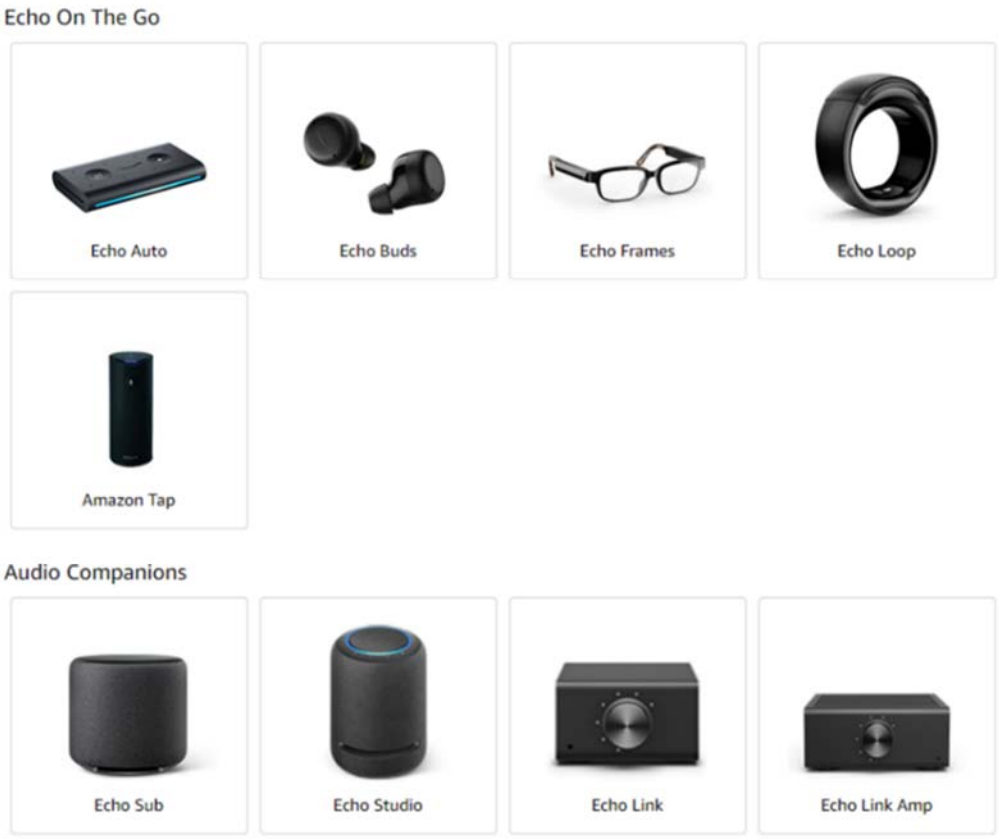
Upon receipt of a Mgmt_NWK_Update_req with a change of channels, the local network manager shall set a timer equal to the *nwkNetworkBroadcastDeliveryTime* and shall switch channels upon expiration of this timer. Each node shall also increment the *nwkUpdateId* parameter and also reset the total transmit count and the transmit failure counters.

Page 517, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf

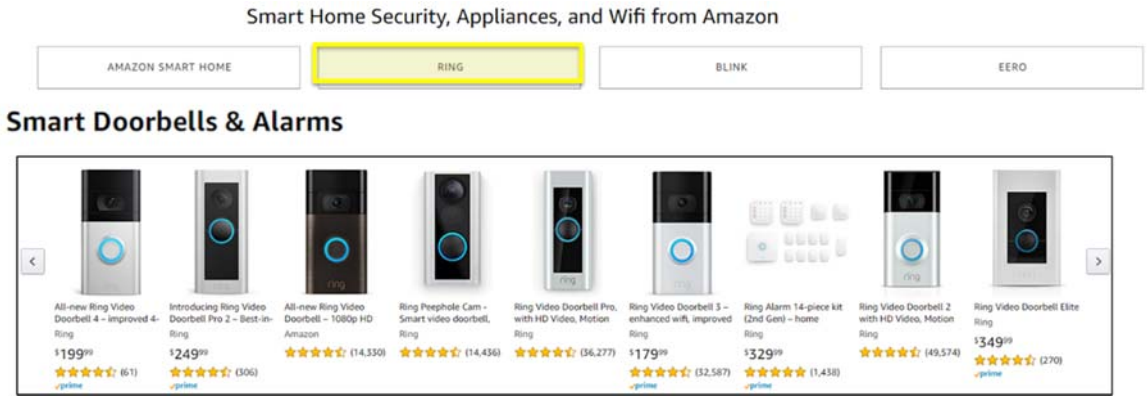
63. The Asserted Patents also cover certain Accused Products that utilize the Wi-Fi protocol (IEEE 802.11). Examples of Echo-branded devices that utilize the Wi-Fi protocol include the following smart speakers and smart displays:



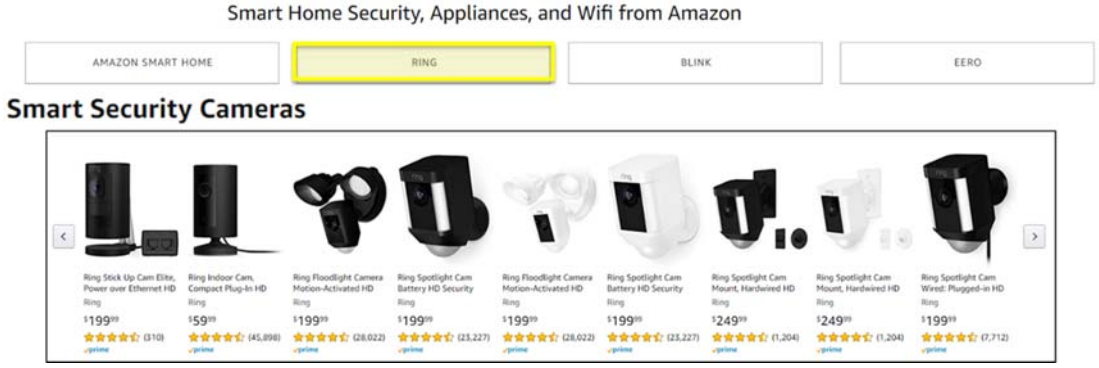
64. Examples of Echo-branded devices that utilize the Wi-Fi protocol include the following Echo On the Go and Audio Companions:



