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

STINGRAY IP SOLUTIONS, LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**JURY TRIAL DEMANDED**
	§	
SAMSUNG ELECTRONICS CO., LTD.,	§	
and	§	**CIVIL ACTION NO. 2:21-cv-27**
SAMSUNG ELECTRONICS AMERICA,	§	
INC.,	§	
	§	
Defendants.	§	
	§	
	§	

PLAINTIFF'S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

Plaintiff Stingray IP Solutions, LLC ("Stingray") files this Complaint against Defendants Samsung Electronics Co., Ltd. ("SEC") and Samsung Electronics America, Inc. ("SEA") (collectively, "Samsung" or "Defendants") for infringement of U.S. Patent No. 7,082,117 (the "'117 patent"), U.S. Patent No. 7,224,678 (the "'678 patent"), U.S. Patent No. 7,440,572 (the "'572 patent"), and U.S. Patent No. 7,616,961 ("the "'961 patent").

THE PARTIES

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

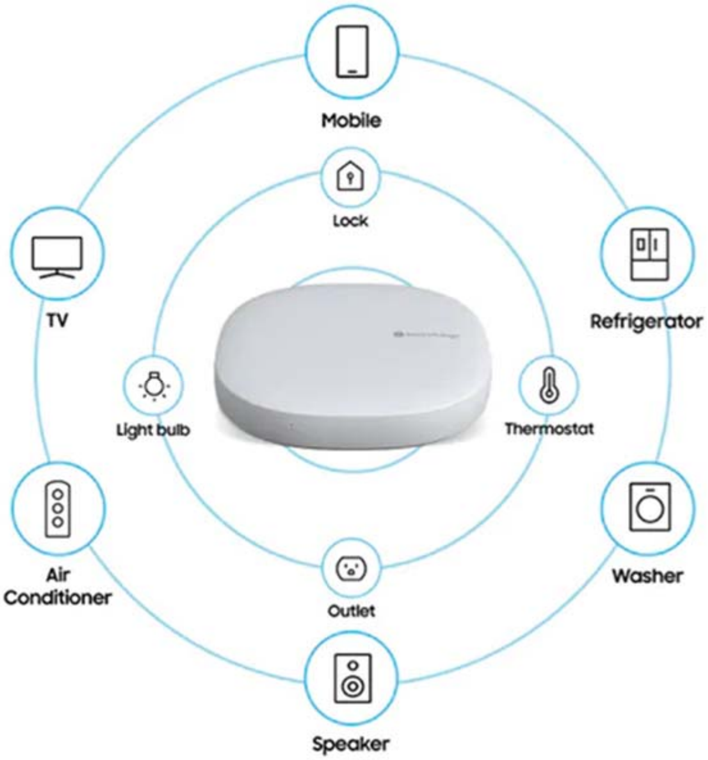
2. On information and belief, Defendant Samsung Electronics Co., Ltd. ("SEC") is a multi-national corporation organized under the laws of the Republic of Korea, with its principal place of business located at 129 Samsung-Ro, Yeongtong-Gu, Suwon, Gyeonggi-do, South Korea. SEC was established as "Samsung Electronics Industry Co., Ltd." in 1984. SEC changed its name to Samsung Electronics Co., Ltd. in 1984.

3. SEC is a "global electronics firm comprised of the headquarters in Korea and 240 subsidiaries." *See 2019 Business Report*, Samsung Electronics Co., Ltd., at p. 4/261, https://images.samsung.com/is/content/samsung/p5/global/ir/docs/2019_Business_Report.pdf. SEC's business consists of the following four divisions: CE (Consumer Electronics); IM (Information Technology & Mobile Communications); DS (Device Solutions); and Harman (Harman International Industries, Inc., and its subsidiaries). *Id*. The CE division produces "TVs, monitors, refrigerators, washing machines, air conditioners, etc." *Id*. The IM division produces "HHPs, network systems, computers, etc." The DS division produces "DRAM, NAND flash, mobile APs, OLED smartphone panels, LCD TV panels, etc." *Id*. And the Harman division produces "[h]ead units, infotainment systems, telematics, speakers, etc." *Id*.

