

3. On information and belief, Defendant Somfy Activités SA (“Somfy Activites”) is a company organized under the laws of France, with its principal place of business located at 50 avenue du Nouveau Monde, 74300 Cluses, France. Somfy SA and Somfy Activites share the same headquarters in France. Moreover, Somfy Activites is a wholly owned and controlled subsidiary of Somfy SA, and Somfy Activites is part of a multi-national group of companies (“the Somfy Group”) of which Somfy SA is the parent and controlling entity.

4. On information and belief, Somfy SA was founded in 1969. *See Annual Financial Report*, p. 112, SOMFY SA, available for download at <https://www.somfy-group.com/en-en/finance/documentation/financial-reports> (last visited May 26, 2021). Today, it operates in 58 countries, including the U.S. *Id.* at p. 8.

5. On information and belief, the Somfy SA states that the Group is “the global leader in opening and closing automation for both residential and commercial buildings.” *Id.* at p. 112. Somfy SA further states that it is “a pioneer in the connected home.” *Id.* Somfy SA along with its subsidiaries in the Somfy Group, including Somfy Activites, are engaged in research and development, manufacturing, importation, distribution, sales, and related technical services for motorized shades, blinds, curtains, awnings, screens, pergolas, and rolling shutters for residential and commercial applications. *See Products*, SOMFY, <https://www.somfysystems.com/en-us/products/shades-blinds-curtains/motorized-blinds-shades> (last visited May 26, 2021). Moreover, the Somfy Group provides smart home applications, controls, and automation systems to enhance the consumers use of Somfy’s products. *Id.* Somfy’s products are manufactured outside the U.S. and then imported into the United States, distributed, and sold to end-users via the internet and in brick and mortar stores and/or via dealers and “Somfy experts” in the U.S., in Texas and the Eastern District of Texas.

6. On information and belief, Somfy maintains a corporate presence in the United States, including in Texas and in this District, via at least its wholly owned and controlled U.S.-based subsidiaries, including Somfy Systems Inc. (“Somfy Systems”), which is a Delaware corporation with its principal office located at 121 Herrod Blvd., Dayton, NJ 08810. *See List of Consolidated and Equity-Accounted Entities, Annual Financial Report*, p. 149-151. On behalf and for the benefit of Defendants, Somfy Systems coordinates the importation, distribution, marketing, offers for sale, sale, and use of the Somfy’s products in the U.S. For example, Somfy Systems maintains distribution channels in the U.S. for Somfy products via online stores, distribution partners, retailers, reseller partners, dealers, and other related service providers. *See Where to Buy, SOMFY*, <https://www.somfysystems.com/en-us/where-to-buy> (accessible via menu “Where to Buy” and providing links for “Search Our Dealer Locator,” “Connect With a Local Somfy Dealer,” and “Shop Online for Somfy Controls & Accessories”) (last visited May 26, 2021). Somfy Systems’ registered agent in Delaware is The Prentice-Hall Corporation System, Inc., 251 Little Fallas Drive, Wilmington, DE 19808.

7. On information and belief, Somfy maintains a corporate presence in the United States, including in Texas and in this District, also via at least its wholly owned and controlled U.S.-based subsidiary BFT Americas, Inc. (“BFT”), which is a Florida corporation with its principal office located at 1200 SW 35th Avenue, Suite B, Boynton Beach, FL 33426. *See List of Consolidated and Equity-Accounted Entities, Annual Financial Report*, p. 149-151. BFT’s registered agent for service is Gary Goldstein located also at 1200 SW 35th Avenue, Suite B, Boynton Beach, FL 33426. BFT specializes in “gate automation, sliding gates, swing gates, automatic doors, bollards, barriers, and access control.” *See BFT Americas, Inc.*, LINKEDIN, <https://www.linkedin.com/company/bft-u.s.-inc./about/> (last visited May 26, 2021). BFT provides

its products and services as a “brand of Somfy Group,” and has been “a part of the Somfy group” since 2004, allowing it to “create a structured distribution network.” *See Our History*, BFT, https://www.bft-automation.com/en_US/bft/our-history/ (last visited May 26, 2021).

8. On information and belief, Somfy also maintains wholly owned and controlled subsidiary Somfy, LLC (“Somfy LLC”), which is a limited liability company organized under the laws of Delaware. *See List of Consolidated and Equity-Accounted Entities, Annual Financial Report*, p. 149-151. Somfy LLC’s registered agent in Delaware is Corporate Agents, Inc. located at 1209 Orange St., Wilmington, DE 19801.

9. As a result, via at least Somfy’s established distribution channels operated and maintained by at least Somfy’s U.S. based subsidiaries in concert with the Somfy Group, including Defendant Somfy DA and wholly owned and controlled Defendant Somfy Activites, Somfy products are distributed, sold, advertised, and used nationwide, including being sold to consumers via Somfy dealers operating in Texas and this District. Thus, Defendants do business in the U.S., 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 Somfy SA

12. On information and belief, Somfy SA 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, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, Somfy SA is related to, owns, and/or controls subsidiaries (such as Somfy Systems, BFT, and Somfy LLC) and business sectors (such as its Somfy and BFT business) 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 Somfy products in Texas, including in this District.

13. This Court has personal jurisdiction over Defendant Somfy SA, directly and/or through the activities of Somfy SA's intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including through the activities of Defendant Somfy Activites, other members of the Somfy Group, and U.S. based subsidiaries. Through direction and control of these entities, Somfy SA 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 Somfy SA would not offend traditional notions of fair play and substantial justice.

14. On information and belief, Somfy SA controls or otherwise directs and authorizes all activities of its subsidiaries and related entities, including, but not limited to Defendant Somfy Activites, other members of the Somfy Group, and U.S. based subsidiaries. Directly via its agents in the U.S. and via at least distribution partners, retailers, reseller partners, dealers, professional

installers, and other service providers, Somfy SA has placed and continues to place infringing Somfy products into the U.S. stream of commerce. For example, import records show that Somfy SA's subsidiary and Defendant Somfy Activites supplies Somfy products to Somfy Systems in the U.S. *See, e.g., U.S. Customs Records for Somfy Activites SA*, IMPORT GENIUS, <https://www.importgenius.com/suppliers/somfy-activites-sa> (showing shipments to Somfy Systems totaling "22" in the period from 2006 to 2021). Somfy SA 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. Somfy utilizes established distribution channels to distribute, market, offer for sale, sell, service, and warrant infringing products directly to consumers and other users, including providing links via its own website to online stores, retailers, detailers, resellers, distributors, and dealers offering such products and related services for sale. *See Where to Buy*, SOMFY, <https://www.somfysystems.com/en-us/where-to-buy> (accessible via menu "Where to Buy" and providing links for "Search Our Dealer Locator," "Connect With a Local Somfy Dealer," and "Shop Online for Somfy Controls & Accessories") (last visited May 26, 2021). Such Somfy products and services have been sold in both brick and mortar and online retail stores and showrooms within this District and in Texas, including Universal Screens located in Plano, Texas.