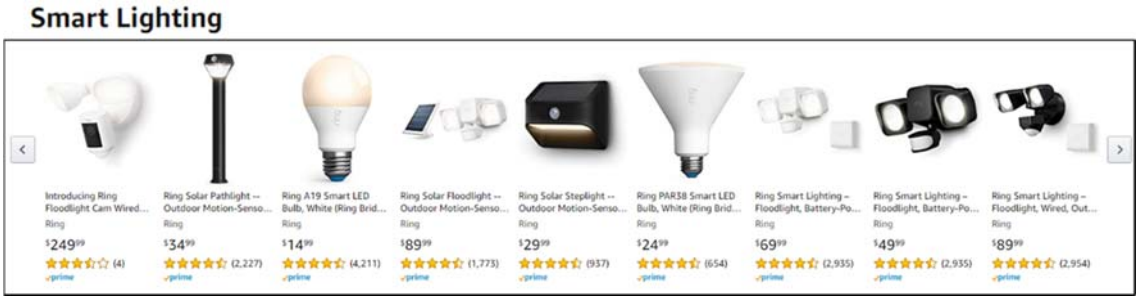
65. Examples of Ring-branded devices that utilize the Wi-Fi protocol include the following smart doorbells and alarms:



66. Examples of Ring-branded devices that utilize the Wi-Fi protocol include the following smart security cameras:



67. Examples of Ring-branded devices that utilize the Wi-Fi protocol include the following smart lighting products:

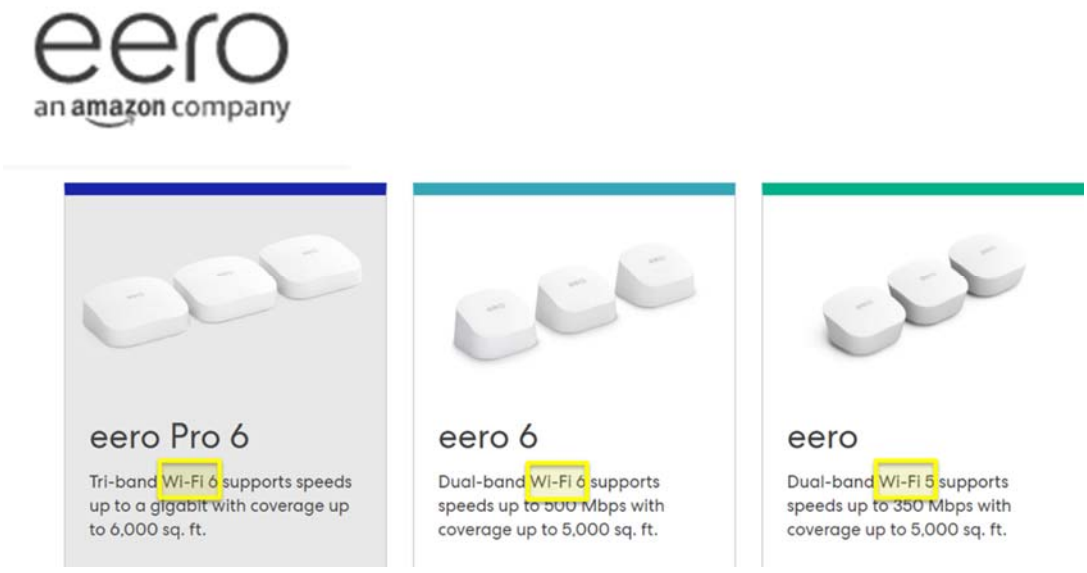


68. Ring's lighting products utilize a Ring bridge for network communication using the Wi-Fi protocol, as indicated below:

69. Examples of Blink-branded devices that utilize the Wi-Fi protocol include the following smart home security cameras:

Source: *https://www.amazon.com/Blink-Outdoor-Wireless-Security-Camera/dp/B086DKSYTS?ref_=ast_sto_dp&th=1*

70. Examples of eero-branded devices that utilize the Wi-Fi protocol include the following smart home security cameras:



Source: *https://eero.com/shop/eero-pro-6* and *https://eero.com/technology*

71. The Accused Products include an intrusion detection method for a local or metropolitan area. As described below, the IEEE 802.11 WEP utilized by the Accused Products utilize a TKIP that includes a "MIC" defend against active attacks.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

72. Stations (STAs) in an IEEE 802.11 network of the Accused Products associate with each other using a robust security network association (RSNA). As described below, RSNA supports intrusion detection by employing authentication mechanisms and data frame protection mechanisms (such as, temporal key integrity protocol - TKIP) between the STAs. Data is

exchanged between the STAs in the form of MPDUs (medium access control (MAC) protocol data units). The MAC frame (MPDU) comprises a MSDU (information frame) in the frame body, and four addresses that identify, among others, source MAC address (SA) and destination MAC address (DA) for the MSDU.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

5.1.1.4 Interaction with other IEEE 802® layers

IEEE Std 802.11 is required to appear to higher layers [logical link control (LLC)] as a wired IEEE 802 LAN. This requires that the IEEE 802.11 network handle STA mobility within the MAC sublayer. To meet reliability assumptions (that LLC makes about lower layers), it is necessary for IEEE Std 802.11 to incorporate functionality that is untraditional for MAC sublayers.

