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

| | | |
|---|---|---|
| STINGRAY IP SOLUTIONS LLC,<br><br>Plaintiff,<br><br>v.<br><br>LEEDARSON IOT TECHNOLOGY INC., and LEEDARSON LIGHTING CO. LTD.,<br><br>Defendants. | §<br>§<br>§<br>§<br>§<br>§<br>§<br>§<br>§<br>§<br>§<br>§ | CIVIL ACTION NO. _____<br><br>JURY TRIAL DEMANDED |

**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 Leedarson IoT Technology Inc. and Leedarson Lighting Co. Ltd. (collectively, "Defendants" or "Leedarson") for infringement of U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No. 7,440,572 (the "'572 patent"), U.S. Patent No. 7,441,126 (the "'126 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 Leedarson IoT Technology Inc. ("Leedarson IoT") is a public company organized under the laws of China, with its principal place of business and registered office located at 1511 Second Fanghu North Road, Xiamen, Fujian, 361010 China. Leedarson IoT may be served via its agents and its alter egos, including, for example, Leedarson America Inc ("Leedarson America"), a Georgia corporation having registered agent Zhiping Chen, 300 Technology Ct SE, Suite 100, Smyrna, GA, 30082, USA; and AiDot Inc. ("AiDot"), a

California corporation, having registered agent Runfu Zhang, 8605 Santa Monica Blvd #30327, West Hollywood, CA 90069, USA.

3. On information and belief, Defendant Leedarson Lighting Co. Ltd., Inc. ("Leedarson Lighting") is a company organized under the laws of China, with its principal place of business and registered office located at 1511 Second Fanghu North Road, Xiamen, Fujian, 361010 China. Leedarson IoT and Leedarson Lighting share the same world headquarters in Xiamen, China. Moreover, Leedarson Lighting is, directly or indirectly, a wholly owned and controlled subsidiary of Leedarson IoT. Leedarson Lighting may be served via its agents and its alter egos, including, for example, Leedarson IOT; Leedarson America Inc, a Georgia corporation having registered agent Zhiping Chen, 300 Technology Ct SE, Suite 100, Smyrna, GA, 30082, USA; and AiDot Inc., a California corporation, having registered agent Runfu Zhang, 8605 Santa Monica Blvd #30327, West Hollywood, CA 90069, USA.

4. Leedarson IoT was originally incorporated in China in 2000 as Leedarson Lighting Group Co. Ltd. and was renamed to Leedarson IoT Technology Inc. in 2019. Leedarson specializes in the "R&D and production of Internet of Things (IoT) products consisting of sensors, controls, cameras, and home appliances, along with connected and non-connected LED bulbs, fixtures, luminaires, light sources, and more." *See About,* LEEDARSON, https://www.leedarson.com/about-leedarson.

5. Leedarson states that, "As a world-leading IoT solution provider, Leedarson partners with businesses to help them design, manufacture, test, certify, package, kit and deliver extraordinary IoT devices and end-to-end IoT services to empower every aspect within the home and commercial building. We apply our honed expertise to help fuel an intelligent world, leveraging multi-protocol standards, platforms and ecosystems to ensure IoT device

interoperability." *Id*. at p. 2. Leedarson further states that they provide "Connected Modules for the IoT devices with full range of wireless technologies, including Wi-Fi, Bluetooth, Zigbee and Z-Wave." *See Connected Modules,* LEEDARSON, https://www.leedarson.com/products/connected-modules.

6. Leedarson states that Leedarson IoT "owns two smart production bases that cover a total area of 430,000m² and integrate a self-built, vertical supply chain covering key components, final assembly and packaging worldwide. Together, the two bases contain hundreds of automated production lines that produce tens of millions of units per month." *See Manufacturing Capabilities,* LEEDARSON, https://www.leedarson.com/about/manufacturing-capabilities. Indeed, in 2020, Leedarson established a "Thailand Manufacturing Base to expand manufacturing capabilities abroad." *See Milestones,* LEEDARSON, https://www.leedarson.com/about/milestones. According to Leedarson, "the company has formed long-term and stable cooperative relations with many internationally renowned channel vendors and brand vendors and has become an important partner of world-renowned vendors such as The Home Depot, IKEA, and Amazon, and has been awarded the 'Best Partner of the Year,' 'Best Quality Award,' 'Best Global Supplier Award,' and other honors by core customers including the Home Depot and IKEA. The above-mentioned companies are leading companies in their respective fields, and their suppliers are strictly screened. That the company is selected as one of their major suppliers of LED lighting and Internet of Things products fully demonstrates the comprehensive recognition of the company's product development, design capabilities, production capabilities, and product reliability. In addition, the company has resident teams in the United States, Germany, Japan, and other countries which can better provide customers with high-quality, fast response and localized service advantages. Through long-term cooperation with many high-quality customers in the industry, the company has an in-depth

understanding of the needs of different customers and can fully understand and comprehend the individual needs of customers." *See 2022 Annual Report of Lidaxin IoT Technology Co., Ltd.,* available for download at http://static.sse.com.cn/disclosure/listedinfo/announcement/c/new/2023-04-26/605365_20230426_4IIC.pdf – Translated to English by Google Translate (last visited July 24, 2023) [hereinafter "Leedarson Annual Report"]. Leedarson products, including products sold by their subsidiaries, are (i) manufactured outside the U.S. and then imported into the United States or (ii) manufactured inside the U.S. and distributed, and sold to end-users via the internet, brick-and-mortar stores and/or via dealers in the U.S., in Texas and the Eastern District of Texas.

7. On information and belief, Leedarson operates its IoT business through various business segments and brands, including AiDot. *Id.* at 184. "Building Solutions North America designs, sells, installs and services HVAC, controls, building management, refrigeration, integrated electronic security and integrated fire-detection and suppression systems for commercial, industrial, retail, small business, institutional and governmental customers in the United States and Canada. Building Solutions North America also provides energy efficiency solutions and technical services, including inspection, scheduled maintenance, and repair and replacement of mechanical and controls systems, as well as data-driven 'smart building' solutions, to non-residential building and industrial applications in the United States and Canadian marketplace." *Id.* "Global Products designs, manufactures and sells HVAC equipment, controls software and software services for residential and commercial applications to commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide. In addition, Global Products designs, manufactures and sells refrigeration equipment and controls globally. The Global Products business also designs, manufactures and sells fire protection, fire

suppression and security products, including intrusion security, anti-theft devices, access control, and video surveillance and management systems, for commercial, industrial, retail, residential, small business, institutional and governmental customers worldwide." *Id.* at 102-03.

8. On information and belief, Leedarson maintains a corporate presence in the United States, including in Texas and in this District, via at least making, using, importing, offering to sale, and/or selling Leedarson products in or into the United States, including, for example, on behalf of, in conjunction with, for and/or via customers in the United States and Leedarson's alter egos, related entities and/or wholly controlled U.S.-based subsidiaries, including Leedarson America, AiDot, Doyen Inc. ("Doyen"), Anshe Innovation Co. ("Anshe"), Welove Life Inc. ("Welove"), Homax Link Inc. ("Homax Link"), and/or Syvio Technology Inc. ("Syvio"). *See Leedarson Annual Report,* p. 185. Yongchuan Li is the CEO, CFO and Secretary of Leedarson America (per the Georgia Secretary of State's Corporations Division website) and is also a founder, officer, third largest shareholder, Vice Chairman and Deputy General Manager of the Defendant Leedarson IoT (per Leedarson IoT's 2022 Annual Report). On behalf and for the benefit of Defendants, Leedarson IoT, including via its shared executive Yongchuan Li, engages in, controls, orders, provides for, induces, jointly participates in, and/or coordinates the importation, distribution, marketing, offers for sale, sale, and use of the Leedarson products in the U.S. For example, Leedarson IoT maintains distribution and support channels in the U.S. for Leedarson products via online stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *See Leedarson Annual Report,* p. 16; *Contact Us*, LEEDARSON.COM, https://www.leedarson.com/support/contact-us (accessible via menu "Support" and link for "Contact Us,") (last visited Sep. 27, 2023).

9. As a result, via at least Leedarson's established distribution channels operated and maintained by at least Defendant Leedarson IoT, Leedarson Lighting and Leedarson's U.S. based subsidiaries, including, at least, wholly controlled Leedarson America and AiDot, Leedarson products are distributed, sold, advertised, and used nationwide, including being sold to consumers via Leedarson dealers operating in Texas and this District. Thus, Defendants do business in the United States, the State of Texas, and in this District.

## JURISDICTION AND VENUE

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

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

### A. Defendant Leedarson IoT

12. On information and belief, Leedarson IoT 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 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, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. For example, Leedarson IoT is related to, owns, and/or controls subsidiaries, businesses, and/or brands (including Leedarson America,

AiDot, Anshe, Arnoo, Welove, Homax, Linkind, Orein, MuJoy, Winees, Syvio, Enhulk, ganiza, Hyderson, GoGonova) that have a significant business presence in the U.S. and in Texas. Such a presence furthers the development, design, manufacture, importation, distribution, sale, and use (including by inducement) of infringing Leedarson products in Texas, including in this District.

13. This Court has personal jurisdiction over Defendant Leedarson IoT, directly and/or through the activities of Leedarson IoT's alter egos, intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of Defendant Leedarson Lighting, other members, segments, companies and/or brands of Leedarson, and U.S. based subsidiaries. Through direction and control of these entities, Leedarson IoT has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Leedarson IoT would not offend traditional notions of fair play and substantial justice.

14. On information and belief, Leedarson IoT controls or otherwise directs and authorizes all activities of its alter egos, subsidiaries and related entities, including, but not limited to Defendant Leedarson Lighting, and other alter egos, members, segments, companies and/or brands of Leedarson, for example, Leedarson America and AiDot. *See, e.g., See Contact Us*, LEEDARSON.COM, https://www.leedarson.com/support/contact-us (showcasing the primary contact for Leedarson IoT in America as Leedarson America Inc.) (last visited Sep. 27, 2023); *Leedarson Annual Report,* p. 184-186 (disclosing 100% ownership of numerous American companies). Directly via its alter egos and/or agents in the U.S. and via at least distribution partners, retailers, reseller partners, dealers, professional installers, and other service providers, Leedarson IoT has placed and continues to place infringing Leedarson products into the U.S. stream of commerce.

Examples include the manufacture and/or importation of Leedarson products in and into the United States. *See Leedarson Annual Report,* p. 15-16. Leedarson IoT 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)).