See, e.g., Contact Us, Universal Screens (showing that Somfy products are used in Universal Screen products and sold from the showroom located at 1801 10th Street, Suite 100, Plano, TX 75074, i.e., in this District). Somfy also sells to third-party manufacturers, such as Universal Screens, who integrate Somfy products into their own products to add automation features. *See id.* (“Screen/Shade Manufacturing...We have made sure to align ourselves with some of the best vendors in the industry, including Somfy...”). Somfy products are also sold via the national retailer Amazon.com. *See, e.g., Somfy MyLink RTS Smartphone and Tablet Interface/WiFi to Radio Technology Control Blinds with phone!*, AMAZON.COM, https://www.amazon.com/Somfy-RTS-Smartphone-Technology-1811403/dp/B00USMNU14/ref=sr_1_5?dchild=1&keywords=somfy&qid=1622135026&sr=8-5 (last visited May 27, 2021). Somfy, via its wholly owned and controlled subsidiaries, also provides application software (“apps”), the “myLink” app for download and use in conjunction with and as a part of the wireless communication network that connects Somfy products and other network devices. *See, e.g., Systems Requirements*, SOMFY SYSTEMS, <https://www.somfysystems.com/en-us/products/smart-home-controls/controls/mylink> (“Download the myLink™ App...The myLink™ app is available on the Apple App Store and Google Play.”) (last visited May 27, 2021). These apps are available via digital distribution platforms operated by Apple Inc. and Google for download by users and execution on smartphone devices. *Id.*

16. Based on Somfy SA’s connections and relationship with manufacturers, dealers, retailers, and digital distribution platforms, Somfy SA knows that Texas is a termination point of the established distribution channel, namely online and brick and mortar stores offering Somfy 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. Somfy SA, 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, Somfy SA alone and in concert with other related entities such as Defendant Somfy Activites, and subsidiaries Somfy Systems, BFT, and Somfy LLC, manufactures and purposefully places infringing Somfy 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 listed on Somfy Systems’ website. For example, Somfy SA imports to Texas or through a related entity or subsidiary and directly sells and offers for sale infringing Somfy products in Texas to resellers or dealers. Ross Howard Designs, for example, advertises that it services the DFW area including “Addison, Castle Hills, Flower Mound, Fort Worth, Garland, Highland Park, Little Elm, Lakewood, Park Cities, University Park, White Rock Lake, TX and surrounding areas,” which includes areas in this District. *See, e.g., Motorized Blinds, Shades and Draperies*, ROSS HOWARD DESIGNS, <https://rosshoward.com/window-treatment-motorization/>. Other resellers and/or dealers, such as Shade Works of Texas, offer infringing Somfy products for sale on their website. *See, e.g., Motorized Blinds & Shades Powered by Somfy*, SHADE WORKS OF TEXAS, <https://shadeoftexas.wpengine.com/motorized-blinds-shades/> (providing a webpage within its own website devoted to Somfy products offered for sale) (last visited May 27, 2021). These suppliers, distributors, dealers, and/or resellers import, advertise, offer for sale and sell Somfy

products and 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 Somfy SA'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 Ross Howard Designs and Shade Works of Texas, Somfy SA knows and has known that Texas is a termination point of the established distribution channels for Somfy products. Somfy SA, alone and in concert with subsidiaries Defendant Somfy Activites, and U.S.-based Somfy Systems, BFT, and Somfy LLC 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 Somfy SA under Federal Rule of Civil Procedure 4(k)(2), because the claims for patent infringement in this action arise under federal law, Somfy SA is not subject to the jurisdiction of the courts of general jurisdiction of any state, and exercising jurisdiction over Somfy SA is consistent with the U.S. Constitution.

19. Venue is proper in this District pursuant to 28 U.S.C. § 1391. Defendant Somfy SA 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 Somfy Activites

20. On information and belief, Defendant Somfy Activites 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, Somfy Activites and parent Defendant Somfy SA and U.S.-based subsidiaries Somfy Systems, BFT, and Somfy LLC manufacture, import, distribute, offer for sale, sell, and induce infringing use of Somfy products to distribution partners, retailers (including national retailers), resellers, dealers, service providers, consumers, and other users.

21. This Court has personal jurisdiction over Somfy Activites, directly and/or indirectly via the activities of Somfy Activites’s intermediaries, agents, related entities, distributors, importers, customers, subsidiaries, and/or consumers, including parent Defendant Somfy SA and U.S.-based subsidiaries Somfy Systems, BFT, and Somfy LLC. Alone and in concert with or via direction and control of or by at least these entities, Somfy Activites 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, Somfy

Activites operates within a global network of sales and distribution of Somfy products that includes subsidiaries of Somfy, retail stores and showrooms, dealers, resellers, professional installers, and distributors operating in Texas, including this District.

22. As a part of Somfy's global manufacturing and distribution network, Somfy Activites also purposefully places infringing Somfy 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. For example, Somfy Activites imports Somfy products directly to subsidiary Somfy Systems Inc. in containers marked "SOMFY USA" in May 2021. *See Search Global Trade Data*, SEAIR, EXIM SOLUTION, <https://www.seair.co.in/us-import/shipments-of-119329082.aspx> (last visited May 27, 2021). Therefore, Somfy Activites, alone and in concert with other members of the Somfy Group, its parent entity Defendant Somfy SA and its U.S. based Somfy 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 Somfy SA, Somfy Activites 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 Somfy Activites would not offend traditional notions of fair play and substantial justice.

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

24. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because, among other things, Somfy Activites is not a resident in the United States, and thus may be sued in any judicial district, including this one, pursuant to 28 U.S.C. § 1391(c)(3).