In a robust security network association (RSNA), IEEE Std 802.11 provides functions to protect data frames, IEEE Std 802.1X-2004 provides authentication and a Controlled Port, and IEEE Std 802.11 and IEEE Std 802.1X-2004 collaborate to provide key management. All STAs in an RSNA have a corresponding IEEE 802.1X entity that handles these services. This standard defines how an RSNA utilizes IEEE Std 802.1X-2004 to access these services.

3.126 robust security network (RSN): A security network that allows only the creation of robust security network associations (RSNAs). An RSN can be identified by the indication in the RSN information element (IE) of Beacon frames that the group cipher suite specified is not wired equivalent privacy (WEP).

3.127 robust security network association (RSNA): The type of association used by a pair of stations (STAs) if the procedure to establish authentication or association between them includes the 4-Way Handshake. Note that the existence of an RSNA by a pair of devices does not of itself provide robust security. Robust security is provided when all devices in the network use RSNAs.

5.2.3.2 RSNA

An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- Enhanced authentication mechanisms for STAs
- Key management algorithms
- Cryptographic key establishment
- An enhanced data cryptographic encapsulation mechanism, called Counter mode with Cipher-block chaining Message authentication code Protocol (CCMP), and, optionally, Temporal Key Integrity Protocol (TKIP).

Page 72, 61, 75 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

73. In the TKIP protocol of the Accused Products, an MSDU transmitter STA calculates cryptographic message integrity code (MIC) using the MAC addresses (SA & DA) corresponding

to the MSDU. As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is verified/authenticated at the receiver. MSDUs with invalid MICs are discarded and countermeasures are invoked.

8.3 RSNA data confidentiality protocols

8.3.1 Overview

This standard defines two RSNA data confidentiality and integrity protocols: TKIP and CCMP. Implementation of CCMP shall be mandatory in all IEEE 802.11 devices claiming RSNA compliance. Implementation of TKIP is optional for an RSNA. A design aim for TKIP was that the algorithm should be implementable within the capabilities of most devices supporting only WEP, so that many such devices would be field-upgradeable by the supplier to support TKIP.

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1 TKIP overview

The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

a) A transmitter calculates a keyed cryptographic message integrity code (MIC) over the MSDU SA and DA, the MSDU priority (see 8.3.2.3), and the MSDU plaintext data. TKIP appends the computed MIC to the MSDU data prior to fragmentation into MPDUs. The receiver verifies the MIC after decryption, ICV checking, and defragmentation of the MPDUs into an MSDU and discards any received MSDUs with invalid MICs. TKIP's MIC provides a defense against forgery attacks.

b) Because of the design constraints of the TKIP MIC, it is still possible for an adversary to compromise message integrity; therefore, TKIP also implements countermeasures. The countermeasures bound the probability of a successful forgery and the amount of information an attacker can learn about a key.

Page 213, 214 https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

74. The TKIP MIC implementation of the Accused Products prevents intrusion attacks, such as, message redirection by modifying destination/receiver MAC address (DA or RA) and impersonation by modifying the source/transmitter MAC address (SA or TA). As described below, the transmission is monitored if the MIC (which is obtained using the MAC addresses) is

verified/authenticated at the receiver. MSDU with an invalid MIC will indicate a modified MAC address (SA or DA), thereby resulting in discarding the MSDU and invoking the countermeasures.

8.3.2.3 TKIP MIC

Flaws in the IEEE 802.11 WEP design cause it to fail to meet its goal of protecting data traffic content from casual eavesdroppers. Among the most significant WEP flaws is the lack of a mechanism to defeat message forgeries and other active attacks. To defend against active attacks, TKIP includes a MIC, named Michael. This MIC offers only weak defenses against message forgeries, but it constitutes the best that can be achieved with the majority of legacy hardware. TKIP uses different MIC keys depending on the direction of the transfer as described in 8.6.1 and 8.6.2.

Annex H contains an implementation of the TKIP MIC. It also provides test vectors for the MIC.

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates. Active attacks enabled by the original WEP design include the following:

- Bit-flipping attacks
- Data (payload) truncation, concatenation, and splicing
- Fragmentation attacks
- Iterative guessing attacks against the key
- Redirection by modifying the MPDU DA or RA field
- Impersonation attacks by modifying the MPDU SA or TA field