4. Upon information and belief, SEC purchased the startup company SmartThings, Inc. ("STI") in 2014. At the time, STI was cited as "a poster child for a movement to bring intelligence to all manner of everyday devices." Clark, Don. *Samsung reaches Deal to Buy Startup SmartThings*, THE WALL STREET JOURNAL (14 August 2014) https://www.wsj.com/articles/samsung-reaches-deal-to-buy-startup-smartthings-1408062020. The purchase price for STI was estimated at $200 million. *Id*. SmartThings is "an open platform for smart home devices." *Samsung snaps up SmartThings, embracing Internet of Things*, CNET (14 August 2014) https://www.cnet.com/news/samsung-snaps-up-smartthings-embracing-internet-of-things/. The idea behind the acquisition of STI was to "pair Samsung's resources with SmartThings' platform so that the two can boost innovation in the Internet of Things." *Id*. SEC lists STI as a wholly-owned subsidiary and engages in the "sale of smart home electronics," operating in SEC's IM division. *See 2019 Business Report* at 78/261. STI is located at 665 Clyde Ave, Mountain View, CA 94043, United States, where it operates on behalf of SEC (and SEC's

subsidiaries), to provide "website(s), products, services, mobile applications, IoT plug-ins and other software," including the SmartThings application, which is a smartphone app used to integrate SmartThings devices. *See Welcome to SmartThings!*, SMARTTHINGS, https://www.smartthings.com/terms (terms of use page).

5. Regarding SEC's IM division, SEC touts that it "will lead growth of the smartphone market and deliver exceptional user experiences by… investing in future growth drivers such as Cloud, IoT, healthcare, AR, and VR." *See 2019 Business Report* at 5/261. To that end, SEC manufactures, imports, distributes, offers for sale, and sells Cloud and IoT wireless communication network devices in the U.S. generally referred to as "SmartThings" devices, which can "[t]urn your home into a smart home." *See SmartThings*, SAMSUNG, https://www.samsung.com/us/smart-home/. SEC's SmartThings are designed to "manage Wi-Fi signal usage [and] monitor and control automated devices." *Id*. One device, the "SmartThings Hub," is "[t]he brain of your smart home" which can "[c]onnect with a wide range of smart devices and make them work together." Some of these smart devices, i.e., IoT and smart home devices, including Smart TVs, smartphones, home appliances, audio devices, sensors, electrical outlets, and home security devices, operating in a SmartThings network are illustrated below in relation to the SmartThings Hub:



Id.

6. Moreover, "SmartThings works with 100s of compatible devices," manufactured by third parties, "including lights, cameras, voice assistants, locks, thermostats, and more." *Id.* To connect, communicate, and control IoT and smart home devices, the SmartThings network utilizes communication protocols including those based off of the IEEE 802.15.4 standard, such as the ZigBee®, Z-Wave, or WiFi protocols. *See, e.g., SmartThings Hub*, SAMSUNG, https://www.samsung.com/us/smart-home/smartthings/hubs/samsung-smartthings-hub--2018--gp-u999sjvlgda/#benefits (listing as "Communication Features" the protocols ZigBee, WiFi, and Z-Wave). Consumers may integrate, use, and control SmartThings devices via the SmartThings app, which is available for download at least on iOS and Android operating systems.

7. In SEC's CE division, the "TV is the core product." *See 2019 Business Report* at 4/261. SEC states that it has "maintained its position as the market leader for 14 consecutive years

by leveraging competitive advantages in hardware such as LCD/LED TVs as well as software driven product features within our Smart TV product portfolio." *Id*. In 2018, SEC "aimed to elevate the viewer experience to another level by…improving connectivity via AI or IoT technologies." *Id*. at 28/261. To that end, Samsung Smart TVs "along with SmartThings, [are] designed to connect to a wide range of connected devices across [the user's] home." *See Smart TV Highlights*, SAMSUNG, https://www.samsung.com/us/televisions-home-theater/tvs/smart-tv/highlights/. Samsung adds that "[t]his ecosystem of products work together, wirelessly, to automate your home and make life a little bit easier." *Id*. Such convenience includes "start[ing] the wash," "turning on [the user's] vacuum" and other features from "activating porch lights to monitoring the thermostat" allowing "alerts stream right to your Smart TV, so [the user] can have a complete view of [the user's] house at a moment's notice." *See Smart Home*, SAMSUNG, https://www.samsung.com/us/televisions-home-theater/tvs/smart-tv/smart-home-with-iot-devices/. As part of its Smart Home ecosystem, in addition to SmartThings devices and Smart TVs, SEC also provides to U.S. consumers other connected home appliances, including smart doorbells, smart lights and lightbulbs, soundbars, refrigerators, cameras, and smart washers. Smartphones produced by SEC also include smart features which enable the phone to access, connect to, and control other network devices, including controlling devices via the SmartThings app. *See, e.g.*, *Galaxy S20 5G and Smart Washer Bundle*, SAMSUNG, ("Syncing is simple with the SmartThings app, which enables your Samsung phone and smart washer to work together, giving you more control of your laundry."). Upon information and belief, SEC, STI, and other SEC subsidiaries develop, design, manufacture, import, distribute, advertise, offer for sale, sell, and use SEC's IoT and smart home devices and related services in the U.S. market, including in Texas and this judicial district.