25. On information and belief, Defendants Somfy SA and Somfy Activites each have significant ties to, and presence in, the State of Texas and this District, making venue in this District both proper and convenient for this action.

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

28. 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.

29. 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.

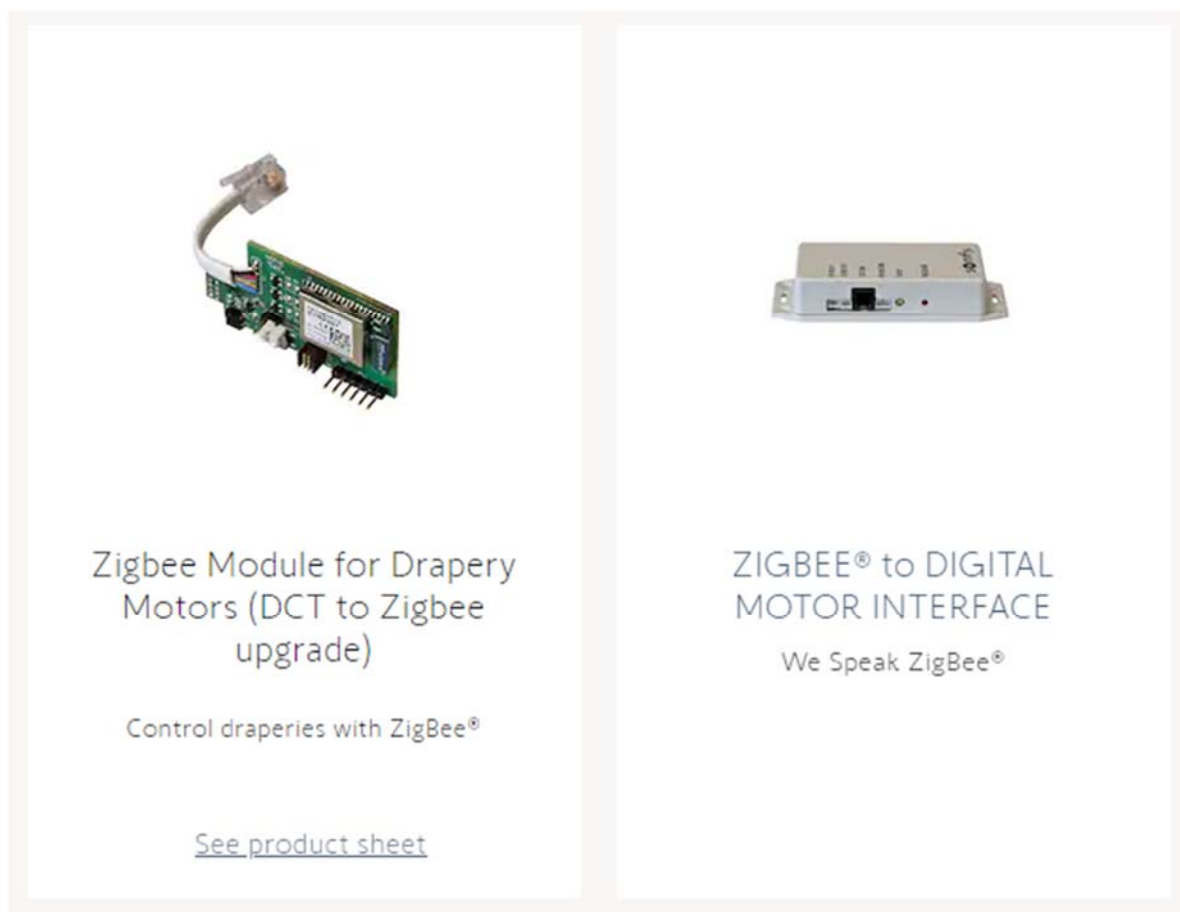
30. The '572 patent involves providing secure wireless local area networks (LAN). A device for securing such a LAN may include a housing with a wireless transceiver carried by the housing. A medium access controller (MAC) also carried by the housing. A cryptography circuit may be connected to the MAC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

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 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, Somfy reported for North America 107 million euros in sales in 2020 (about \$130.5 million U.S. dollars). *See Annual Financial Report*, p. 116.

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 Z-Wave, ZigBee, and Wi-Fi. *See, e.g., Smart Home Controls for Motorized Window Coverings*, SOMFY, <https://www.somfysystems.com/en-us/products/smart-home-controls/smart-homeSomfy> (last visited May 27, 2021). Somfy also utilizes its own proprietary protocol Radio Technology Somfy (“RTS”) and has products that translate between one protocol (Wi-Fi, Z-Wave, or ZigBee) and RTS so that consumers may control Somfy products via other third-party devices or communication platforms. *See id.* (“Through Somfy myLink™, easily connect your Somfy blinds, shades, awning, and more with handheld smart devices or third-party smart home services like Amazon Alexa and IFTTT.”). Defendants’ infringing Somfy products include, but are not limited to, ZigBee modules and digital motor interfaces, Z-Wave digital motor interface, motor modules, and Z-Wave to RTS Plug-in Wall module, and myLink RTS smartphone and tablet Wi-Fi interfaces, 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 Somfy that use the ZigBee protocol to communicate with other devices on a communication network, including those of third-party manufacturers. Examples of the Somfy’s ZigBee products include the “Zigbee Module for Drapery Motors,” including (model no. 1870221) which “[r]eceives ZigBee® transmissions and converts

them to motor control commands,” and “ZigBee® to Digital Motor Interface,” which “[a]ccepts commands from ZigBee® remotes” are shown below:



See Search results for “Zigbee,” SOMFY, <https://www.somfysystems.com/en-us/search?q=zigbee> (last visited May 27, 2021); see also <https://www.somfysystems.com/en-us/products/1870221/zigbee-module-for-drapery-motors-dct-to-zigbee-upgrade>; <https://www.somfysystems.com/en-us/products/1870220/zigbee-to-digital-motor-interface>.

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 plurality of network nodes.