15. On information and belief, Leedarson IoT utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including providing links via its own website to online stores, retailers, vendors, resellers, distributors, and/or dealers offering such products and related services for sale. *See Leedarson Annual Report,* p. 16 ("[Leedarson] has become an important partner of world-renowned vendors such as The Home Depot, IKEA and Amazon, and has been awarded the "Best Partner of the Year" [and] "Best Global Supplier Award" by core customers such as [The] Home Depot and IKEA"); *Products*, LEEDARSON, https://www.leedarson.com/products/smart-living-products (accessible in the United States for sales inquiries) (last visited Oct. 6, 2023); *Deliver Peace of Mind to Your Customers*, LEEDARSON, https://www.leedarson.com/solutions/smart-living-solution (last visited Oct. 6, 2023) (Under the heading "*One-Stop IoT Solution,*" stating that "We offer a multitude of products and services to prevent you having to deal with multiple suppliers." Under the heading "*Seamless Connectivity,*" stating that "We support direct

connections between hardware, access gateways or cloud solutions to enable interoperability across most IoT devices and systems." Under the heading "*Data Analysis Service,*" stating that "Our experts help you optimize your sales channels and improve your products through unmatched statistical analysis." Under the heading "*Value-Added Service,*" stating that "Grow your business and expand service offerings by utilizing LEEDARSON's value-added subscription, financial reports and/or payment services to bolster visibility into business and IT successes." Under the heading "*After-Sale Service,*" stating that "Ensure sales and drive loyalty programs by providing good after-sales services, including user feedback, maintenance service, knowledge base, etc."). Leedarson products and/or services have been sold from and/or in both brick-and-mortar and/or online retail stores within this District and in Texas, with examples being, at least, The Home Depot, nationwide dealers or distributors, and nationwide online retailers. *See., e.g., 60-Watt Equivalent Smart A19 Color Changing CEC LED Light Bulb with Voice Control (1-Bulb) Powered by Hubspace,* HOME DEPOT, https://www.homedepot.com/p/EcoSmart-60-Watt-Equivalent-Smart-A19-Color-Changing-CEC-LED-Light-Bulb-with-Voice-Control-1-Bulb-Powered-by-Hubspace-11A19060WRGBWH1/318411935 (last visited Oct. 9, 2023) (Being offered for sale to individuals in zip code 75024 in Plano, Collin County, Texas in the Eastern District of Texas and being assigned Model # 11A19060WRGBWH1 and Item # 1006931917). Additionally, Leedarson products, including infringing products and/or services, are sold nationwide, in Texas and this District via, for example, direct sales, online retailers, Leedarson's subsidiary AiDot, and/or under Leedarson brands such as OREIN. *See, e.g. OREiN Matter Smart Light Bulbs Reliable WiFi Bulb with A19 E26 LED Color Changing 60W Equi 800LM CRI>90 Work Alexa/Google Home/Apple Home/SmartThings/Siri 2Pack*, AMAZON.COM, *https://www.amazon.com/-/es/OREiN-Matter-Smart-Light-Blulbs/dp/B0BLTWFJWY?th=1* (showing a "Model Name" of "OS0100811267" sold

by "OREiN-US" with "Country of Origin" being "China" and using "Connectivity Technology" that includes "Wi-Fi") (last visited Oct. 6, 2023); *OREiN-US Seller Page*, AMAZON.COM, https://www.amazon.com/sp?ie=UTF8&seller=A3UO4V3GPIKR2L&asin=B0BLTWFJWY&ref=dp_merchant_link&isAmazonFulfilled=1 (listing "Detailed Seller Information" for "OREiN-US" including "Business name: Syvio Technology CO., Limited" and "Business Address: Room A, 8/F,Kwok Cheung Building" on "635-637 Shanghai Street" in "HK," signifying Hong Kong, China, with postal code "999077"); *Operation Manual for OSO100811267 Wi-Fi Smart Light Bulb user manual Syvio Technology Limited*, OREIN, https://fccid.io/2AZR9OS0100811267/Users-Manual/User-Manual-6376472 (showing the Operation Manual for the OREIN brand "Wi-Fi Smart Light Bulb" with Model name "OSO100811267," which states "Made in China," "Manufacturer: Leedarson IoT Technology Inc.," and "Adress: No.1511, 2nd Fanghu North Rd, Hull District, Xiamen, China") (last visited Oct. 6, 2023); *Who We Are*, AiDot, https://www.aidot.com/about-us (last visited Oct. 6, 2023) (listing brands of Aidot including OREiN, Syvio, ganiza, Hyderson, MuJoy, Welov, GoGonova, Winees, Linkind, and Enhulk); *Smart Bulb*, AIDOT, https://www.aidot.com/products/smart-lights/bulbs.html (selling numerous Wi-Fi enabled smart bulb products that are available in Texas and in this district via the internet). Leedarson IoT, via its wholly owned and controlled subsidiaries, also provides application software ("apps") for download and use in conjunction with and as a part of the wireless communication network that connects Leedarson products and other network devices. *See, e.g., Control Your Smart Living arbitrarily : Smart Home App,* AIDOT, https://www.aidot.com/blog/post/smart-home-app (last visited Sep. 29, 2023) ("AiDot is a popular smart home app with tons of powerful functions. Currently, it supports many smart home devices including smart light bulb, security camera, and smart home appliance, and the scale of its

connectable smart devices is still increasing."). These apps are available via digital distribution platforms operated, for example, by Apple Inc. and Google for download by users and execution on smartphone devices. *Id*.

16. Based on Leedarson IoT's connections and relationship with its U.S. subsidiaries, manufacturers, dealers, retailers, and digital distribution platforms, Leedarson IoT knows that Texas is a termination point of the established distribution channel, namely online and brick-and-mortar stores offering Leedarson products and related services and software to third-party manufacturers, distribution partners, retailers (including national retailers), reseller partners, dealers, service providers, consumers, and other users in Texas. Leedarson IoT, 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").

17. On information and belief, Leedarson IoT alone and in concert with other related entities such as Defendant Leedarson Lighting, and subsidiaries, and members, segments, companies and/or brands of Leedarson, manufactures and purposefully places infringing Leedarson products in established distribution channels in the stream of commerce, including in Texas, via third-party manufacturers, distributors, dealers, and reseller partners, such as at least those operating online and/or those listed on Leedarson's website. As an example, Leedarson IoT imports Leedarson products to Texas directly and/or through a related entity or subsidiary and directly sells and offers for sale infringing Leedarson products in Texas to resellers or dealers. For example, EcoSmart light bulbs are offered for sale and pickup at least at a Home Depot store

located in this District at 4600 State Hwy 121, Plano, TX 75024. *See., e.g., 60-Watt Equivalent Smart A19 Color Changing CEC LED Light Bulb with Voice Control (1-Bulb) Powered by Hubspace,* HOME DEPOT, https://www.homedepot.com/p/EcoSmart-60-Watt-Equivalent-Smart-A19-Color-Changing-CEC-LED-Light-Bulb-with-Voice-Control-1-Bulb-Powered-by-Hubspace-11A19060WRGBWH1/318411935 (last visited Oct. 9, 2023) (Being offered for sale to individuals in zip code 75024 in Plano, Collin County, Texas in the Eastern District of Texas and being assigned Model # 11A19060WRGBWH1 and Item # 1006931917). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and/or sell Leedarson products and/or related services, such as consultation and installation, via their own websites to U.S. consumers, including to consumers in Texas and this District. Based on Leedarson IoT's connections and relationship, including supply contracts and other agreements with the U.S. and Texas-based suppliers, distributors, dealers, and/or resellers, such as at least The Home Depot and Lowe's, Leedarson IoT knows and has known that Texas is a termination point of the established distribution channels for Leedarson products. Leedarson IoT, alone and in concert with subsidiaries Defendant Leedarson Lighting, and U.S.-based Members, segments, companies and/or brands of Leedarson has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this additional basis. *See Ultravision Technologies, LLC v. Holophane Europe Limited*, 2020 WL 3493626, at *5 (E.D. Tex. 2020) (finding sufficient to make a *prima facie* showing of personal jurisdiction allegations that "Defendants either import the products to Texas themselves or through a related entity"); *see also Bench Walk Lighting LLC v. LG Innotek Co., Ltd et al.*, Civil Action No. 20-51-RGA, 2021 WL 65071, at *7-8 (D. Del., Jan. 7, 2021) (denying motion to dismiss for lack of personal jurisdiction based on the foreign defendant entering into supply contract with U.S. distributor and the

distributor sold and shipped defendant's products from the U.S. to the a customer in the forum state).

18. In the alternative, this Court has personal jurisdiction over Leedarson IoT under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, Leedarson IoT is not subject to the jurisdiction of the courts of general jurisdiction of any state, and exercising jurisdiction over Leedarson IoT is consistent with the U.S. Constitution.

19. Venue is proper in this District with respect to Defendant Leedarson IoT, for example, pursuant to 28 U.S.C. § 1391. Defendant Leedarson IoT is a foreign entity and may be sued in any district under 28 U.S.C. § 1391(c). *See also In re HTC Corporation*, 889 F.3d 1349, 1357 (Fed. Cir. 2018) ("The Court's recent decision in *TC Heartland* does not alter" the alien-venue rule.).

**B. Defendant Leedarson Lighting.**

20. On information and belief, Defendant Leedarson Lighting 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 partners, alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, Leedarson Lighting and parent Defendant Leedarson IoT and Leedarson IoT's U.S.-

based direct and/or indirect subsidiaries, and members, segments, companies and/or brands of Leedarson manufacture, import, distribute, offer for sale, sell, and induce infringing use of Leedarson products to distribution partners, retailers (including national retailers), resellers, dealers, service providers, consumers, and other users.

21. On information and belief, this Court has personal jurisdiction over Leedarson Lighting, directly and/or indirectly via the activities of Leedarson Lighting's alter egos, intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including parent Defendant Leedarson IoT and Leedarson IoT's direct and/or indirect U.S.-based subsidiaries, and members, segments, companies and/or brands of Leedarson.

22. On information and belief, Leedarson Lighting utilizes established distribution channels to distribute, market, offer for sale, sell, service, and/or warrant infringing products directly to consumers and other users, including offering such products and/or related services for sale. Leedarson products and services have been sold from and/or in both brick-and-mortar stores and online retail stores by entities within this District and in Texas. Alone and in concert with or via direction and control of or by at least these entities, Leedarson Lighting has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas. For example, Leedarson Lighting operates within a global network of sales and distribution of Leedarson products that includes subsidiaries of Leedarson, retail stores and showrooms, dealers, resellers, professional installers, and distributors operating in Texas, including this District.