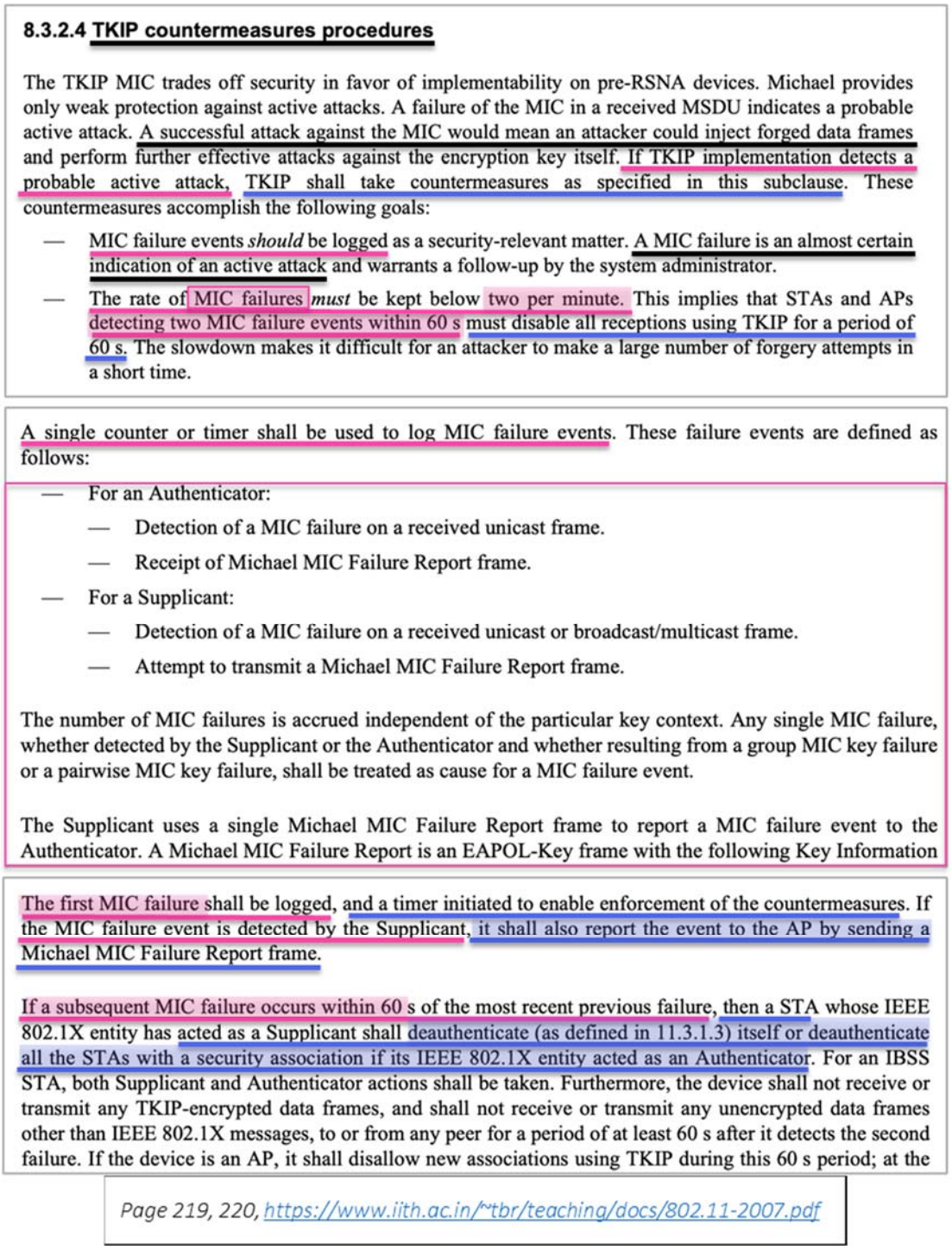
The MIC makes it more difficult for any of these attacks to succeed.

All of these attacks remain at the MPDU level with the TKIP MIC. The MIC, however, applies to the MSDU, so it blocks successful MPDU-level attacks. TKIP applies the MIC to the MSDU at the transmitter and verifies it at the MSDU level at the receiver. If a MIC check fails at the MSDU level, the implementation shall discard the MSDU and invoke countermeasures (see 8.3.2.4).

Page 217, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

75. Upon detecting a first MIC failure, as described below, a countermeasure timer is initiated, and a failure event (alert) is reported to the AP by sending a Michael MIC Failure Report frame. Upon detecting a second consecutive MIC failure within 60 seconds, i.e., detecting a number of failed attempts, the participating STAs are deauthenticated, wherein deauthentication

involves sending a notification (i.e., generating an alert) to deauthenticate due to an intrusion (2 consecutive MIC failures has occurred).



8.3.2.4 TKIP countermeasures procedures

The TKIP MIC trades off security in favor of implementability on pre-RSNA devices. Michael provides only weak protection against active attacks. A failure of the MIC in a received MSDU indicates a probable active attack. A successful attack against the MIC would mean an attacker could inject forged data frames and perform further effective attacks against the encryption key itself. If TKIP implementation detects a probable active attack, TKIP shall take countermeasures as specified in this subclause. These countermeasures accomplish the following goals:

— MIC failure events *should* be logged as a security-relevant matter. A MIC failure is an almost certain indication of an active attack and warrants a follow-up by the system administrator.

— The rate of MIC failures *must* be kept below two per minute. This implies that STAs and APs detecting two MIC failure events within 60 s must disable all receptions using TKIP for a period of 60 s. The slowdown makes it difficult for an attacker to make a large number of forgery attempts in a short time.

A single counter or timer shall be used to log MIC failure events. These failure events are defined as follows:

— For an Authenticator:
  — Detection of a MIC failure on a received unicast frame.
  — Receipt of Michael MIC Failure Report frame.
— For a Supplicant:
  — Detection of a MIC failure on a received unicast or broadcast/multicast frame.
  — Attempt to transmit a Michael MIC Failure Report frame.

The number of MIC failures is accrued independent of the particular key context. Any single MIC failure, whether detected by the Supplicant or the Authenticator and whether resulting from a group MIC key failure or a pairwise MIC key failure, shall be treated as cause for a MIC failure event.

The Supplicant uses a single Michael MIC Failure Report frame to report a MIC failure event to the Authenticator. A Michael MIC Failure Report is an EAPOL-Key frame with the following Key Information

The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. For an IBSS STA, both Supplicant and Authenticator actions shall be taken. Furthermore, the device shall not receive or transmit any TKIP-encrypted data frames, and shall not receive or transmit any unencrypted data frames other than IEEE 802.1X messages, to or from any peer for a period of at least 60 s after it detects the second failure. If the device is an AP, it shall disallow new associations using TKIP during this 60 s period; at the

Page 219, 220, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

76. The Asserted Patents also cover Amazon's Wi-Fi compliant devices, which support WPA and WPA2-AES security mechanisms, as described below. Of the WPA and WPA2 security

mechanism used by the Accused Products, such as Amazon's smart home Wi-Fi devices, the WPA is based on Temporal Key Integrity Protocol (TKIP), while, as described below, the WPA2-AES is based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below is an exemplary IEEE 802.11 complaint Amazon Echo device/station (STA). The device has a housing.