IEEE STANDARDS ASSOCIATION

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

4.5 Functional overview

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

4.5.1 Superframe structure

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

5.1.1.1.1 Contention access period (CAP)

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

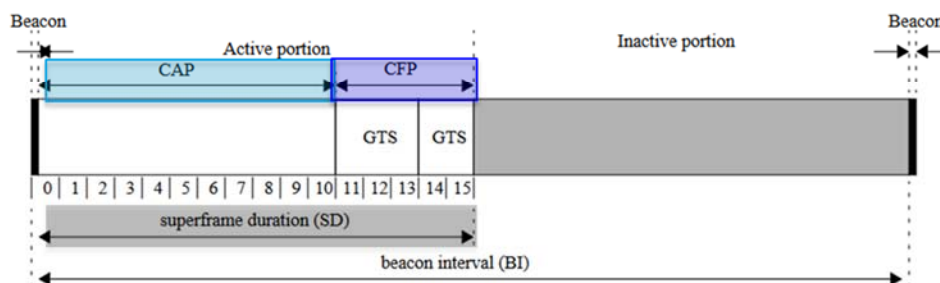


Figure 8—An example of the superframe structure

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

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

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

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

5.1.7.2 GTS allocation

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

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

5.2.2.1.2 Superframe Specification field

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

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

Figure 41—Format of the Superframe Specification field

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

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

5.1.7.1 CAP maintenance

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

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

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

5.1.7.1 CAP maintenance

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

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

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

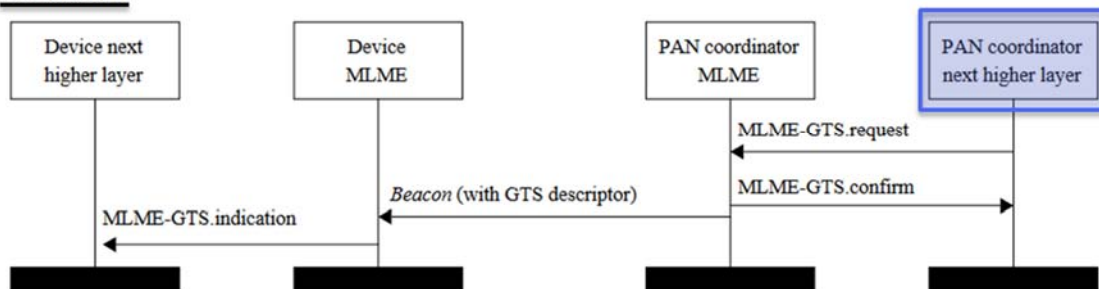


Figure 32—Message sequence chart for GTS deallocation initiated by the PAN coordinator

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

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

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



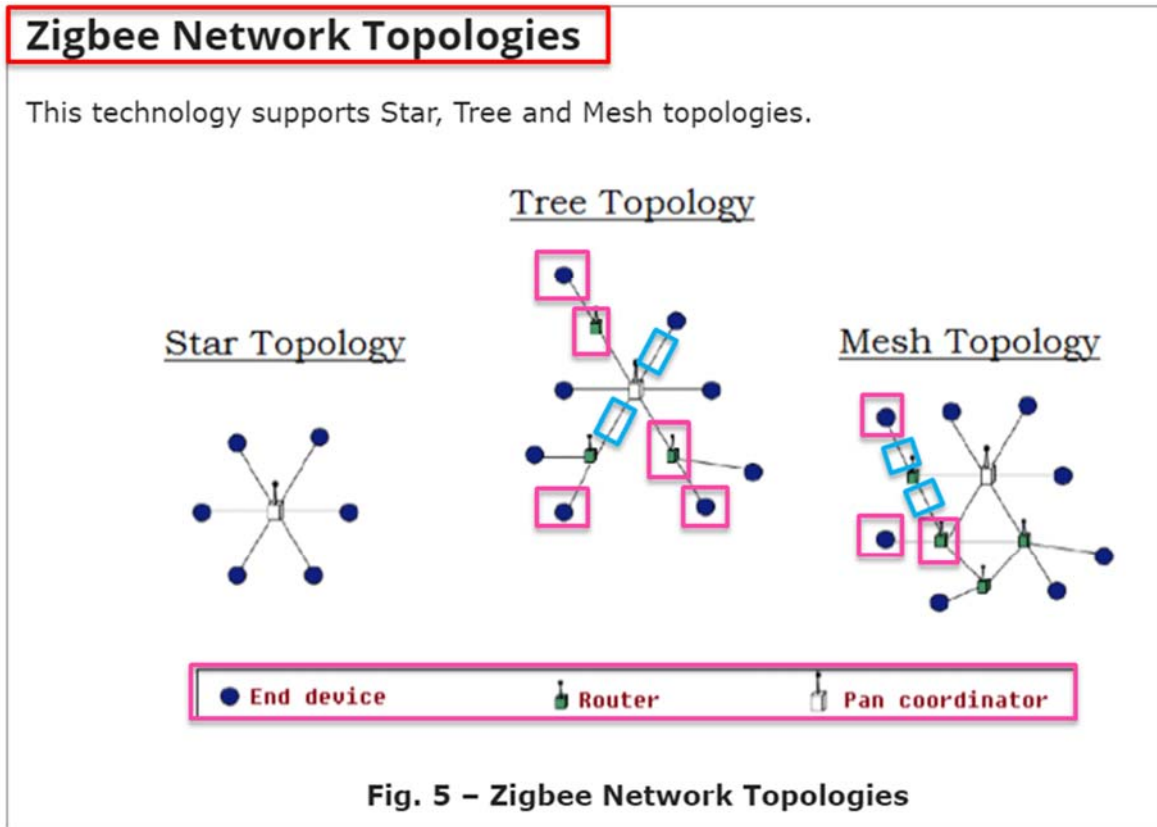
A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated 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 procedure¹:

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 acknowledgement 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>

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



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

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

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



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

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

Each router or coordinator is responsible for tracking transmit failures using the TransmitFailure field in the neighbor table and also keeping a NIB counter for total transmissions attempted. A device that detects a significant number of transmission failures may take action to determine if interference is a cause. The following steps are an example of that procedure¹:

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 acknowledgement 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>

42. 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.



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 procedure¹:

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 than 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 acknowledgement 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>

43. 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.