23. On information and belief, as a part of Leedarson' global manufacturing and distribution network, Leedarson Lighting also purposefully places infringing Leedarson products in established distribution channels in the stream of commerce, including in Texas, via distribution

partners, retailers (including national retailers), resellers, dealers, brand ambassadors, service providers, consumers, and other users. *See., e.g., Leedarson Declaration regarding M-LA02302 Wi-Fi and Bluetooth SMART (BLE) Combo Module*, LEEDARSON/LEEDARSON LIGHTING CO., LTD. https://fccid.io/2AB2Q-MLA02302/Letter/Declaration-nonUS-Channel-4885689 (July 30, 2020) (last visited Oct. 9, 2023) (letter to Federal Communications Commission stating under "LEEDARSON" letterhead: "We LEEDARSON LIGHTING CO., LTD. hereby declare that M-LA02302 WI-FI and Bluetooth SMART (BLE) Combo Module is capable of operating with channel 12 and 13 in regions other than the US and Canada. However, these two channels will be disabled via software, this device available for import and sale in the US and Canada will not operate on channels 12 and 13 and it will not be possible for users to configure these channels in the US and Canada."); *USE AND CARE GUIDE: Wireless Controlled A19 Smart Bulb,* HOMEDEPOT.COM/ECOSMART, https://images.thdstatic.com/catalog/pdfImages/f7/f70a7802-6d86-424a-9328-91736423e757.pdf (last visited Oct. 9, 2023) (indicating that Model # 11A19060WRGBWH1 and Item # 1006931917 "Contains FCC ID 2AB2Q-MLA02302," which refers to the M-LA02302 WI-FI and Bluetooth SMART (BLE) Combo Module available for import and sale into the United States); *60-Watt Equivalent Smart A19 Color Changing CEC LED Light Bulb with Voice Control (1-Bulb) Powered by Hubspace,* HOME DEPOT, https://www.homedepot.com/p/EcoSmart-60-Watt-Equivalent-Smart-A19-Color-Changing-CEC-LED-Light-Bulb-with-Voice-Control-1-Bulb-Powered-by-Hubspace-11A19060WRGBWH1/318411935 (last visited Oct. 9, 2023) (Being offered for sale to individuals in zip code 75024 in Plano, Collin County, Texas in the Eastern District of Texas and being assigned Model # 11A19060WRGBWH1 and Item # 1006931917 per the associated URL and the associated product manual, *USE AND CARE GUIDE: Wireless Controlled A19 Smart*

*Bulb,* for which a link is provided). Therefore, Leedarson Lighting, alone and in concert with members, related entities, segments, companies and/or brands of Leedarson, its parent entity Defendant Leedarson IoT, and Leedarson IoT's direct and/or indirect U.S. based subsidiaries, has purposefully directed its activities at Texas, and should reasonably anticipate being brought in this Court, at least on this basis. Through its own conduct and through direction and control of its subsidiaries or control by other Defendant Leedarson IoT, Leedarson Lighting has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere within the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over Leedarson Lighting would not offend traditional notions of fair play and substantial justice.

24. In the alternative, this Court has personal jurisdiction over Leedarson Lighting under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, Leedarson Lighting is not subject to the jurisdiction of the courts of general jurisdiction of any state, and exercising jurisdiction over Leedarson Lighting is consistent with the U.S. Constitution.

25. Venue is proper in this District with respect to Defendant Leedarson Lighting, for example, pursuant to 28 U.S.C. § 1391. Defendant Leedarson Lighting is a foreign entity and may be sued in any district under 28 U.S.C. § 1391(c). *See also In re HTC Corporation*, 889 F.3d 1349, 1357 (Fed. Cir. 2018) ("The Court's recent decision in *TC Heartland* does not alter" the alien-venue rule.).

## THE ASSERTED PATENTS AND TECHNOLOGY

26. 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.

27. 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.

28. 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.

29. 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) is 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.

30. The ’126 patent provides a secure wireless local area network (LAN) utilizing a LAN device. This device may include a housing that carries a wireless transceiver and, a media access

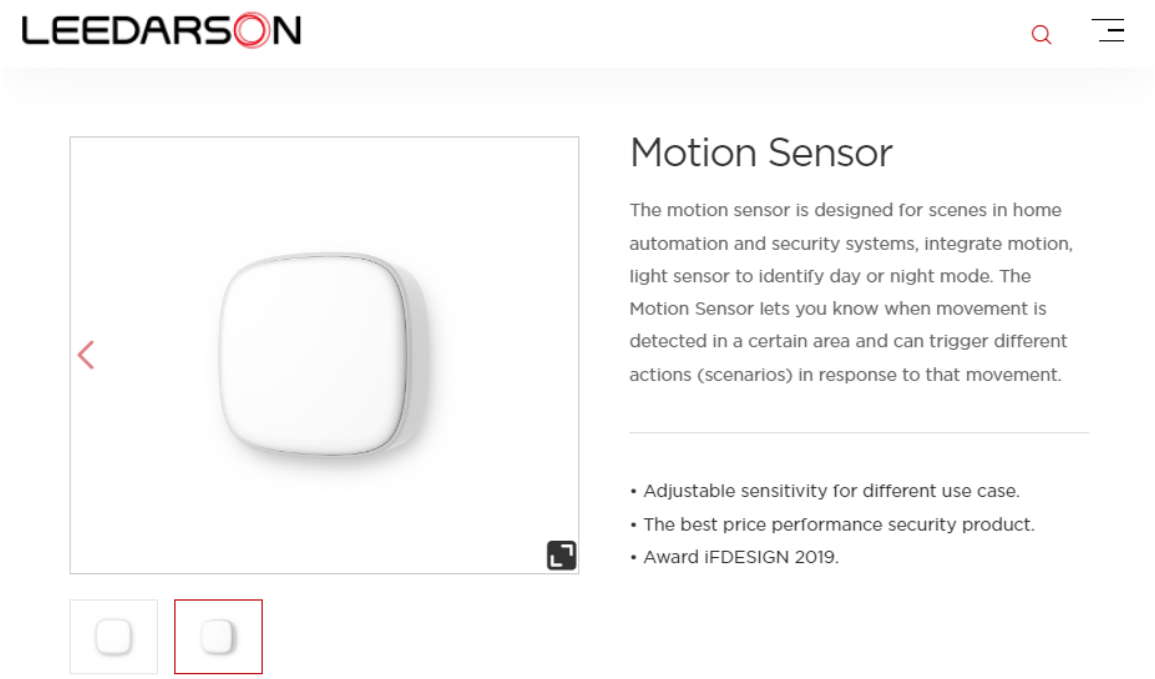
controller (MAC). A cryptography circuit carried by the housing may be connected to the MAC and the wireless transceiver. And the cryptography circuit may comprise a volatile memory provided for storing cryptography information and may also comprise a battery provided for maintaining the cryptography information stored on the volatile memory.

31. On information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture, distribution, sale, and use of home and business networking, IoT, and smart home products and components, which are manufactured in or imported into the United States, distributed to resellers, dealers, and third-party manufacturers, and ultimately sold to and used by U.S. consumers. For example, Leedarson reported that they had over 6.6 billion RMB in overseas sales and over 2.1 billion RMB in IoT sales in the 2022 reporting period. *See Leedarson Financial Report,* p. 18-19.

32. The Asserted Patents cover Defendants' home and business IoT and smart home products and components, software, services, and processes related to same that generally connect to other devices in a network or other networks using a wireless protocol, such as ZigBee and Wi-Fi. *See, e.g., Smart Living Products*, LEEDARSON, https://www.leedarson.com/products/smart-living-products, (last visited Sep. 29, 2023); *Aidot Products*, AIDOT, https://www.aidot.com/products.html (last visited Sep. 30, 2022); *LEEDARSON'S IoT Innovation Journey with Zigbee Alliance,* LEEDARSON https://www.leedarson.com/news/leedarsons-iot-innovation-journey-with-zigbee-alliance ('In 2016, LEEDARSON joined the Zigbee Alliance to fully utilize Zigbee technology to build and certify IoT products for US and European markets."). Defendants' infringing products include, but are not limited to, devices enabled or compliant with Wi-Fi and/or ZigBee, including without limitation smart lighting (for example, A60 806lm Dimmable E27, A19 800lm Tunable White E26, A60 806lm Tunable White E27, PAR16 350lm

RGBW GU10, BR30 650lm RGBW E26, Ceiling Luna C4d, DownLight DS1 1450lm, Filament ST64 Clear 470lm Dimmable E27, Global G95 Clear 470lm Dimmable E27, AiDot Mujoy Matter Version BR30 WiFi Smart Flood Light Bulb, AiDot Linkind Smart Color Changing Solar Pathway Lights, AiDot Orein LED Smart Motion Sensor Outdoor Flood Light, AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs); security cameras (for example, AiDot Winees L1 Outdoor Wireless Solar Security Camera, AiDot Winees M2 Pro 2K Indoor Security Camera, AiDot Winees F2/F2 Pro, AiDot Winees Baby Monitor 1080P Indoor Camera with Night Vision, A215 Smart Indoor IP Camera, Outdoor Camera F101 Spotlight IP Camera, F102 Outdoor Floodlight IP Camera Pro); connected modules (for example, LWK32B500A, LWK31C510A, LZS11F210A, LDS73R010A); wireless alarm and/or home automation gateways (for example, Leedarson Mini Hub/Gateway, Leedarson Siren Hub, Leedarson Multi-protocol Hub NA); kitchen appliances (for example, AiDot Welov 8-Quart Air Fryer with Visible Cooking Window); Keypads (for example, Leedarson Keypad, Leedarson Key Fob); sensors (for example, AiDot Linkind PIR Motion Sensor, Winees WP0500187 Water Leak Detector, Leedarson Motion Sensor, Leedarson 4-in-1 Sensor); house appliances (for example, Smart Air Purifier AP2008S, AiDot Welov P200S/P200 PRO(WIFI) Air Purifier, AiDot Welov D300 WiFi Smart Aroma Diffuser, AiDot Welov H500D/ H500 PRO(WIFI) Long-Lasting Humidifier, AiDot Welov S300 Smart Body Fat Scale with BIA Technology, AiDot Welov R300 BLE Smart Jump Rope with 4 Modes); energy management (for example, Leedarson Smart Plug/NA/15A,); thermostats (for example, Leedarson Smart Thermostat-Medium); and related accessories and software (all collectively referred to as the "Accused Products"). These Accused Products infringe the Asserted Patents by at least their manufacture, importation, distribution, sale, and use in the U.S.

33. The Asserted Patents cover Accused Products of Leedarson that use the ZigBee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of the Leedarson's ZigBee products include the Leedarson Motion Sensor (Model Number 8A-SS-BA-H0) which uses the Zigbee protocol to "trigger different actions (scenarios) in response to … movement" which is shown below:



## Specifications

| Name | Value |
|---|---|
| Model Number | 8A-SS-BA-H0 |
| Protocol | Zigbee 3.0 |
| Detection Technology | PIR |
| Detection Angle | 110° |
| Detection Range | 5m(16ft.) |
| Light Sensor | 50lux, for day/night |
| Power Source | 3VDC, CR2450 x 1 |
| Battery Life | 2 Years |

| Name | Value |
|---|---|
| Radio Frequency | Zigbee 2.4GHz |
| Operating Range | 130ft(40m) LOS |
| Operating Temperature | 32°F - 104°F(0°C - 40°C) |
| Operating Humidity | Up to 85%, Non-condensing |
| Mounting | Screw or Foam Tape |
| Mounting Height | 7.22ft. to 9.19ft. (2.2m to 2.8m) |
| Certification | CE/FCC |

*See Leedarson Motion Sensor,* LEEDARSON, https://www.leedarson.com/products/motion-sensor-detail (last visited Oct. 3, 2023).

34. ZigBee protocols, which are covered by the Asserted Patents and utilized by certain Accused Products, are based on the IEEE 802.15.4 standard for wireless network communication. Below is an excerpt from the technical specification for ZigBee protocols describing the basic architecture and standards that enable wireless network communication.

## 1.1 Protocol Description

The ZigBee Alliance has developed a very low-cost, very low-power-consumption, two-way, wireless communications standard. Solutions adopting the ZigBee standard will be embedded in consumer electronics, home and building automation, industrial controls, PC peripherals, medical sensor applications, toys, and games.