Legal Notices for Echo (4th Generation), Echo Dot (4th Generation), and Echo Dot with Clock (2nd Generation)

Notices for System Software

==========

**** Component: wpa_supplicant - IEEE 802.1X, WPA, WPA2, RSN, IEEE 802.11i

Source: https://www.amazon.com/gp/help/customer/display.html?nodeId=GNTC79KDZV3HRUEE

77. As shown below, the Accused Products provide 2.4 GHz and 5 GHz Wi-Fi speeds. This capability ascertains the presence of a Wi-Fi antenna and transceiver in the device.

Wifi connectivity	Dual-band wifi supports 802.11a/b/g/n/ac (2.4 and 5 GHz) networks. Does not support connecting to ad-hoc (or peer-to-peer) wifi networks.

https://www.amazon.com/dp/B085HK4KL6?ref=MarsFS_AUCC_lr

78. Shown below is a block diagram of TKIP (used with WPA) based cryptography circuit utilized in the Accused Products. The circuit shown encrypts both address (destination address (DA), source address (SA)) and data information (plaintext MSDU) by adding encryptions

bits (MIC key) to both the address and data. The cryptography circuit of the Accused Products is also configured to decrypt the encrypted address and data information.

IEEE Std 802.11™-2007
(Revision of
IEEE Std 802.11-1999)

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1.1 TKIP cryptographic encapsulation

TKIP enhances the WEP cryptographic encapsulation with several additional functions, as depicted in Figure 8-4.

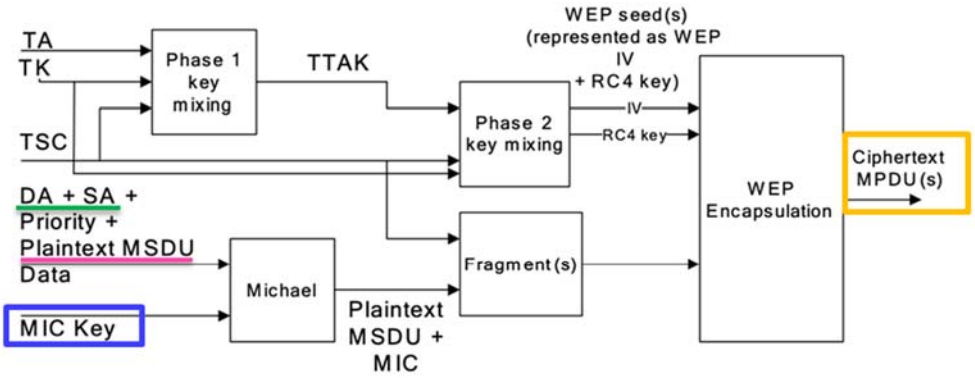


Figure 8-4—TKIP encapsulation block diagram

a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC.

b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 8.3.2.2).

c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.

d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 7.1.3.6), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key.

Page 213, 214, https://www.iith.ac.in/~tbr/teaching/docs/802.11-2007.pdf

COUNT I

(INFRINGEMENT OF U.S. PATENT NO. 7,082,117)

79. Plaintiff incorporates paragraphs 1 through 78 herein by reference.

80. Plaintiff is the assignee of the '117 patent, entitled "Mobile ad-hoc network with intrusion detection features and related methods," with ownership of all substantial rights in the '117 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

81. The '117 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '117 patent issued from U.S. Patent Application No. 10/217,097.

82. Amazon has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '117 patent in this District and elsewhere in Texas and the United States.

83. On information and belief, Amazon designs, develops, manufactures, assembles, and markets smart home devices configured to utilize ZigBee, Z-Wave, and Wi-Fi protocols such as the Accused Products, including via Amazon.com's subsidiaries, such as Defendants Amazon Services, Ring, eero, and Blink, affiliates, partners, distributors, retails, customers, and consumers.

84. Amazon directly infringes the '117 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '117 patent to, for example, its alter egos, agents, intermediaries, distributors, importers, customers, subsidiaries, affiliates, and/or consumers. Furthermore, on information and belief, Amazon sells and makes the Accused Products outside of the United States, delivers those products to its customers, distributors, and/or subsidiaries in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby

directly infringing the '117 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

85. Furthermore, Amazon directly infringes the '117 patent through its direct involvement in the activities of its subsidiaries, including Amazon Services, Ring, eero, and Blink, including by selling and offering for sale the Accused Products in the U.S. directly for Amazon.com and importing the Accused Products into the United States for Amazon.com. On information and belief, Amazon's subsidiaries and affiliates conduct activities that constitutes direct infringement of the '117 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products. Amazon is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendants Amazon Services, Ring, eero, and Blink (under both the alter ego and agency theories) because, as an example and on information and belief, Amazon.com, Amazon Services, Ring, eero, and Blink are essentially the same company. Amazon.com has the right and ability to control other subsidiaries' infringing acts (including those activities of Amazon Services, Ring, eero, and Blink) and receives a direct financial benefit from their infringement.

86. For example, Amazon infringes claim 24 of the '117 patent via the Accused Products such as Amazon Echo (4th Gen), Echo Show 10 (3rd Gen), eero 6 systems, Ring home security products, e.g., base station, keypad, contact sensors, motion detectors, range extender, flood & freeze sensor, smoke & CO listener, panic button, which utilize the ZigBee protocol.

87. Those Accused Products include "[a] mobile ad-hoc network (MANET)"

comprising the limitations of claim 24. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include a plurality of nodes for transmitting data therebetween, said plurality of nodes intermittently operating in a contention-free mode during contention-free periods (CFPs) and in a contention mode outside CFPs; and a policing node for detecting intrusions into the MANET by monitoring transmissions among said plurality of nodes to detect contention-free mode operation outside of a CFP; and generating an intrusion alert based upon detecting contention-free mode operation outside a CFP.