8. On information and belief, SEC maintains a corporate presence in the United States, including in this judicial district, via at least its wholly-owned U.S.-based subsidiary and Defendant in this action Samsung Electronics America, Inc. ("SEA"). SEA is a corporation organized under the laws of the State of New York. SEC classifies SEA as a "major subsidiary." *See 2019 Business Report* at 7/261. SEA was established in 1978 and its "[m]ajor business" is listed as "[e]lectronics goods sales." *Id*. In 2018, SEA opened its "Flagship North Texas Campus" in this judicial district at 6625 Excellence Way, Plano, Texas 75023, and occupancy began in 2019. *See Samsung Electronics America to Open Flagship North Texas Campus*, SAMSUNG NEWSROOM U.S. (April 6, 2018), https://news.samsung.com/us/samsung-electronics-america-open-flagship-north-texas-campus/. This location consolidated "more than 1,000 regional employees" from prior locations in Richardson and Plano, Texas. Now, this location is "home to Samsung Electronics America's second biggest employee population in the U.S. across multiple divisions." On information and belief, SEA oversees domestic sales and distribution of Samsung's IoT and smart home devices accused of infringement in this case. *Id*. Thus, SEA does business in the U.S., the state of Texas, and in the Eastern District of Texas, and may be served with process through its agent, CT Corporation System, 1999 Bryan Street, Suite 900, Dallas, Texas 75201.

9. In 2017, SEA acquired full ownership of Harman International Industries, Inc. ("Harman"). *See 2019 Business Report*, at 19/261. Harman, along with its subsidiaries operating in the division, focus on connected technologies for automotive, consumer and enterprise markets. In 2018, Harman entered an "engineering partnership with Samsung SmartThings, the industry leader for consumer IoT technology and the easiest way for people to turn a traditional home into a smart home with sensors, smart devices and a native mobile application." *See HARMAN Announces Strategic Association with Samsung SmartThings*, HARMAN: A SAMSUNG COMPANY,

https://news.harman.com/releases/releases-20180313. The Harman division of SEC's business "designs and develops connected products and solutions for automakers, consumers, and companies worldwide and is a global leader in the market for connected car systems, audio and visual products, professional solutions, and connected services." *See 2019 Business Report*, at 5/261. Such products include "connected car systems, audio and visual products, enterprise automation solutions; and services supporting the Internet of Things," including Harman Amplify products. *See HARMAN Announces Strategic Association with Samsung SmartThings*, HARMAN: A SAMSUNG COMPANY, https://news.harman.com/releases/releases-20180313. For example, SEC provides the Harman Amplify product and service which "offer[s] a unique convergence of LTE Small Cell, Digital Voice Assistant, and IoT" that "provides integrated personal voice assistant and control of Smart Home Devices using Amazon Alexa eco-system." *See Harman Amplify*, HARMAN: A SAMSUNG COMPANY, https://services.harman.com/products-and-solutions/internet-of-things/harman-amplify#:~:text=HARMAN%20Amplify%20offer%20a%20unique,using%20Amazon%20Alexa%20eco%2Dsystem.

10. Through offers to sell, sales, imports, distributions, and other related agreements to transfer ownership of SEC's IoT and smart home devices and services with distributors and customers operating in and maintaining a significant business presence in the U.S. and/or its U.S. subsidiaries, including via Defendant SEA and its U.S.-based subsidiary STI, SEC does business in the U.S., the state of Texas, and in the Eastern District of Texas. SEC may be served with process via its agents in the U.S., including via Defendant SEA and STI, and/or at its principal place of business at 129 Samsung-Ro, Yeongtong-Gu, Suwon, Gyeonggi-do, South Korea.

JURISDICTION AND VENUE

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

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

13. On information and belief, SEC 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 judicial 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 judicial district and, thus, submits itself to the jurisdiction of this court; and; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this judicial 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 judicial district vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, SEC owns and/or controls multiple subsidiaries and affiliates that have a significant business presence in the U.S. and in Texas. *See Samsung in America*, SAMSUNG NEWSROOM U.S., https://news.samsung.com/us/in-america/ (scroll down to map titled "Samsung's Footprint in the United States"). Such a presence furthers the development, design, manufacture, importation, distribution, and sale of SEC's infringing electronic devices in Texas, including in this judicial district. For example, SEC's wholly-owned, U.S.-based subsidiary SEA has its "Flagship North Texas Campus" in Plano, Texas which employs more than one thousand employees working "across multiple divisions." Furthermore, SEC's subsidiary Samsung Austin Semiconductor has a

production facility in Austin, Texas that employs "thousands." *See History*, SAMSUNG AUSTIN SEMICONDUCTOR, https://www.samsung.com/us/sas/company/history (last visited Jan. 5, 2021). In its Austin location, SEC manufactures computer chips that "power Samsung's mobile phones, tablets and other electronic devices." *Id*. Through direction and control of its subsidiary, SEC has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over SEC would not offend traditional notions of fair play and substantial justice.