### 1.1.3 Stack Architecture

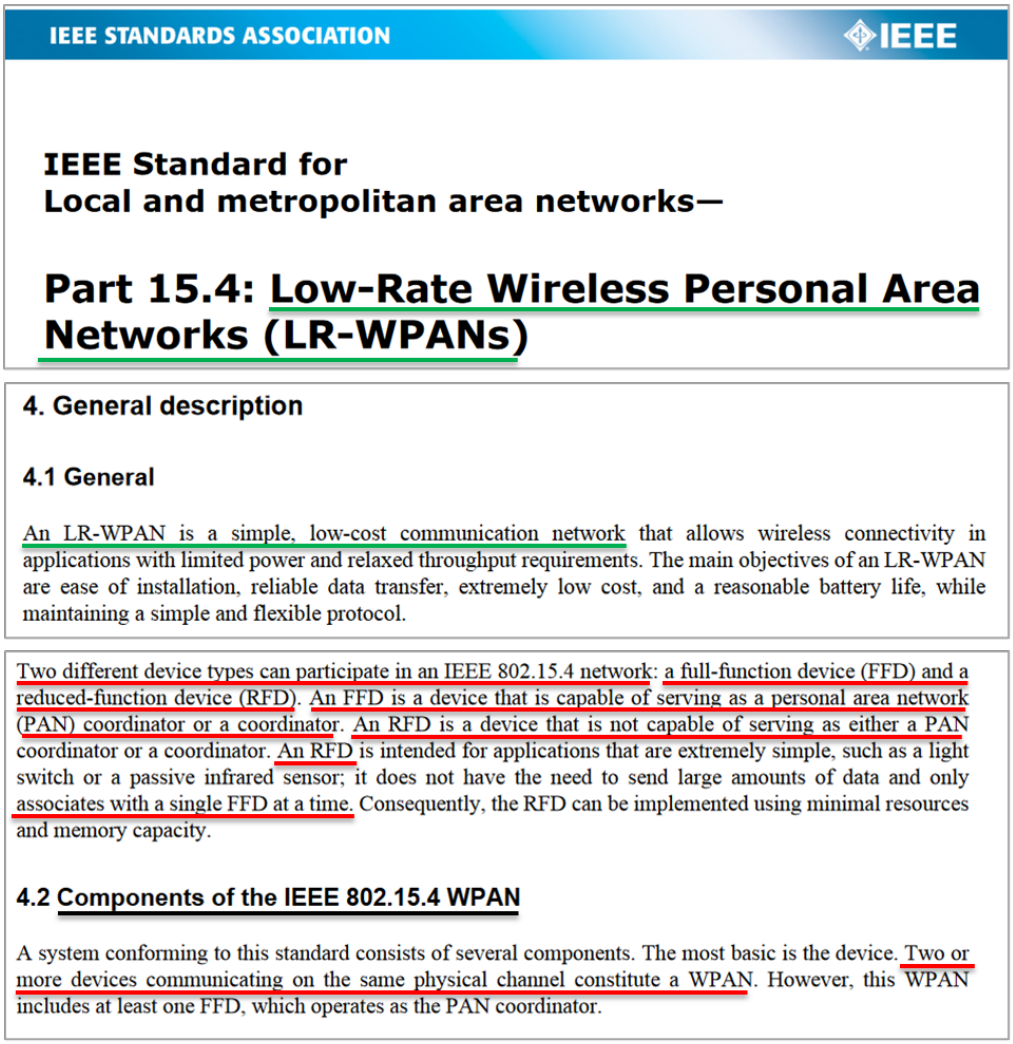
The ZigBee stack architecture is made up of a set of blocks called layers. Each layer performs a specific set of services for the layer above. A data entity provides a data transmission service and a management entity provides all other services. Each service entity exposes an interface to the upper layer through a service access point (SAP), and each SAP supports a number of service primitives to achieve the required functionality.

The IEEE 802.15.4 standard defines the two lower layers: the physical (PHY) layer and the medium access control (MAC) sub-layer. The ZigBee Alliance builds on this foundation by providing the network (NWK) layer and the framework for the application layer. The application layer framework consists of the application support sub-layer (APS) and the ZigBee device objects (ZDO). Manufacturer-defined application objects use the framework and share APS and security services with the ZDO.

The PHY layer operates in two separate frequency ranges: 868/915 MHz and 2.4 GHz. The lower frequency PHY layer covers both the 868 MHz European band and the 915 MHz band, used in countries such as the United States and Australia. The higher frequency PHY layer is used virtually worldwide. A complete description of the PHY layers can be found in [B1].

*ZigBee Specification*, revision r21 at 1, THE ZIGBEE ALLIANCE, https://zigbeealliance.org/wp-content/uploads/2019/11/docs-05-3474-21-0csg-zigbee-specification.pdf (August 5, 2015).

35. 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 a 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*

36. 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.

ZigBee Control your world

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.

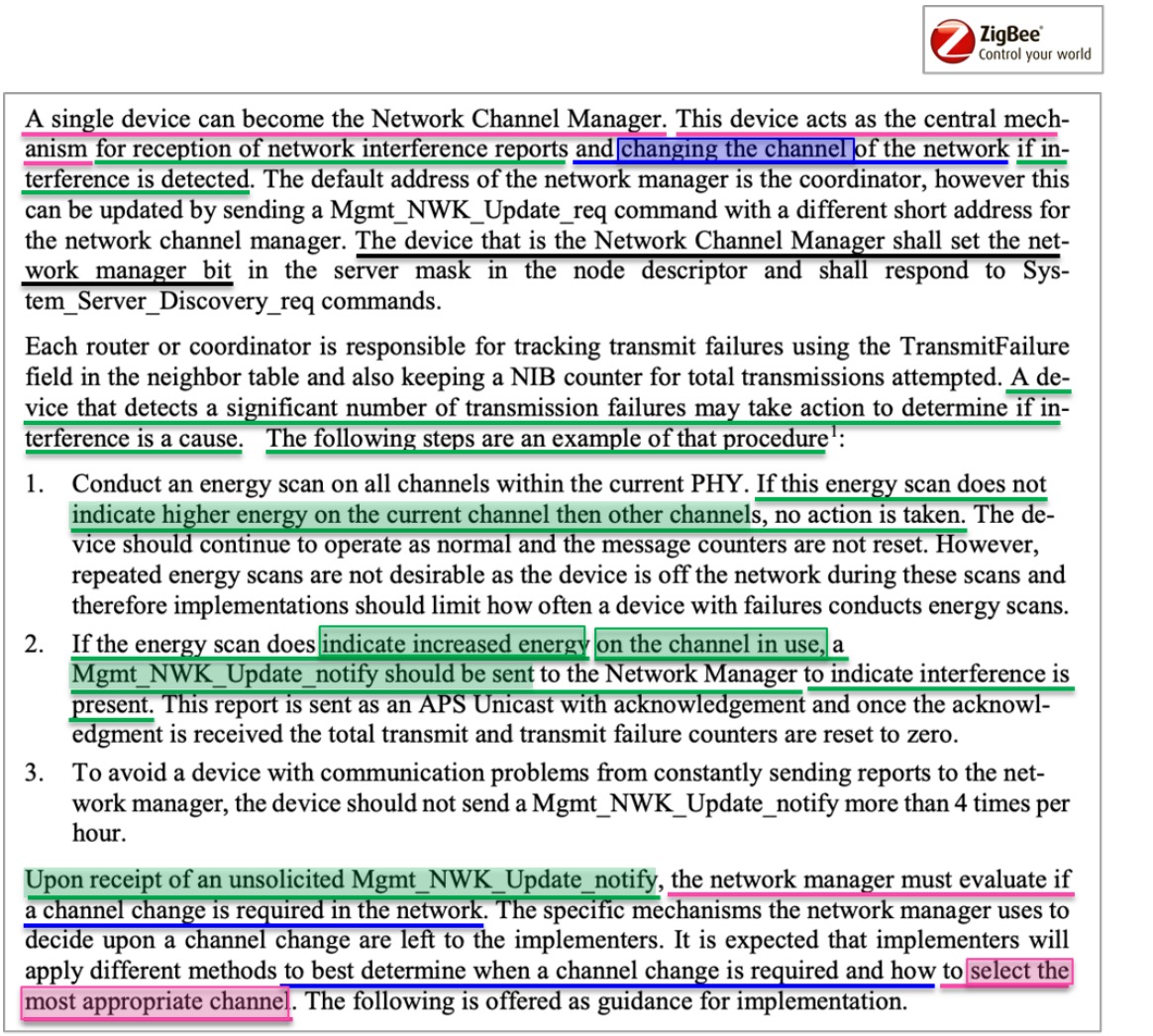
Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference 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*

37. 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*

38. 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*

39. The Asserted Patents also cover Accused Products of Leedarson that utilize the Wi-Fi protocol. Examples of such products include the AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs and AiDot App. As shown below, the AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs and AiDot App are Wi-Fi (IEEE 802.11) compliant:


*AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs*, OREiN, https://www.amazon.com/-/es/OREiN-Matter-Smart-Light-Blulbs/dp/B0BLTWFJWY?th=1 (last visited Sep. 29, 2023).


*AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs*, OREiN, https://www.aidot.com/aidot-orein-a19-matter-smart-reliable-wifi-light-bulbs.html?utm_source=web&utm_medium=Orein&utm_campaign=AiDot+OREiN+A19+Matter+Smart+Reliable+WiFi+Light+Bulbs&utm_term=OS01013-RGBTW-WB-NA-6 (last visited Sep. 30, 2023).

| | |
|---|---|
| Size | A19-2PACK |
| Model Name | OS0100811267 |
| Connectivity Technology | Matter, Wi-Fi |

| | |
|---|---|
| Manufacturer | OREiN |
| Part Number | OS01013-RGBTW-WB-NA-2 |
| Item Weight | 4.6 ounces |
| Product Dimensions | 1 x 1 x 2.36 inches |
| Country of Origin | China |

*Product information Technical Details*, OREiN, https://www.amazon.com/-/es/OREiN-Matter-Smart-Light-Blulbs/dp/B0BLTWFJWY?th=1 (last visited Sep. 30, 2023).