88. At a minimum, Amazon has known of the '117 patent at least as early as the filing date of this complaint. In addition, Amazon has known about the '117 patent since at least its receipt of a letter from Harris Corporation ("Harris") dated May 2, 2018, regarding infringement of Harris' patent portfolio. The letter specifically references the '117 patent and notifies Amazon of its infringing use of "wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standard," in at least the Amazon Echo Plus product.

89. On information and belief, since at least the above-mentioned date when Amazon was on notice of its infringement, Amazon has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '117 patent to directly infringe one or more claims of the '117 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Amazon does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '117 patent. On information and belief, Amazon intends

to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing ZigBee and Z-Wave protocol features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *ZigBee: Connect Your Devices Locally Using Zigbee*, AMAZON ALEXA, https://developer.amazon.com/en-US/alexa/devices/connected-devices/development-resources/zigbee (last visited May 25, 2021).

90. On information and belief, despite having knowledge of the '117 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '117 patent, Amazon has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Amazon's infringing activities relative to the '117 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

91. Stingray has been damaged as a result of Amazon's infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to Stingray in an amount that adequately compensates Stingray for Amazon's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

(INFRINGEMENT OF U.S. PATENT NO. 7,224,678)

92. Plaintiff incorporates paragraphs 1 through 91 herein by reference.

93. Plaintiff is the assignee of the ’678 patent, entitled “Wireless local or metropolitan area network with intrusion detection features and related methods,” with ownership of all substantial rights in the ’678 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

94. The ’678 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The ’678 patent issued from U.S. Patent Application No. 10/217,042.

95. Amazon has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’678 patent in this District and elsewhere in Texas and the United States.

96. On information and belief, Amazon designs, develops, manufactures, assembles, and markets smart home devices configured to utilize ZigBee, Z-Wave, and Wi-Fi protocols such as the Accused Products, including via Amazon.com’s subsidiaries, such as Defendants Amazon Services, Ring, eero, and Blink, affiliates, partners, distributors, retails, customers, and consumers.

97. Amazon directly infringes the ’678 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the ’678 patent to, for example, its alter egos, agents, intermediaries, distributors, importers, customers, subsidiaries, affiliates, and/or consumers. Furthermore, On information and belief, Amazon sells and makes the Accused Products outside of the United States, delivers those products to its customers,

distributors, and/or subsidiaries in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby directly infringing the '678 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

98. Furthermore, Amazon directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries, including Amazon Services, Ring, eero, and Blink, including by selling and offering for sale the Accused Products in the U.S. directly for Amazon.com and importing the Accused Products into the United States for Amazon.com. On information and belief, Amazon's subsidiaries and affiliates conduct activities that constitutes direct infringement of the '678 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products. Amazon is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendants Amazon Services, Ring, eero, and Blink (under both the alter ego and agency theories) because, as an example and on information and belief, Amazon.com, Amazon Services, Ring, eero, and Blink are essentially the same company. Amazon.com has the right and ability to control other subsidiaries' infringing acts (including those activities of Amazon Services, Ring, eero, and Blink) and receives a direct financial benefit from their infringement.

99. For example, Amazon infringes claim 51 of the '678 patent via its Accused Products that utilize the Wi-Fi protocols. Ring's alarm systems utilize the Wi-Fi communication protocols

to control and monitor security sensors, such as keypads, contact sensors, motion detectors, range extenders, flood and freeze sensors, smoke and CO listeners, and panic buttons. Other Ring-branded products that utilize the Wi-Fi protocol include smart doorbells and alarms, smart security cameras, and smart lighting. Amazon's Echo brand products utilize Wi-Fi communication protocols, including smart speakers, smart displays, smart streaming devices, that when coupled with voice-controls, such as Amazon's Alexa application, allow customers to control other Amazon and third-party smart home devices, including smart plugs, cameras, lights, and appliances. eero-branded products provide home mesh Wi-Fi. And Blink-branded products include smart home security cameras that utilize the Wi-Fi protocol.

100. Those Accused Products include "[a]n intrusion detection method for a wireless local or metropolitan area network comprising a plurality of stations" comprising the limitations of claim 51. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include the steps of transmitting data between the plurality of stations using a media access layer (MAC), each of the stations having a respective MAC address associated therewith; monitoring transmissions among the plurality of stations to detect failed attempts to authenticate MAC addresses; and generating an intrusion alert based upon detecting a number of failed attempts to authenticate a MAC address.

101. At a minimum, Amazon has known of the '678 patent at least as early as the filing date of this complaint. In addition, Amazon has known about infringement of Harris Corporation's ("Harris") patent portfolio, which includes the '678 patent, since at least its receipt of a letter from Harris dated May 2, 2018. The letter notifies Amazon of its infringing use of "wireless

communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standard," in at least the Amazon Echo Plus product.

102. On information and belief, since at least the above-mentioned date when Amazon was on notice of its infringement, Amazon has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '678 patent to directly infringe one or more claims of the '678 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Amazon does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. On information and belief, Amazon intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing ZigBee and Wi-Fi protocol features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *ZigBee: Connect Your Devices Locally Using Zigbee*, AMAZON ALEXA, https://developer.amazon.com/en-US/alexa/devices/connected-devices/development-resources/zigbee (last visited May 25, 2021).