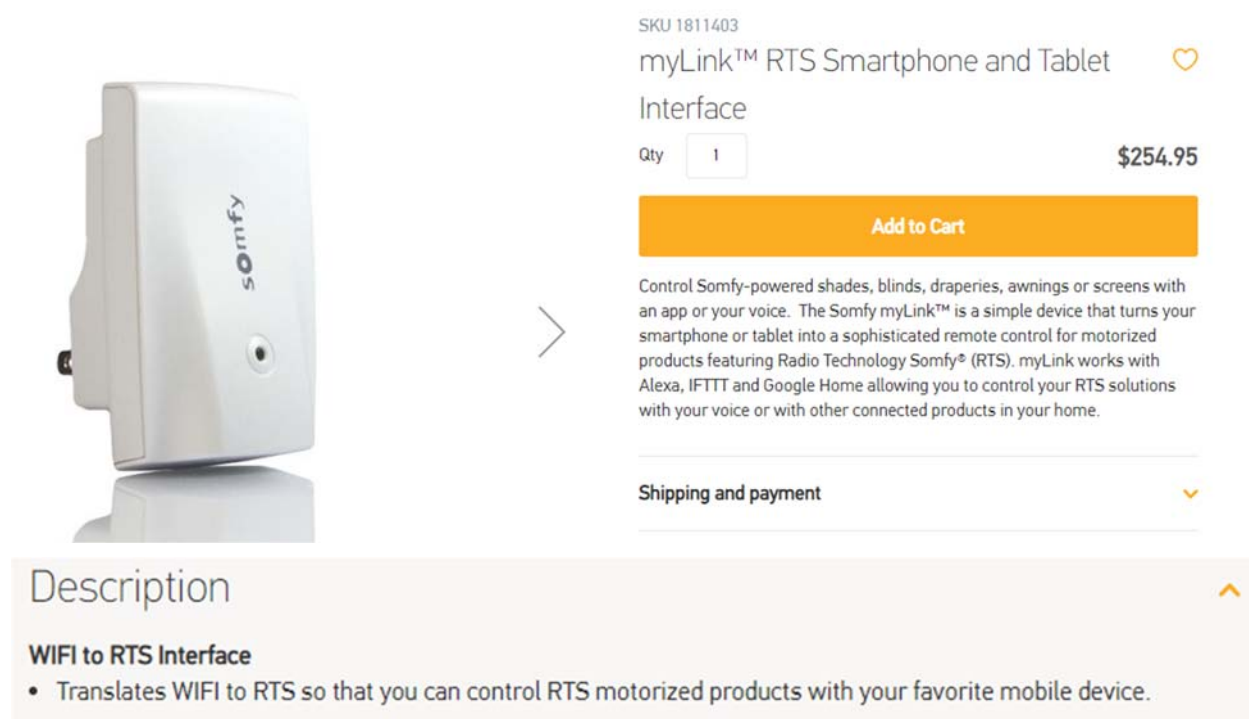
The network manager may do the following:


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>

44. The Asserted Patents also cover Accused Products of Somfy that utilize the Wi-Fi protocol. Such products include the myLink™ RTS Smartphone and Tablet Interface, which “turns your smartphone or tablet into a sophisticated remote control for motorized products featuring Radio Technology Somfy® (RTS) [and] works with Alexa, IFTTT and Google Home allowing you to control your RTS solutions with your voice or with other connected products in your home.” See *myLink™ RTS Smartphone and Tablet Interface*, SOMFY, <https://store.somfysystems.com/mylink-rt-smartphone-and-tablet-interface.html> (scroll down and access “Description”) (last visited May 27, 2021). As shown below, the myLink is Wi-Fi (IEEE 802.11) compliant:





SKU 1811403
myLink™ RTS Smartphone and Tablet Interface 

Qty \$254.95

Add to Cart

Control Somfy-powered shades, blinds, draperies, awnings or screens with an app or your voice. The Somfy myLink™ is a simple device that turns your smartphone or tablet into a sophisticated remote control for motorized products featuring Radio Technology Somfy® (RTS). myLink works with Alexa, IFTTT and Google Home allowing you to control your RTS solutions with your voice or with other connected products in your home.

Shipping and payment 

Description 

WIFI to RTS Interface

- Translates WIFI to RTS so that you can control RTS motorized products with your favorite mobile device.

See *myLink™ RTS Smartphone and Tablet Interface*, SOMFY, <https://store.somfysystems.com/mylink-rt-smartphone-and-tablet-interface.html> (last visited May 27, 2021).

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

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

8.3.2.3 TKIP MIC

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

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

8.3.2.3.1 Motivation for the TKIP MIC

Before defining the details of the MIC, it is useful to review the context in which this mechanism operates.

Active attacks enabled by the original WEP design include the following:

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

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

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

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

46. 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>

47. 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>

48. 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>

49. 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>

50. The Asserted Patents also cover Somfy's Wi-Fi compliant devices, which support WPA and WPA2-AES security mechanisms, as described below and in the following paragraph.

Of the WPA and WPA2 security mechanism used by the Accused Products, such as Somfy's smart home Wi-Fi devices, the WPA is based on Temporal Key Integrity Protocol (TKIP), while, as described below, the WPA2-AES is based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below is an exemplary IEEE 802.11 compliant myLink RTS Smartphone and Tablet Interface. The device has a housing.

myLink™ RTS

Smartphone and Tablet Interface


Item #: 1811403




OVERVIEW:

The **myLink™ RTS Smartphone and Tablet Interface** is a WiFi to Radio Technology Somfy® (RTS) bridge that can control up to 16 channels of RTS motorized products using the Somfy myLink apps for iOS and Android devices. Through the app, users can send immediate RTS commands, create scenes (a group of motorized products working together) and schedules (timed events). Users may access their myLinks from anywhere with the app's remote access feature. Though the myLink is a single-zone controller, multiple myLinks can be joined within the same system for multi-zone control. The myLink can also be used as a WiFi to RTS interface for integration with third-party control systems and is compatible with the Somfy Synergy™ API and Amazon Alexa (Recommended for spaces up to 4,000 sq. ft.).

For information about the original myLink (Legacy version), see Legacy spec sheet. Legacy myLinks are identified with the status LED and setup button on the right side of the unit, and device IDs beginning with "AAAA" (EX: AAAA1234).