40. The Accused Products include an intrusion detection method for a local or metropolitan area. As described below, the IEEE 802.11 authentication methods utilized by the Accused Products utilize a TKIP that includes a "MIC" to 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*

41. 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*

42. 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

43. 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*

44. 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

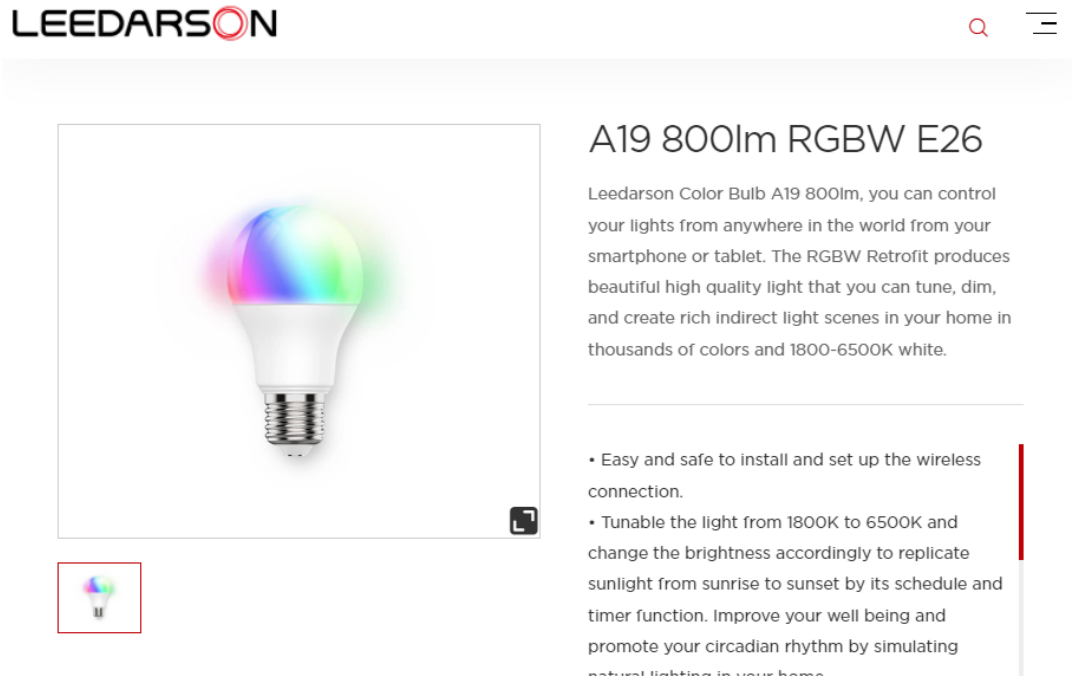
The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

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*

45. The Asserted Patents also cover Leedarson's Wi-Fi compliant devices, which support WPA and WPA2, and WPA3 security mechanisms, as described below and in the following

paragraph. Of the WPA, WPA2 and WPA3 security mechanism used by the Accused Products, such as Leedarson's smart home Wi-Fi devices, the WPA is based on Temporal Key Integrity Protocol (TKIP), while the WPA2 and WPA3 are based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below is an exemplary IEEE 802.11 compliant lightbulb and camera. The devices each have a housing.




*A19 Smart LED Lighting*, LEEDARSON, https://www.leedarson.com/products/a19-800lm-rgbw-e26 (last visited Oct. 4, 2023).

**Wi-Fi CERTIFIED™ Certificate**

This certificate lists the features that have successfully completed Wi-Fi Alliance interoperability testing. Learn more: www.wi-fi.org/certification/programs

**Certification ID: WFA127490**

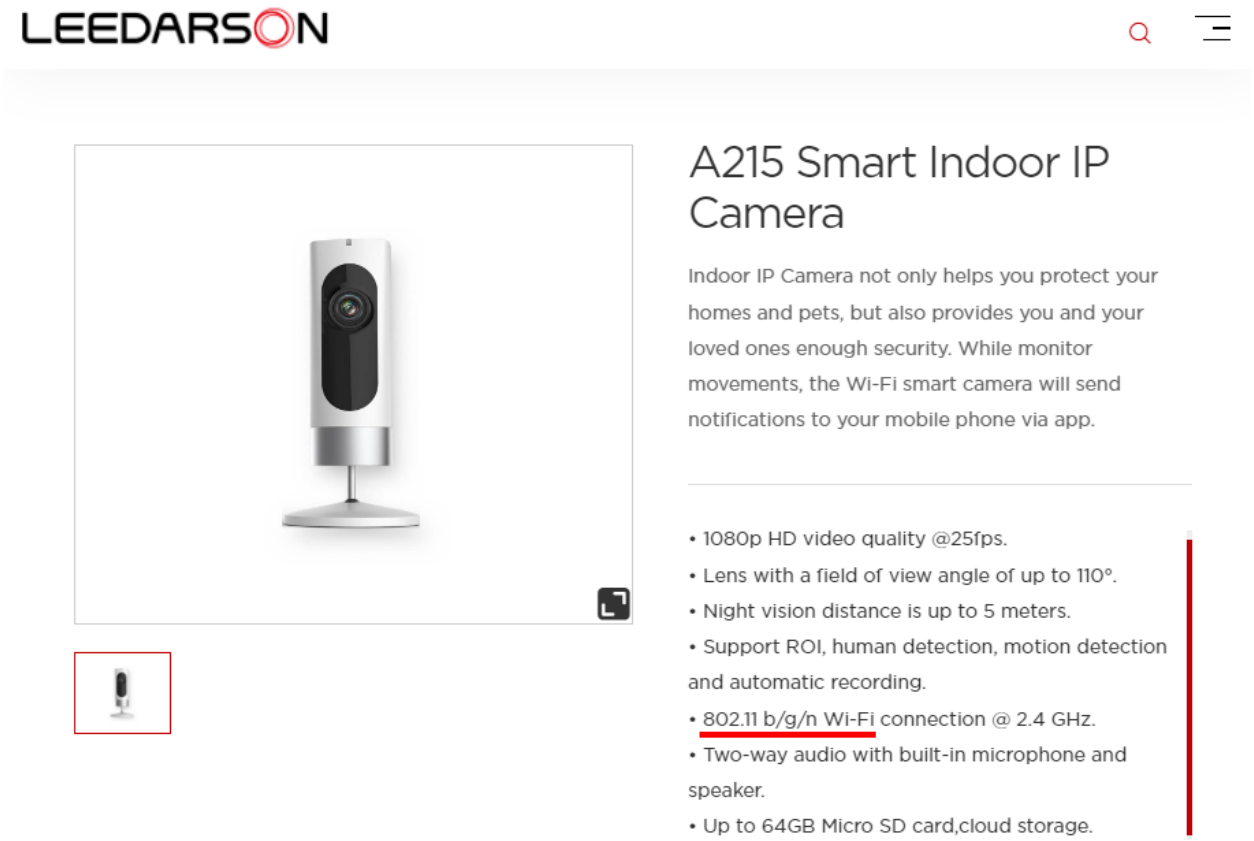
**Product Info**

| | |
|---|---|
| **Date of Certification** | September 25, 2023 |
| **Company** | LEEDARSON IoT Technology Inc. |
| **Product Name** | Smart A19 LED Light Bulb |
| **Product Model Variant** | LA66701 |
| **Model Number** | 13aSBA800STQ1T |
| **Category** | Other |
| **Sub-category** | Other |

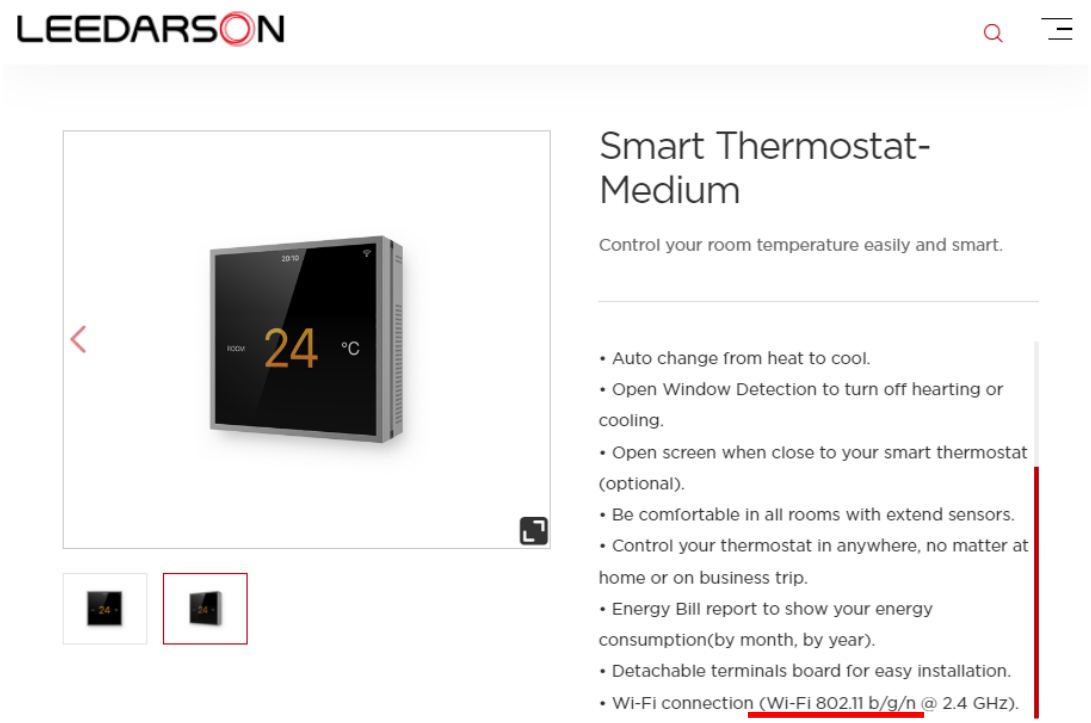
**Summary of Certifications**

| CLASSIFICATION | CERTIFICATION |
|---|---|
| **Connectivity** | 2.4 GHz Spectrum Capabilities<br>Wi-Fi CERTIFIED™ b<br>Wi-Fi CERTIFIED™ g<br>Wi-Fi CERTIFIED™ n |
| **Optimization** | WMM® |
| **Security** | Protected Management Frames<br>WPA2™-Personal 2021-01<br>WPA3™-Personal 2022-06<br>WPA™-Personal |

*Smart Bulb Wi-Fi Certification*, p. 1, WIFI ALLIANCE, *available for download at* https://www.wi-fi.org/product-finder-results?sort_by=certified&sort_order=desc&companies=2665 (last visited Oct. 3, 2023).




*A215 Smart Indoor IP Camera*, LEEDARSON, https://www.leedarson.com/products/a215-indoor-smart-ip-camera (last visited Oct. 4, 2023).




*Smart Thermostat*, LEEDARSON, https://www.leedarson.com/products/smart-thermostat-medium (last visited Oct. 4, 2023).

46. WPA and WPA2 security encryption systems are used in conjunction with 802.11 b/g/n Wi-Fi connections standards. Which as shown above is utilized across Defendants' Accused Product line.

47. As shown above, the Accused Products provide 2.4 and/or 5 GHz Wi-Fi speeds. This capability ascertains the presence of a Wi-Fi antenna and transceiver in the device and provides a secure wireless LAN.

48. 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.