103. On information and belief, despite having knowledge of the '678 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '678 patent,

Amazon has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Amazon's infringing activities relative to the '678 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

104. Stingray has been damaged as a result of Amazon's infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to Stingray in an amount that adequately compensates Stingray for Amazon's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

(INFRINGEMENT OF U.S. PATENT NO. 7,440,572)

105. Plaintiff incorporates paragraphs 1 through 104 herein by reference.

106. Plaintiff is the assignee of the '572 patent, entitled "Secure wireless LAN device and associated methods," with ownership of all substantial rights in the '572 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

107. The '572 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '572 patent issued from U.S. Patent Application No. 09/760,619.

108. Amazon has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '572 patent in this District and elsewhere in Texas and the United States.

109. On information and belief, Amazon designs, develops, manufactures, assembles, and markets smart home devices configured to utilize ZigBee, Z-Wave, and Wi-Fi protocols such as the Accused Products, including via Amazon.com's subsidiaries, such as Defendants Amazon Services, Ring, eero, and Blink, affiliates, partners, distributors, retails, customers, and consumers.

110. Amazon directly infringes the '572 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '572 patent to, for example, its alter egos, agents, intermediaries, distributors, importers, customers, subsidiaries, affiliates, and/or consumers. Furthermore, On information and belief, Amazon sells and makes the Accused Products outside of the United States, delivers those products to its customers, distributors, and/or subsidiaries in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby directly infringing the '572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

111. Furthermore, Amazon directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries, including Amazon Services, Ring, eero, and Blink, including by selling and offering for sale the Accused Products in the U.S. directly for Amazon.com and importing the Accused Products into the United States for Amazon.com. On information and belief, Amazon's subsidiaries and affiliates conduct activities that constitutes

direct infringement of the '572 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products. Amazon is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendants Amazon Services, Ring, eero, and Blink (under both the alter ego and agency theories) because, as an example and on information and belief, Amazon.com, Amazon Services, Ring, eero, and Blink are essentially the same company. Amazon.com has the right and ability to control other subsidiaries' infringing acts (including those activities of Amazon Services, Ring, eero, and Blink) and receives a direct financial benefit from their infringement.

112. For example, Amazon infringes claim 1 of the '572 patent via its Accused Products that utilize Wi-Fi protocols. Ring's alarm systems utilize the Wi-Fi communication protocols to control and monitor security sensors, such as keypads, contact sensors, motion detectors, range extenders, flood and freeze sensors, smoke and CO listeners, and panic buttons. Other Ring-branded products that utilize the Wi-Fi protocol include smart doorbells and alarms, smart security cameras, and smart lighting. Amazon's Echo brand products utilize Wi-Fi communication protocols, including smart speakers, smart displays, smart streaming devices, that when coupled with voice-controls, such as Amazon's Alexa application, allow customers to control other Amazon and third-party smart home devices, including smart plugs, cameras, lights, and appliances. eero-branded products provide home mesh Wi-Fi. And Blink-branded products include smart home security cameras that utilize the Wi-Fi protocol.

113. Those Accused Products include "[a] secure wireless local area network (LAN) device" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include a housing; a wireless transceiver carried by said

housing; a medium access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver for encrypting both address and data information for transmission by at least adding a plurality of encrypting bits to both the address and the data information, and for decrypting both the address and the data information upon reception.

114. Amazon further infringes the '572 patent via 35 U.S.C. § 271(g) by selling, offering to sell, and/or importing IoT and smart home devices, their components, and/or products containing same, that are made by a process covered by the '572 patent. On information and belief, the infringing IoT and smart home devices, their components, and/or products containing same are not materially changed by subsequent processes, and they are neither trivial nor nonessential components of another product.

115. Amazon further infringes based on the importation, sale, offer for sale, or use of the Accused Products that are made from a process covered by the '572 patent. To the extent that Plaintiff made reasonable efforts to determine whether the patented processes of the '572 patent were used in the production of the Accused Products but was not able to so determine, the Accused Products should be presumed by this Court to have been so made, pursuant to 35 U.S.C. § 295.

116. At a minimum, Amazon has known of the '572 patent at least as early as the filing date of this complaint. In addition, Amazon has known about the '572 patent since at least its receipt of a letter from Harris Corporation ("Harris") dated May 2, 2018, regarding infringement of Harris' patent portfolio. The letter specifically references the '572 patent and notifies Amazon of its infringing use of "wireless communication networks, network management/security, as well

as innovations pertinent to the IEEE 802 and Zigbee standard," in at least the Amazon Echo Plus product.

117. On information and belief, since at least the above-mentioned date when Amazon was on notice of its infringement, Amazon has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '572 patent to directly infringe one or more claims of the '572 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Amazon does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '572 patent. On information and belief, Amazon intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing ZigBee and Wi-Fi protocol features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *ZigBee: Connect Your Devices Locally Using Zigbee*, AMAZON ALEXA, https://developer.amazon.com/en-US/alexa/devices/connected-devices/development-resources/zigbee (last visited May 25, 2021).

118. On information and belief, despite having knowledge of the '572 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '572 patent,

Amazon has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Amazon's infringing activities relative to the '572 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

119. Stingray has been damaged as a result of Amazon's infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to Stingray in an amount that adequately compensates Stingray for Amazon's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV

(INFRINGEMENT OF U.S. PATENT NO. 7,616,961)

120. Plaintiff incorporates paragraphs 1 through 119 herein by reference.

121. Plaintiff is the assignee of the '961 patent, entitled "Allocating channels in a mobile ad hoc network," with ownership of all substantial rights in the '961 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

122. The '961 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '961 patent issued from U.S. Patent Application No. 10/134,862.

123. Amazon has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '961 patent in this District and elsewhere in Texas and the United States.

124. On information and belief, Amazon designs, develops, manufactures, assembles, and markets smart home devices configured to utilize ZigBee, Z-Wave, and Wi-Fi protocols such as the Accused Products, including via Amazon.com's subsidiaries, such as Defendants Amazon Services, Ring, eero, and Blink, affiliates, partners, distributors, retails, customers, and consumers.