TECHNICAL SPECIFICATIONS:

- 120V AC; 50-60Hz
- Ultra Low Power Wi-Fi (802.11 a/b/g/n)
- 3.64" L x 2.35" W x 1.95" H
- Radio Frequency:
 - RTS 433.42 MHz
 - WiFi: 2.4 & 5GHz
- iOS Version: 7 and higher
- Android Version: Jelly Bean and higher
- FCC ID: DWNMYLINK
- Operating Temp: 41°F to 113°F (5°C to 45°C)
- Rated Current (Amps): 10 to 50 milliamps
- Insulation Class: Class II
- For Indoor Use Only
- Enclosure:
 - PE
 - UL94V-0 flame rating
 - RoHS compliant
- Shipping Weight: 1lb

FEATURES SUMMARY:

- Control for up to 16 RTS channels per myLink™ from iOS and Android devices
- Join up to 10 myLinks together for multi-zone control
- Manually activate RTS products
- Automate window coverings with scenes and schedules
- Supports Up/Down/My/Stop commands and incremental control (tilt/brightness)
- Multiple users
- Remote access
- Integration with third-party systems over IP
- Compatible with Somfy Synergy™ API
- Compatible with Amazon Alexa and Google Assistant via IFTTT

WHAT'S IN THE BOX:

- myLink™
- Quick Start Guide

Source: https://service.somfy.com/downloads/nam_v5/mylinkv2_-_legacy_spec_sheet_5.4.2020.pdf

51. As shown below, the Accused Products provide 2.4 GHz and 5 GHz Wi-Fi speeds. This capability ascertains the presence of a Wi-Fi antenna and transceiver in the device and provides a secure wireless LAN. The device also has a housing.



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

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

8.3.2 Temporal Key Integrity Protocol (TKIP)

8.3.2.1.1 TKIP cryptographic encapsulation

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

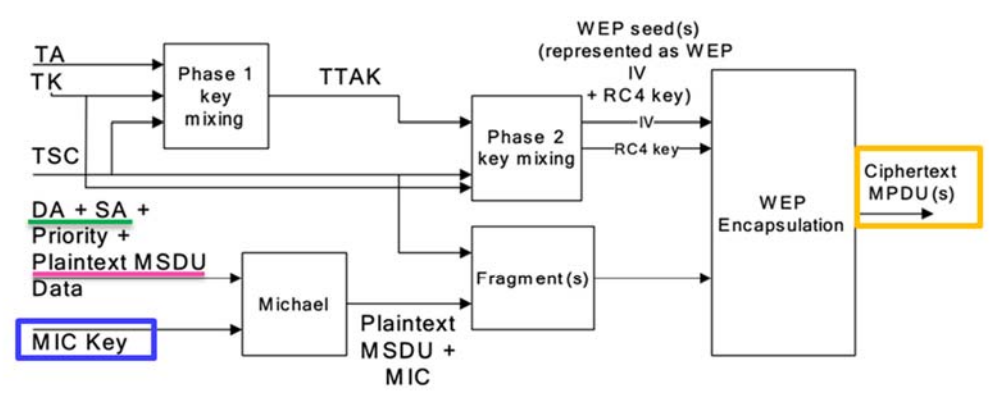


Figure 8-4—TKIP encapsulation block diagram

- a) TKIP MIC computation protects the MSDU Data field and corresponding SA, DA, and Priority fields. The computation of the MIC is performed on the ordered concatenation of the SA, DA, Priority, and MSDU Data fields. The MIC is appended to the MSDU Data field. TKIP discards any MIC padding prior to appending the MIC.
- b) If needed, IEEE Std 802.11 fragments the MSDU with MIC into one or more MPDUs. TKIP assigns a monotonically increasing TSC value to each MPDU, taking care that all the MPDUs generated from the same MSDU have the same value of extended IV (see 8.3.2.2).
- c) For each MPDU, TKIP uses the key mixing function to compute the WEP seed.
- d) TKIP represents the WEP seed as a WEP IV and ARC4 key and passes these with each MPDU to WEP for generation of the ICV (see 7.1.3.6), and for encryption of the plaintext MPDU, including all or part of the MIC, if present. WEP uses the WEP seed as a WEP default key, identified by a key identifier associated with the temporal key.

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

COUNT I

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

53. Plaintiff incorporates paragraphs 1 through 52 herein by reference.

54. Plaintiff is the assignee of the '117 patent, entitled “Mobile ad-hoc network with intrusion detection features and related methods,” with ownership of all substantial rights in the

'117 patent, including the right to exclude others and to enforce, sue, and recover damages for past and future infringements.

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

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

57. On information and belief, Somfy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Somfy and its subsidiaries or related entities, such as Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC.

58. Defendants each directly infringe the '117 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '117 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, subsidiaries, 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 '117 patent. *See, e.g., Lake Cherokee Hard*

Drive Techs., L.L.C. v. Marvell Semiconductor, Inc., 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers ... constitute an infringing sale under § 271(a)”).

59. Furthermore, Defendant Somfy directly infringes the ’117 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S. based subsidiaries, including at least Somfy Systems and BFT, conduct activities that constitute direct infringement of the ’117 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. Somfy SA is vicariously liable for the infringing conduct of Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC (under both the alter ego and agency theories). On information and belief, Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC are essentially the same company, comprising some members of the Somfy Group. Moreover, Somfy SA, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

60. For example, Somfy infringes claim 24 of the ’117 patent via the Accused Products that utilize ZigBee protocols, including, but not limited to ZigBee modules and digital motor interfaces and related accessories and software.

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

62. At a minimum, Somfy has known of the ’117 patent at least as early as the filing date of this complaint. In addition, Somfy has known about the ’117 patent since at least its receipt of a letter from North Forty Consulting representing Harris Corporation (“Harris”) dated April 20, 2018, regarding infringement of Harris’ patent portfolio. The letter specifically references the ’117 patent and notifies Somfy of its infringing use of “wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standards,” in at least the “ZigBee to Digital Motor Interface; ZigBee Module for Curtain Motorization; Glydea; Temperature & Humidity Sensor; Opening Sensor; Motion Detector.”