**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.

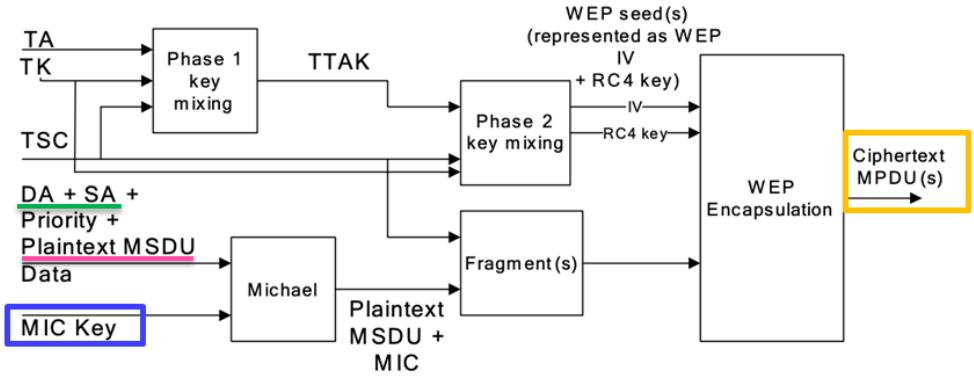



**Figure 8-4—TKIP encapsulation block diagram**

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).

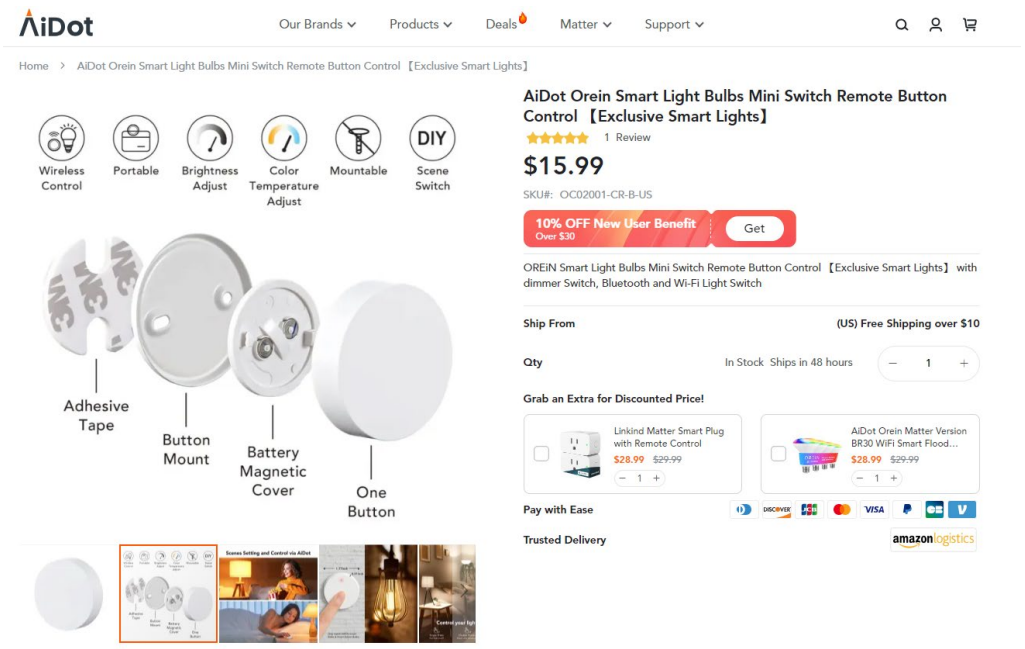
c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.

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*

49. On information and belief, Defendant also infringes the ’126 patent via products that utilize a volatile memory for storing cryptography information utilized in the cryptography circuit and a battery for maintaining the cryptography information in the volatile memory. As shown in Vivint’s Smart Hub control panel specifications, the control panel utilizes a battery that provides power to maintain data, including cryptographic information in the product’s internal

(volatile) memory. Such cryptographic information allows data encryption to be carried out over a secure wireless 802.11 network.




**Specification**

| | |
|---|---|
| Brand | OREiN |
| Special Feature | Dimmable, High Efficiency |
| Wattage | 1 watts |
| Specific Uses For Product | Remote Control, Brightness Control, Dimmer Switch |
| Number of Items | 1 |
| Material | Plastic |
| Connectivity Technology | Bluetooth, Wi-Fi |
| Indoor/Outdoor Usage | Indoor |
| Controller Type | Google Assistant, Amazon Alexa |
| Style | Modern |
| Included Components | Magnet, Remote, 3M Adhesive Paper |
| Item Weight | 1.13 ounces |
| Package Dimensions | 2.2 x 2.2 x 0.83 inches |
| Batteries | 1 CR2032 batteries required. (included) |
| Average Life | 25000 Hours |

*AiDot Orien Smart Light Bulbs Mini Switch Remote Button Control*, AIDOT, https://www.aidot.com/aidot-orein-smart-light-bulbs-mini-switch-remote-button-control-exclusive-smart-lights.html (last visited Oct. 3, 2023).

50. As shown above, the exemplary Accused Product utilizes a battery to maintain cryptography information involved in a secure wireless 802.11 network.

**COUNT I**

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

51. Plaintiff incorporates paragraphs 1 through 49 herein by reference.

52. 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.

53. 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.

54. Leedarson 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.

55. On information and belief, Leedarson designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Leedarson and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants Leedarson IoT and Leedarson Lighting and U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson.

56. Defendants each directly infringe 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, related entities, distributors, dealers,

importers, customers, parent, subsidiaries, members, segments, companies, brands, and/or consumers. Furthermore, on information and belief, Defendants make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, customers and other related service providers 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 and use 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)").

57. Furthermore, Defendant Leedarson IoT directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Leedarson Lighting, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Leedarson's U.S.-based subsidiaries, including at least Leedarson America and AiDot, conduct activities that constitute direct infringement of the '678 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Leedarson IoT. Defendant Leedarson IoT is vicariously liable for the infringing conduct of Leedarson America, AiDot, and other U.S.-

based subsidiaries, members, related entities, segments, companies and/or brands of Leedarson (under both the alter ego and agency theories). On information and belief, Defendants Leedarson IoT and Leedarson Lighting, and U.S. based subsidiaries members, segments, companies and/or brands of Leedarson are essentially the same company (i.e., "Leedarson"), operating in the U.S. via at least the Leedarson America, AiDot, Anshe, Arnoo, Welove, Homax, Linkind, Orein, MuJoy, Winees, Syvio, Enhulk, ganiza, Hyderson, GoGonova brands, segments, mergers, or acquisitions of Leedarson. Moreover, Leedarson IoT, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

58. For example, Leedarson infringes claim 51 of the '678 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to smart lighting (for example, A60 806lm Dimmable E27, A19 800lm Tunable White E26, A60 806lm Tunable White E27, PAR16 350lm RGBW GU10, BR30 650lm RGBW E26, Ceiling Luna C4d, DownLight DS1 1450lm, Filament ST64 Clear 470lm Dimmable E27, Global G95 Clear 470lm Dimmable E27, AiDot Mujoy Matter Version BR30 WiFi Smart Flood Light Bulb, AiDot Linkind Smart Color Changing Solar Pathway Lights, AiDot Orein LED Smart Motion Sensor Outdoor Flood Light, AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs); security cameras (for example, AiDot Winees L1 Outdoor Wireless Solar Security Camera, AiDot Winees M2 Pro 2K Indoor Security Camera, AiDot Winees F2/F2 Pro, AiDot Winees Baby Monitor 1080P Indoor Camera with Night Vision, A215 Smart Indoor IP Camera, Outdoor Camera F101 Spotlight IP Camera, F102 Outdoor Floodlight IP Camera Pro); connected modules (for example, LWK32B500A, LWK31C510A); wireless alarm and/or home automation gateways (for example, Leedarson Mini

Hub/Gateway, Leedarson Siren Hub, Leedarson Multi-protocol Hub NA); kitchen appliances (for example, AiDot Welov 8-Quart Air Fryer with Visible Cooking Window); house appliances (for example, Smart Air Purifier AP2008S, AiDot Welov P200S/P200 PRO(WIFI) Air Purifier, AiDot Welov D300 WiFi Smart Aroma Diffuser, AiDot Welov H500D/ H500 PRO(WIFI) Long-Lasting Humidifier, AiDot Welov S300 Smart Body Fat Scale with BIA Technology); energy management (for example, Leedarson Smart Plug/NA/15A,); thermostats (for example, Leedarson Smart Thermostat-Medium); and related accessories and software.

59. 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.

60. At a minimum, Leedarson has known of the '678 patent at least as early as the filing date of this complaint. In addition, Leedarson has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '678 patent, since at least its receipt of a letter dated April 20, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Leedarson of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards.

61. Additional correspondence sent by Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition and licensing attempt of the Harris patent portfolio (which Leedarson had notice of at least by April 20, 2018), was sent directly to Leedarson, on March 15, 2022. Leedarson did not respond. On March 22, 2022, a follow-up email was sent on behalf of Stingray to Leedarson again notifying Leedarson of and providing Leedarson with the opportunity to license Stingray's "portfolio of wireless networking patents." Again, Leedarson did not respond to this and several other subsequent attempts by Stingray to license the Harris patent portfolio.

62. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use 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 date or dates of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '678 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers 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. Moreover,

Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance) in the Accused Products, and provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., Product Finder Filtered Results*, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-results?keywords=leedarson (last visited Oct. 24, 2023) (showing Leedarson's WiFi Certified™ products include the "LA02301 WI-FI and Bluetooth SMART (BLE) Combo Module" with model number "LA02301" and "Last Certified Date: 2021-04-23," the "Smart A19 LED Light Bulb" with model number "13aSBA800STQ1T" and "Last Certified Date: 2023-09-25," and the "M-LA02302 WI-FI and Bluetooth SMART (BLE) Combo Module," with model number "M-LA02302" and "Last Certified Date: 2023-07-11," with several variants for each product); *LA02301 Module User Manual*, LEEDARSON, available at https://fccid.io/2AB2Q-LA02301/User-Manual/User-Manual-4959691.pdf (last visited Oct. 24, 2023); *Arnoo: A Cloud-based, Single-App for Smart Living Solutions*, LEEDARSON, https://www.youtube.com/watch?v=dOdCF55ZouI (including a description that states "Arnoo can help you to integrate all your smart products into your one and only branded App, allows you to focus on the areas of expertise with which you are familiar" and displaying symbols indicating Wi-Fi and Zigbee compatibility in the video).

63. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Leedarson's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) such as the AiDot App to

provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g., Control Your Smart Living arbitrarily : Smart Home App,* AIDOT, https://www.aidot.com/blog/post/smart-home-app (last visited Sep. 29, 2023).

64. Leedarson's apps also induce infringing use of the Accused Products by providing compatibility between Leedarson products and third-party products that share or access the same wireless networks. *See, e.g.*, *id* ("Besides, all the supported brands and third-party apps including Linkind, Winees, Orein, Ecobee, Honeywell Home, Alexa, Google Assistant, Smartthings, IFTTT of smart devices are listed in app for you to choose."); *Getting Started*, AIDOT, https://www.aidot.com/page/getting-start ("Link your Alexa or Google account with AiDot.") (last visited Sep. 29, 2023). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '678 patent.

65. 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, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' 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.

66. Plaintiff Stingray has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their 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. 7,440,572)

67. Plaintiff incorporates paragraphs 1 through 65 herein by reference.

68. 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.

69. 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.

70. Leedarson 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.

71. On information and belief, Leedarson designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Leedarson and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants Leedarson IoT and Leedarson Lighting and U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson.

72. Defendants each directly infringe the '572 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms, resellers, dealers, installers, customers and other related service providers 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 and use 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)").