125. Amazon directly infringes the '961 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '961 patent to, for example, its alter egos, agents, intermediaries, distributors, importers, customers, subsidiaries, affiliates, and/or consumers. Furthermore, on information and belief, Amazon sells and makes the Accused Products outside of the United States, delivers those products to its customers, distributors, and/or subsidiaries in the United States, or in the case that it delivers the Accused Products outside of the United States it does so intending and/or knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby directly infringing the '961 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

126. Furthermore, Amazon directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries, including Amazon Services, Ring, eero, and Blink, including by selling and offering for sale the Accused Products in the U.S. directly for Amazon.com and importing the Accused Products into the United States for Amazon.com. On information and belief, Amazon's subsidiaries and affiliates conduct activities that constitutes

direct infringement of the '961 patent under 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing those Accused Products. Amazon is vicariously liable for this infringing conduct of its subsidiaries and affiliates, including Defendants Amazon Services, Ring, eero, and Blink (under both the alter ego and agency theories) because, as an example and on information and belief, Amazon.com, Amazon Services, Ring, eero, and Blink are essentially the same company. Amazon.com has the right and ability to control other subsidiaries' infringing acts (including those activities of Amazon Services, Ring, eero, and Blink) and receives a direct financial benefit from their infringement.

127. For example, Amazon infringes claim 1 of the '961 patent via the Accused Products such as Amazon Echo (4th Gen), Echo Show 10 (3rd Gen), eero 6 systems, Ring home security products, e.g., base station, keypad, contact sensors, motion detectors, range extender, flood & freeze sensor, smoke & CO listener, panic button, which utilize the ZigBee protocol.

128. Those Accused Products include a "method for dynamic channel allocation in a mobile ad hoc network comprising a plurality of wireless mobile nodes and a plurality of wireless communication links connecting the plurality of wireless mobile nodes together over a plurality of separate channels at different frequencies" comprising the limitations of claim 1. The technology discussion above and the example Accused Products provide context for Plaintiff's allegations that each of those limitations are met. For example, the Accused Products include the steps of at each node, monitoring link performance on a first channel, link performance being based upon at least one quality of service (QoS) threshold; at each node, scouting one or more other available separate channels at different frequencies when the monitored link performance on the first channel falls below the QoS threshold by at least switching to a second separate channel at a different frequency, broadcasting a channel activity query to determine link performance for the second separate

channel, and processing replies to the channel activity query to determine the link performance for the second separate channel; and at each node, updating respective channel activity for the first and second separate channels at different frequencies based upon the processed replies.

129. At a minimum, Amazon has known of the '961 patent at least as early as the filing date of this complaint. In addition, Amazon has known about infringement of Harris Corporation's ("Harris") patent portfolio, which includes the '961 patent, since at least its receipt of a letter from Harris dated May 2, 2018. The letter notifies Amazon of its infringing use of "wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standard," in at least the Amazon Echo Plus product.

130. On information and belief, since at least the above-mentioned date when Amazon was on notice of its infringement, Amazon has actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, or sell the Accused Products that include or are made using all of the limitations of one or more claims of the '961 patent to directly infringe one or more claims of the '961 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Amazon does so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '961 patent. On information and belief, Amazon intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing

ZigBee and Z-Wave protocol features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g.*, *ZigBee: Connect Your Devices Locally Using Zigbee*, AMAZON ALEXA, https://developer.amazon.com/en-US/alexa/devices/connected-devices/development-resources/zigbee (last visited May 25, 2021).

131. On information and belief, despite having knowledge of the '961 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '961 patent, Amazon has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Amazon's infringing activities relative to the '961 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

132. Stingray has been damaged as a result of Amazon's infringing conduct described in this Count. Each Defendant is thus, jointly and severally, liable to Stingray in an amount that adequately compensates Stingray for Amazon's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

133. Plaintiff is entitled to recover from Defendants the damages sustained by Plaintiff as a result of Defendants' wrongful acts in an amount subject to proof at trial, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court.

134. Plaintiff has incurred and will incur attorneys' fees, costs, and expenses in the prosecution of this action. The circumstances of this dispute may give rise to an exceptional case within the meaning of 35 U.S.C. § 285, and Plaintiff is entitled to recover its reasonable and

necessary attorneys' fees, costs, and expenses.

JURY DEMAND

135. Plaintiff hereby requests a trial by jury pursuant to Rule 38 of the Federal Rules of Civil Procedure.

PRAYER FOR RELIEF

136. Plaintiff requests that the Court find in its favor and against Defendants, and that the Court grant Plaintiff the following relief:

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;
3. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
5. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
6. Such other and further relief as the Court deems just and equitable.

Dated: June 1, 2021

Respectfully submitted,

/s/ Jeffrey R. Bragalone by permission Wesley Hill

Jeffrey R. Bragalone (lead attorney)
Texas Bar No. 02855775
Terry A. Saad
Texas Bar No. 24066015
Marcus Benavides
Texas Bar No. 24035574
Hunter S. Palmer
Texas Bar No. 24080748
BRAGALONE OLEJKO SAAD PC
2200 Ross Avenue
Suite 4600W
Dallas, TX 75201
Tel: (214) 785-6670
Fax: (214) 785-6680
jbragalone@bosfirm.com
tsaad@bosfirm.com
mbenavides@bosfirm.com
hpalmer@bosfirm.com

Wesley Hill
Texas Bar No. 24032294
WARD, SMITH, & HILL, PLLC
P.O. Box 1231
Longview, TX 75606
Tel: (903) 757-6400
Fax: (903) 757-2323
wh@wsfirm.com

ATTORNEYS FOR PLAINTIFF STINGRAY IP SOLUTIONS, LLC