63. On information and belief, since at least the above-mentioned date when Somfy was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, 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 ’117 patent to directly infringe one or more claims of the ’117 patent by using, offering for sale,

selling, and/or importing the Accused Products. Since at least the notice provided on the above-mentioned date, Defendants each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '117 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, consumers, 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, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g., Service & Support*, SOMFY, <https://www.somfysystems.com/en-us/discover-somfy/contact-us/service-support> (providing consumers with “help with an existing project”); *see also somfysystems*, YOUTUBE.COM, <https://www.youtube.com/user/somfysystems> (providing consumers with Somfy-produced how-to videos related to Somfy products) (last visited May 27, 2021). Furthermore, Somfy markets myLink RTS smartphone and tablet interface and its application software as “a simple device that turns your smartphone or tablet into a sophisticated remote control for motorized products featuring Radio Technology Somfy® (RTS) [and] works with Alexa, IFTTT and Google Home allowing you to control your RTS solutions with your voice or with other connected products in your home.” *See myLink™ RTS Smartphone and Tablet Interface*, SOMFY, <https://store.somfysystems.com/mylink-rt-smartphone-and-tablet-interface.html> (scroll down and access “Description”) (last visited May 27, 2021). Such compatibility provides convenience

and added functionality that induces consumers to use Somfy products, including ZigBee modules and digital motor interfaces and myLink RTS smartphone and tablet Wi-Fi interfaces utilizing ZigBee and/or WiFi protocols in networks with other third-party devices, and thus further infringe the '117 patent.

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

65. Plaintiff Stingray has been damaged as a result of Somfy'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 Somfy's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT II

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

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

67. 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.

68. 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.

69. Somfy 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.

70. On information and belief, Somfy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Somfy and its subsidiaries or related entities, such as Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC.

71. 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, subsidiaries, 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)”).

72. Furthermore, Defendant Somfy directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S. based subsidiaries, including at least Somfy Systems and BFT, 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. Somfy SA is vicariously liable for the infringing conduct of Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC (under both the alter ego and agency theories). On information and belief, Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC are essentially the same company, comprising some members of the Somfy Group. Moreover, Somfy SA, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

73. For example, Somfy infringes claim 51 of the '678 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to the myLink RTS smartphone and tablet Wi-Fi interfaces, and related accessories and software.

74. 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.

75. At a minimum, Somfy has known of the ’678 patent at least as early as the filing date of this complaint. In addition, Somfy has known about infringement of Harris Corporation’s (“Harris”) patent portfolio, which includes the ’678 patent, since at least its receipt of a letter from North Forty Consulting representing Harris dated April 20, 2018. The letter notifies Somfy of its infringing use of “wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standards,” in at least the “ZigBee to Digital Motor Interface; ZigBee Module for Curtain Motorization; Glyde; Temperature & Humidity Sensor; Opening Sensor; Motion Detector.”

76. On information and belief, since at least the above-mentioned date when Somfy was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, 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 notice provided on the above-mentioned date, Defendants each do so 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, consumers, 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, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g., Service & Support*, SOMFY, <https://www.somfysystems.com/en-us/discover-somfy/contact-us/service-support> (providing consumers with “help with an existing project”); *see also somfysystems*, YOUTUBE.COM, <https://www.youtube.com/user/somfysystems> (providing consumers with Somfy-produced how-to videos related to Somfy products) (last visited May 27, 2021). Furthermore, Somfy markets myLink RTS smartphone and tablet interface and its application software as “a simple device that turns your smartphone or tablet into a sophisticated remote control for motorized products featuring Radio Technology Somfy® (RTS) [and] works with Alexa, IFTTT and Google Home allowing you to control your RTS solutions with your voice or with other connected products in your home.” *See myLink™ RTS Smartphone and Tablet Interface*, SOMFY, <https://store.somfysystems.com/mylink-rt-smartphone-and-tablet-interface.html> (scroll down and access “Description”) (last visited May 27, 2021). Such compatibility provides convenience

and added functionality that induces consumers to use Somfy products, including the myLink RTS smartphone and tablet Wi-Fi interfaces utilizing ZigBee protocols in networks with other third-party devices, and thus further infringe the '678 patent.

77. 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, Somfy has nevertheless continued its 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.

78. Plaintiff Stingray has been damaged as a result of Somfy'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 Somfy's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT III

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

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

80. 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.

81. 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.

82. Somfy 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.

83. On information and belief, Somfy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Somfy and its subsidiaries or related entities, such as Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC.

84. Defendants each directly infringe the '572 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '572 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers, importers, customers, subsidiaries, 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 '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)").

85. Furthermore, Defendant Somfy directly infringes the '572 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S. based subsidiaries, including at least Somfy Systems and BFT, 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. Somfy SA is vicariously liable for the infringing conduct of Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC (under both the alter ego and agency theories). On information and belief, Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC are essentially the same company, comprising some members of the Somfy Group. Moreover, Somfy SA, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

86. For example, Somfy infringes claim 1 of the '572 patent via the Accused Products that utilize 802.11 (Wi-Fi) protocols, including, but not limited to the myLink RTS smartphone and tablet Wi-Fi interfaces, and related accessories and software.

87. 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.

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

89. Somfy 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.

90. At a minimum, Somfy has known of the '572 patent at least as early as the filing date of this complaint. In addition, Somfy has known about the '572 patent since at least its receipt of a letter from North Forty Consulting representing Harris Corporation ("Harris") dated April 20, 2018, regarding infringement of Harris' patent portfolio. The letter specifically references the '572

patent and notifies Somfy of its infringing use of “wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standards,” in at least the “ZigBee to Digital Motor Interface; ZigBee Module for Curtain Motorization; Glydea; Temperature & Humidity Sensor; Opening Sensor; Motion Detector.”

91. On information and belief, since at least the above-mentioned date when Somfy was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, 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 notice provided on the above-mentioned date, Defendants each do so 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, consumers, 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, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or services for these products to purchasers in the United States. *See, e.g., Service & Support, SOMFY*, <https://www.somfysystems.com/en-us/discover-somfy/contact-us/service-support> (providing

consumers with “help with an existing project”); *see also somfysystems*, YOUTUBE.COM, <https://www.youtube.com/user/somfysystems> (providing consumers with Somfy-produced how-to videos related to Somfy products) (last visited May 27, 2021). Furthermore, Somfy markets myLink RTS smartphone and tablet interface and its application software as “a simple device that turns your smartphone or tablet into a sophisticated remote control for motorized products featuring Radio Technology Somfy® (RTS) [and] works with Alexa, IFTTT and Google Home allowing you to control your RTS solutions with your voice or with other connected products in your home.” *See myLink™ RTS Smartphone and Tablet Interface*, SOMFY, <https://store.somfysystems.com/mylink-rt-smartphone-and-tablet-interface.html> (scroll down and access “Description”) (last visited May 27, 2021). Such compatibility provides convenience and added functionality that induces consumers to use Somfy products, including the digital motor interfaces and myLink RTS smartphone and tablet Wi-Fi interfaces utilizing ZigBee and/or WiFi protocols in networks with other third-party devices, and thus further infringe the ’572 patent.