73. Furthermore, Defendant Leedarson IoT directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Leedarson Lighting, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Leedarson's U.S.-based subsidiaries, including at least Leedarson America and AiDot, conduct activities that constitute direct infringement of the '572 patent under 35 U.S.C. § 271(a) by

importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Leedarson IoT. Defendant Leedarson IoT is vicariously liable for the infringing conduct of Leedarson America, AiDot, and other U.S.-based subsidiaries, members, related entities, segments, companies and/or brands of Leedarson (under both the alter ego and agency theories). On information and belief, Defendants Leedarson IoT and Leedarson Lighting, and U.S. based subsidiaries members, segments, companies and/or brands of Leedarson are essentially the same company (i.e., "Leedarson"), operating in the U.S. via at least the Leedarson America, AiDot, Anshe, Arnoo, Welove, Homax, Linkind, Orein, MuJoy, Winees, Syvio, Enhulk, ganiza, Hyderson, GoGonova brands, segments, mergers, or acquisitions of Leedarson. Moreover, Leedarson IoT, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

74. For example, Leedarson infringes claim 1 of the '572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to smart lighting (for example, A60 806lm Dimmable E27, A19 800lm Tunable White E26, A60 806lm Tunable White E27, PAR16 350lm RGBW GU10, BR30 650lm RGBW E26, Ceiling Luna C4d, DownLight DS1 1450lm, Filament ST64 Clear 470lm Dimmable E27, Global G95 Clear 470lm Dimmable E27, AiDot Mujoy Matter Version BR30 WiFi Smart Flood Light Bulb, AiDot Linkind Smart Color Changing Solar Pathway Lights, AiDot Orein LED Smart Motion Sensor Outdoor Flood Light, AiDot OREiN A19 Matter Smart Reliable WiFi Light Bulbs); security cameras (for example, AiDot Winees L1 Outdoor Wireless Solar Security Camera, AiDot Winees M2 Pro 2K Indoor Security Camera, AiDot Winees F2/F2 Pro, AiDot Winees Baby Monitor 1080P Indoor Camera with Night

Vision, A215 Smart Indoor IP Camera, Outdoor Camera F101 Spotlight IP Camera, F102 Outdoor Floodlight IP Camera Pro); connected modules (for example, LWK32B500A, LWK31C510A); wireless alarm and/or home automation gateways (for example, Leedarson Mini Hub/Gateway, Leedarson Siren Hub, Leedarson Multi-protocol Hub NA); kitchen appliances (for example, AiDot Welov 8-Quart Air Fryer with Visible Cooking Window); house appliances (for example, Smart Air Purifier AP2008S, AiDot Welov P200S/P200 PRO(WIFI) Air Purifier, AiDot Welov D300 WiFi Smart Aroma Diffuser, AiDot Welov H500D/ H500 PRO(WIFI) Long-Lasting Humidifier, AiDot Welov S300 Smart Body Fat Scale with BIA Technology); energy management (for example, Leedarson Smart Plug/NA/15A,); thermostats (for example, Leedarson Smart Thermostat-Medium);; and related accessories and software.

75. 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.

76. Leedarson 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 make a secure wireless local area network 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.

77. Leedarson 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.

78. At a minimum, Leedarson has known of the '572 patent at least as early as the filing date of this complaint. In addition, Leedarson has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '572 patent, since at least its receipt of a letter dated April 20, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Leedarson of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards.

79. Additional correspondence sent by Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition and licensing attempt of the Harris patent portfolio (which Leedarson had notice of at least by April 20, 2018), was sent directly to Leedarson, on March 15, 2022. Leedarson did not respond. On March 22, 2022, a follow-up email was sent on behalf of Stingray to Leedarson again notifying Leedarson of and providing Leedarson with the opportunity to license Stingray's "portfolio of wireless networking patents." Again, Leedarson did not respond to this and several other subsequent attempts by Stingray to license the Harris patent portfolio which includes the '572 patent.

80. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use 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 date or dates of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '572 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers 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. Moreover, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance) in the Accused Products, and provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., Product Finder Filtered Results*, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-

results?keywords=leedarson (last visited Oct. 24, 2023) (showing Leedarson's WiFi Certified™ products include the "LA02301 WI-FI and Bluetooth SMART (BLE) Combo Module" with model number "LA02301" and "Last Certified Date: 2021-04-23," the "Smart A19 LED Light Bulb" with model number "13aSBA800STQ1T" and "Last Certified Date: 2023-09-25," and the "M-LA02302 WI-FI and Bluetooth SMART (BLE) Combo Module," with model number "M-LA02302" and "Last Certified Date: 2023-07-11," with several variants for each product); *LA02301 Module User Manual*, LEEDARSON, available at https://fccid.io/2AB2Q-LA02301/User-Manual/User-Manual-4959691.pdf (last visited Oct. 24, 2023); *Arnoo: A Cloud-based, Single-App for Smart Living Solutions*, LEEDARSON, https://www.youtube.com/watch?v=dOdCF55ZouI (including a description that states "Arnoo can help you to integrate all your smart products into your one and only branded App, allows you to focus on the areas of expertise with which you are familiar" and displaying symbols indicating Wi-Fi and Zigbee compatibility in the video).

81. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Leedarson's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) such as the AiDot App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g., Control Your Smart Living arbitrarily : Smart Home App,* AIDOT, https://www.aidot.com/blog/post/smart-home-app (last visited Sep. 29, 2023).

82. Leedarson's apps also induce infringing use of the Accused Products by providing compatibility between Leedarson products and third-party products that share or access the same wireless networks. *See, e.g.*, *id* ("Besides, all the supported brands and third-party apps including Linkind, Winees, Orein, Ecobee, Honeywell Home, Alexa, Google Assistant, Smartthings, IFTTT

of smart devices are listed in app for you to choose."); *Getting Started*, AIDOT, https://www.aidot.com/page/getting-start ("Link your Alexa or Google account with AiDot.") (last visited Sep. 29, 2023). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '572 patent.

83. 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, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '126 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.

84. Plaintiff Stingray has been damaged as a result of Leedarson'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 Leedarson'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. 7,616,961)

85. Plaintiff incorporates paragraphs 1 through 83 herein by reference.

86. 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.

87. 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.

88. Leedarson 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.

89. On information and belief, Leedarson designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Leedarson and its parent, subsidiaries, members, segments, companies, brands and/or related entities, such as Defendants Leedarson IoT and Leedarson Lighting and U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson.

90. Defendants each directly infringe the '961 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms,

resellers, dealers, installers, customers and other related service providers 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 and use 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)").

91. Furthermore, Defendant Leedarson IoT directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Leedarson Lighting, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Leedarson's U.S.-based subsidiaries, including at least Leedarson America and AiDot, conduct activities that constitute direct infringement of the '961 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Leedarson IoT. Defendant Leedarson IoT is vicariously liable for the infringing conduct of Leedarson America, AiDot, and other U.S.-based subsidiaries, members, related entities, segments, companies and/or brands of Leedarson (under both the alter ego and agency theories). On information and belief, Defendants Leedarson IoT and Leedarson Lighting, and U.S. based subsidiaries members, segments, companies and/or brands of Leedarson are essentially the same company (i.e., "Leedarson"), operating in the U.S.

via at least the Leedarson America, AiDot, Anshe, Arnoo, Welove, Homax, Linkind, Orein, MuJoy, Winees, Syvio, Enhulk, ganiza, Hyderson, GoGonova brands, segments, mergers, or acquisitions of Leedarson. Moreover, Leedarson IoT, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

92. For example, Leedarson infringes claim 1 of the '961 patent via the Accused Products that utilize ZigBee protocols, including, but not limited to smart lighting (for example, A60 806lm Dimmable E27, A19 800lm Tunable White E26, A60 806lm Tunable White E27, PAR16 350lm RGBW GU10, BR30 650lm RGBW E26, Ceiling Luna C4d, DownLight DS1 1450lm, Filament ST64 Clear 470lm Dimmable E27, Global G95 Clear 470lm Dimmable E27); connected modules (for example, LZS11F210A, LDS73R010A); wireless alarm and/or home automation gateways (for example, Leedarson Mini Hub/Gateway, Leedarson Siren Hub, Leedarson Multi-protocol Hub NA); keypads and locks (for example, Leedarson Keypad, Leedarson Key Fob, Smart Door Lock); sensors (for example, AiDot Linkind PIR Motion Sensor, Winees WP0500187 Water Leak Detector, Leedarson Motion Sensor, Leedarson 4-in-1 Sensor); house appliances (for example, AiDot Welov R300 BLE Smart Jump Rope with 4 Modes); energy management (for example, Leedarson Smart Plug/NA/15A,); ZigBee modules and interfaces; and related accessories and software.

93. 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.

94. At a minimum, Leedarson has known of the '961 patent at least as early as the filing date of this complaint. In addition, Leedarson has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '961 patent, since at least its receipt of a letter dated April 20, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Leedarson of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards.

95. Additional correspondence sent by Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition and licensing attempt of the Harris patent portfolio (which Leedarson had notice of at least by April 20, 2018), was sent directly to Leedarson, on March 15, 2022. Leedarson did not respond. On March 22, 2022, a follow-up email was sent on behalf of Stingray to Leedarson again notifying Leedarson of and providing Leedarson with the opportunity to license Stingray's "portfolio of wireless networking patents." Again,

Leedarson did not respond to this and several other subsequent attempts by Stingray to license the Harris patent portfolio which includes the ’961 patent.

96. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use 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 date or dates of notice provided above, Defendants each conduct infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’961 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers 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. Moreover, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, test and certify the wireless networking features (with for example the Connectivity Standards Alliance, i.e., for ZigBee certification) in the Accused Products, and

provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., Certified Products Search,* CONNECTIVITY STANDARDS ALLIANCE, https://csa-iot.org/csa-iot_products/?p_keywords=leedarson&p_type%5B%5D=17&p_type%5B%5D=14&p_type%5B%5D=1053&p_certificate=&p_family= (last visited Oct. 24, 2023) (showing Leedarson's Zigbee products certified by the Connectivity Standards Alliance include 19 pages of results with 12 products shown per page plus 7 products shown on the 20th page); *Leedarson Zigbee LED Bulb Quick User Guide*, LEEDARSON, available at https://fcc.report/FCC-ID/2AB2Q8ZA806STQ4R/4231571.pdf (last visited Oct. 24, 2023); *Arnoo: A Cloud-based, Single-App for Smart Living Solutions*, LEEDARSON, https://www.youtube.com/watch?v=dOdCF55ZouI (including a description that states "Arnoo can help you to integrate all your smart products into your one and only branded App, allows you to focus on the areas of expertise with which you are familiar" and displaying symbols indicating Wi-Fi and Zigbee compatibility in the video).

97. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Leedarson's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) such as the AiDot App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g., Control Your Smart Living arbitrarily : Smart Home App,* AIDOT, https://www.aidot.com/blog/post/smart-home-app (last visited Sep. 29, 2023).

98. Leedarson's apps also induce infringing use of the Accused Products by providing compatibility between Leedarson products and third-party products that share or access the same

wireless networks. *See, e.g.*, *id* ("Besides, all the supported brands and third-party apps including Linkind, Winees, Orein, Ecobee, Honeywell Home, Alexa, Google Assistant, Smartthings, IFTTT of smart devices are listed in app for you to choose."); *Getting Started*, AIDOT, https://www.aidot.com/page/getting-start ("Link your Alexa or Google account with AiDot.") (last visited Sep. 29, 2023). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '961 patent.

99. 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, Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' 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.

100. Plaintiff Stingray has been damaged as a result of Leedarson' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for Leedarson' 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. 7,441,126)

101. Plaintiff incorporates paragraphs 1 through 99 herein by reference.

102. Plaintiff is the assignee of the '126 patent, entitled "Secure wireless LAN device including tamper resistant feature and associated method," with ownership of all substantial rights in the '126 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements

103. The '126 patent is valid, enforceable, and was duly issued in full compliance with Title 35 of the United States Code. The '126 patent issued from U.S. Patent Application No. 09/761,173 filed on January 16, 2001.

104. Defendants have and continue to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '126 patent in this District and elsewhere in Texas and the United States.

105. On information and belief, the Leedarson Defendants design, develop, manufacture, import, distribute, offer to sell, sell, and use the Accused Products, including via the activities of Leedarson IoT and its subsidiaries, members, segments, companies, brands and/or related entities, such as U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson.

106. Defendants each directly infringe the '126 patent via 35 U.S.C. § 271(a) by manufacturing (including via contract manufacturers), 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 '126 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, parent, subsidiaries, members, segments, companies, brands, resellers, dealers, OEMs, integrators, installers, and/or consumers. Furthermore, on information and belief, Defendants design the Accused Products for U.S. consumers, make and sell the Accused Products outside of the United States, deliver those products to related entities, subsidiaries, online stores, distribution partners, retailers, showrooms,

resellers, dealers, installers, customers and other related service providers 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 and use in the United States, thereby directly infringing the '126 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)").

107. Furthermore, Defendant Leedarson IoT directly infringes the '126 patent through its direct involvement in the activities of its subsidiaries, and related entities, including Defendant Leedarson Lighting, and other U.S.-based subsidiaries, members, segments, companies and/or brands of Leedarson, including by designing the Accused Products for U.S. consumers and selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for sale and/or for its related entities. On information and belief, Leedarson's U.S.-based subsidiaries, including at least Leedarson America, conduct activities that constitute direct infringement of the '126 patent under 35 U.S.C. § 271(a) by importing, offering for sale, selling, and/or using those Accused Products in the U.S. on behalf of and for the benefit of Defendants, including parent company Leedarson IoT. Defendant Leedarson IoT is vicariously liable for the infringing conduct of Leedarson America and other U.S.-based subsidiaries, members, related entities, segments, companies and/or brands of Leedarson (under both the alter ego and agency theories). On information and belief, Defendants Leedarson IoT and Leedarson Lighting, and U.S. based subsidiaries members, segments, companies and/or brands of Leedarson are essentially the same company (i.e., "Leedarson"), operating in the U.S. via at least the

Leedarson America, AiDot, Anshe, Arnoo, Welove, Homax, Linkind, Orein, MuJoy, Winees, Syvio, Enhulk, ganiza, Hyderson, GoGonova brands, segments, mergers, or acquisitions of Leedarson. Moreover, Leedarson IoT, as the parent company, along with its related entities, has the right and ability to control and/or delegate the control of the infringing activities of those subsidiary entities such that Defendants each receive a direct financial benefit from that infringement.

108. For example, Defendants infringe claim 1 of the '126 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to Defendants' infringing Accused Products that are enabled or compliant with Wi-Fi and that utilize a battery and a volatile memory for the storage of device data, including cryptographic data. Such Accused Products include, but are not limited to control modules, smart lights, remotes, and sensors (e.g., the wines Water Leak Sensor Hub, model no. WP0500187, AiDot Orein Smart Light Bulbs Mini Switch Remote Button control, model no. OC02001-CR-B-US, AiDot Orein Smart RGBWW Recessed Lights with Wi-Fi App Control, model no. OD09002-RGBW-W-NA-4).

109. 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 media access controller (MAC) carried by said housing; and a cryptography circuit carried by said housing and connected to said MAC and said wireless transceiver, said cryptography circuit comprising at least one volatile memory for storing cryptography information, and a battery for maintaining the cryptography information in said at least one volatile memory.

110. At a minimum, Leedarson has known of the '126 patent at least as early as the filing date of this complaint. In addition, Leedarson has known about infringement of an L3Harris ("Harris") patent portfolio that was acquired by Stingray, which includes the '126 patent, since at least its receipt of a letter dated April 20, 2018, from North Forty Consulting LLC, working with Harris Corporation. The letter notifies Leedarson of Harris Corporation's (now L3 Harris Technologies, Inc.) ownership of patents relating to wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802.11 and Zigbee standards.

111. Additional correspondence sent by Stingray (a wholly owned subsidiary of Acacia Research Group LLC), regarding Stingray's acquisition and licensing attempt of the Harris patent portfolio (which Leedarson had notice of at least by April 20, 2018), was sent directly to Leedarson, on March 15, 2022. Leedarson did not respond. On March 22, 2022, a follow-up email was sent on behalf of Stingray to Leedarson again notifying Leedarson of and providing Leedarson with the opportunity to license Stingray's "portfolio of wireless networking patents." Again, Leedarson did not respond to this and several other subsequent attempts by Stingray to license the Harris patent portfolio which includes the '126 patent.

112. On information and belief, since at least the above-mentioned date or dates when Defendants were on notice of their infringement, Defendants have each actively induced, under 35 U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, integrators, installers, OEMs, consumers, other users, and other related service providers that import, distribute, purchase, offer for sale, sell, or use the Accused Products that include or are made using all of the limitations of one or more claims of the '126 patent to directly infringe one or more claims of the '126 patent by using, offering for sale, selling, and/or importing the Accused Products. Since at least the date or dates of notice provided above, Defendants each conduct

infringing activities with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '126 patent. On information and belief, Defendants each intend to cause, and have taken affirmative steps to induce, infringement by importers, online stores, distribution partners, retailers, reseller partners, dealers, OEMS, integrators, installers, consumers, other users, and other related service providers 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. Moreover, Defendants manufacture, test, and certify the Accused Products in conformity with and to operate within U.S. laws and regulations, including, for example, the FCC, specifically so that consumers may be induced to purchase and use the Accused Products. Also, Defendants distribute or make available instructions or manuals for these products to consumers, installers, purchasers and/or prospective buyers, test and certify the wireless networking features (with for example the Wi-Fi Alliance) in the Accused Products, and provide technical support, product files, videos, and/or related services for these products to purchasers in the United States. *See, e.g., Product Finder Filtered Results*, WIFI ALLIANCE, https://www.wi-fi.org/product-finder-results?keywords=leedarson (last visited Oct. 24, 2023) (showing Leedarson's WiFi Certified™ products include the "LA02301 WI-FI and Bluetooth SMART (BLE) Combo Module" with model number "LA02301" and "Last Certified Date: 2021-04-23," the "Smart A19 LED Light Bulb" with model number "13aSBA800STQ1T" and "Last Certified Date: 2023-09-25," and the "M-LA02302 WI-FI and Bluetooth SMART (BLE) Combo Module," with model number "M-LA02302" and "Last Certified Date: 2023-07-11," with several variants for each product); *LA02301 Module User Manual*, LEEDARSON, available at https://fccid.io/2AB2Q-LA02301/User-Manual/User-Manual-4959691.pdf (last visited Oct. 24, 2023); *Arnoo: A Cloud-based, Single-App*

*for Smart Living Solutions*, LEEDARSON, https://www.youtube.com/watch?v=dOdCF55ZouI (including a description that states "Arnoo can help you to integrate all your smart products into your one and only branded App, allows you to focus on the areas of expertise with which you are familiar" and displaying symbols indicating Wi-Fi and Zigbee compatibility in the video).

113. Furthermore, Defendants induce infringement by installers, integrators, consumers and other users of Leedarson's products by designing, developing, marketing, and offering smartphone and tablet interfaces as application software (i.e., apps) such as the AiDot App to provide access to the Accused Products to connect such products to and remotely control them via wireless networks, including Wi-Fi and ZigBee networks. *See, e.g., Control Your Smart Living arbitrarily : Smart Home App,* AIDOT, https://www.aidot.com/blog/post/smart-home-app (last visited Sep. 29, 2023).

114. Leedarson's apps also induce infringing use of the Accused Products by providing compatibility between Leedarson products and third-party products that share or access the same wireless networks. *See, e.g.*, *id* ("Besides, all the supported brands and third-party apps including Linkind, Winees, Orein, Ecobee, Honeywell Home, Alexa, Google Assistant, Smartthings, IFTTT of smart devices are listed in app for you to choose."); *Getting Started*, AIDOT, https://www.aidot.com/page/getting-start ("Link your Alexa or Google account with AiDot.") (last visited Sep. 29, 2023). Such compatibility provides convenience and added functionality that induces consumers to use the Defendants' products, including via the smartphone and tablet Wi-Fi apps and other interfaces utilizing Wi-Fi or ZigBee protocols in networks with other third-party devices. Thus, these activities further infringe or induce infringement of the '126 patent.

115. On information and belief, despite having knowledge of the '126 patent and knowledge that it is directly and/or indirectly infringing one or more claims of the '126 patent,

Defendants have nevertheless continued their infringing conduct and disregarded an objectively high likelihood of infringement. Each of Defendants' infringing activities relative to the '126 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.

116. Plaintiff Stingray has been damaged as a result of Defendants' infringing conduct described in this Count. Each Defendant is thus jointly and severally liable to Stingray in an amount that adequately compensates Stingray for their 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

117. 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.

118. 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

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

## PRAYER FOR RELIEF

120. 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: October 24, 2023

Respectfully submitted,

*/s/ Jeffrey R. Bragalone*
Jeffrey R. Bragalone (lead attorney)
Texas Bar No. 02855775
E-mail: jbragalone@bosfirm.com
Terry A. Saad
Texas Bar No. 24066015
E-mail: tsaad@bosfirm.com
Marcus Benavides
Texas Bar No. 24035574
E-mail: mbenavides@bosfirm.com
Brandon Zuniga
Texas Bar no. 24088720
E-mail: bzuniga@bosfirm.com
Mark M. R. Douglass
Texas Bar No. 24131184
E-mail: mdouglass@bosfirm.com
**BRAGALONE OLEJKO SAAD PC**
901 Main Street
Suite 3800
Dallas, Texas 75202
Telephone: (214) 785-6670
Facsimile: (214) 785-6680

Wesley Hill
Texas Bar No. 24032294
E-mail: wh@wsfirm.com
**WARD, SMITH, & HILL, PLLC**
P.O. Box 1231
Longview, Texas 75606
Telephone: (903) 757-6400
Facsimile: (903) 757-2323

**ATTORNEYS FOR PLAINTIFF**
**STINGRAY IP SOLUTIONS LLC**