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

93. Plaintiff Stingray has been damaged as a result of Somfy’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 Somfy's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

COUNT IV

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

94. Plaintiff incorporates paragraphs 1 through 93 herein by reference.

95. 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.

96. 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.

97. Somfy 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.

98. On information and belief, Somfy designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via the activities of Somfy and its subsidiaries or related entities, such as Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC.

99. Defendants each directly infringe the '961 patent via 35 U.S.C. § 271(a) by making, offering for sale, selling, and/or importing the Accused Products, their components, and/or products containing the same that incorporate the fundamental technologies covered by the '961 patent to, for example, its alter egos, agents, intermediaries, related entities, distributors, dealers,

importers, customers, subsidiaries, 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 '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)”).

100. Furthermore, Defendant Somfy directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries and related entities, including Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC, including by selling and offering for sale the Accused Products directly to its related entities and importing the Accused Products into the United States for its related entities. On information and belief, U.S. based subsidiaries, including at least Somfy Systems and BFT, 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. Somfy SA is vicariously liable for the infringing conduct of Defendant Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC (under both the alter ego and agency theories). On information and belief, Defendants Somfy SA and Somfy Activites and U.S. based subsidiaries Somfy Systems, BFT, and Somfy LLC are essentially the same

company, comprising some members of the Somfy Group. Moreover, Somfy SA, as the parent company, along with its related entities, has the right and ability to control the infringing activities of those subsidiary entities such that Defendants receive a direct financial benefit from that infringement.

101. For example, Somfy infringes claim 1 of the '961 patent via the Accused Products that utilize ZigBee protocols, including, but not limited to ZigBee modules and digital motor interfaces and related accessories and software.

102. 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.

103. At a minimum, Somfy has known of the '961 patent at least as early as the filing date of this complaint. In addition, Somfy has known about infringement of Harris Corporation’s

(“Harris”) patent portfolio, which includes the ’961 patent, since at least its receipt of a letter from North Forty Consulting representing Harris dated April 20, 2018. The letter notifies Somfy of its infringing use of “wireless communication networks, network management/security, as well as innovations pertinent to the IEEE 802 and Zigbee standards,” in at least the “ZigBee to Digital Motor Interface; ZigBee Module for Curtain Motorization; Glyde; Temperature & Humidity Sensor; Opening Sensor; Motion Detector.”

104. On information and belief, since at least the above-mentioned date when Somfy was on notice of its infringement, Defendants have each actively induced, under U.S.C. § 271(b), importers, online stores, distribution partners, retailers, reseller partners, dealers, consumers, 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 notice provided on the above-mentioned date, Defendants each do so 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, consumers, 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, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing wireless networking features in the Accused Products, and/or providing technical support, replacement parts, or

services for these products to purchasers in the United States. *See, e.g., Service & Support*, SOMFY, <https://www.somfysystems.com/en-us/discover-somfy/contact-us/service-support> (providing consumers with “help with an existing project”); *see also somfysystems*, YOUTUBE.COM, <https://www.youtube.com/user/somfysystems> (providing consumers with Somfy-produced how-to videos related to Somfy products) (last visited May 27, 2021). Furthermore, Somfy markets myLink RTS smartphone and tablet interface and its application software as “a simple device that turns your smartphone or tablet into a sophisticated remote control for motorized products featuring Radio Technology Somfy® (RTS) [and] works with Alexa, IFTTT and Google Home allowing you to control your RTS solutions with your voice or with other connected products in your home.” *See myLink™ RTS Smartphone and Tablet Interface*, SOMFY, <https://store.somfysystems.com/mylink-rt-smartphone-and-tablet-interface.html> (scroll down and access “Description”) (last visited May 27, 2021). Such compatibility provides convenience and added functionality that induces consumers to use Somfy products, including ZigBee modules and digital motor interfaces utilizing ZigBee protocols in networks with other third-party devices, and thus further infringe the ’961 patent.

105. 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, Somfy has nevertheless continued its 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.

106. Plaintiff Stingray has been damaged as a result of Somfy'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 Somfy's infringements, which, by law, cannot be less than a reasonable royalty, together with interest and costs as fixed by this Court under 35 U.S.C. § 284.

CONCLUSION

107. 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.

108. 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

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

PRAYER FOR RELIEF

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

1. A judgment that Defendants have infringed the Asserted Patents as alleged herein, directly and/or indirectly by way of inducing infringement of such patents;
2. A judgment for an accounting of damages sustained by Plaintiff as a result of the acts of infringement by Defendants;

3. A judgment and order requiring Defendants to pay Plaintiff damages under 35 U.S.C. § 284, including up to treble damages as provided by 35 U.S.C. § 284, and any royalties determined to be appropriate;
4. A judgment and order requiring Defendants to pay Plaintiff pre-judgment and post-judgment interest on the damages awarded;
5. A judgment and order finding this to be an exceptional case and requiring Defendants to pay the costs of this action (including all disbursements) and attorneys' fees as provided by 35 U.S.C. § 285; and
6. Such other and further relief as the Court deems just and equitable.

Dated: June 1, 2021

Respectfully submitted,

/s/ Jeffrey R. Bragalone by permission
Wesley Hill

Jeffrey R. Bragalone (lead attorney)

Texas Bar No. 02855775

Terry A. Saad

Texas Bar No. 24066015

Marcus Benavides

Texas Bar No. 24035574

Hunter S. Palmer

Texas Bar No. 24080748

BRAGALONE OLEJKO SAAD PC

2200 Ross Avenue

Suite 4600W

Dallas, TX 75201

Tel: (214) 785-6670

Fax: (214) 785-6680

jbragalone@bosfirm.com

tsaad@bosfirm.com

mbenavides@bosfirm.com

hpalmer@bosfirm.com

Wesley Hill

Texas Bar No. 24032294

WARD, SMITH, & HILL, PLLC

P.O. Box 1231

Longview, TX 75606

Tel: (903) 757-6400

Fax: (903) 757-2323

wh@wsfirm.com

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