14. Upon information and belief, SEC controls or otherwise directs and authorizes all activities of its subsidiaries, including, but not limited to Defendant SEA and Samsung Austin Semiconductor, which, significantly, both have substantial business operations in Texas. Directly and via at least these subsidiaries and via intermediaries, such as distributors and customers, SEC has placed and continues to place infringing IoT and smart home devices, including SEC's Smart TVs, Harman connected devices, home appliances, and SmartThings devices, among others, into the U.S. stream of commerce. SEC 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 judicial 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. SEC utilizes established distribution channels to distribute, market, offer for sale, sell, service, and warrant infringing products directly to consumers, including offering such products for sale via its own website. *See, e.g., Samsung SmartThings Wifi 1-pack*, SAMSUNG, https://www.samsung.com/us/smart-home/smartthings-wifi/single/samsung-smartthings-wifi-1-pack-et-wv525bwegus/. Moreover, SEC utilizes its subsidiaries and intermediaries, such as Defendant SEA and Samsung Austin Semiconductor, to design, develop, import, distribute, and service infringing IoT and smart home devices, such as SEC's Smart TVs, Harman connected devices, home appliances, and SmartThings devices, among others. Such SEC products and services have been sold in retail stores, both brick and mortar and online, within this judicial district and in Texas. *See., e.g., Buy Direct from Samsung*, SAMSUNG, https://www.samsung.com/us/smart-home/smartthings/hubs/samsung-smartthings-hub--2018--gp-u999sjvlgda-buy/ (providing a link to a purchase a SmartThings Hub at BestBuy location at 3333 Preston Rd Frisco, TX 75034, i.e., in this judicial district).

16. Upon information and belief, SEC purposefully places infringing IoT and smart home devices and services in established distribution channels in the stream of commerce by contracting with national retailers who sell SEC's products in the U.S., including in Texas and this judicial district. SEC contracts with these companies with the knowledge and expectation that SEC's IoT and smart home devices and services will be imported, distributed, advertised, offered for sale, and sold in the U.S. market. For example, at least BestBuy, Amazon.com, Dell.com offer for sale and sell SEC SmartThings devices, Smart TVs, smartphones, and home appliances, in and specifically for the U.S. market, via their own websites or retail stores located in and selling their products to consumers in Texas and this judicial district. *See, e.g., Samsung SmartThings Wifi ET-WV525 - central controller*, DELL, https://www.dell.com/en-us/shop/samsung-smartthings-wifi-

et-wv525-central-controller/apd/aa288487/networking (offering SEC's SmartThings product for sale and indicating "Product not supported outside U.S."). SEC also provides its application software, the "SmartThings App," for download and use in conjunction with and as a part of the wireless communication network that connects SmartThings devices, home appliances, smart TVs, and other network devices. The SmartThings App is available via digital distribution platforms by Apple Inc. and Google for download by users and execution on Samsung smartphones, among other brands. *See, e.g., SmartThings*, GOOGLE PLAY, https://play.google.com/store/apps/details?id=com.samsung.android.oneconnect (offering the application for download and indicating that the application is offered by "Samsung Electronics Co., Ltd.").

17. Based on SEC's connections and relationship with its U.S.-based national retailers and digital distribution platforms, SEC knows that Texas is a termination point of the established distribution channel, namely online and brick and mortar stores offering SEC SmartThings products and software to consumers in Texas. SEC, 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").

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

19. Venue is proper in this judicial district pursuant to 28 U.S.C. § 1391. Defendant SEC is a foreign entity and may be sued in any judicial district under 28 U.S.C. § 1391(c).

20. On information and belief, SEA 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 judicial 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 judicial district and, thus, submits itself to the jurisdiction of this court; and; and (B) regularly doing or soliciting business, engaging in other persistent conduct targeting residents of Texas and this judicial 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 judicial district vicariously through and/or in concert with its alter egos, intermediaries, agents, distributors, importers, customers, subsidiaries, and/or consumers. For example, SEA has its "Flagship North Texas Campus" in Plano, Texas which employs more than one thousand employees working "across multiple divisions." SEA is also registered to do business in Texas. SEA, therefore, has committed acts of direct and/or indirect patent infringement within Texas, and elsewhere in the United States, giving rise to this action and/or has established minimum contacts with Texas such that personal jurisdiction over SEA would not offend traditional notions of fair play and substantial justice.

21. Venue is proper in this judicial district pursuant to 28 U.S.C. §§ 1391(c) and 1400(b). Defendant SEA has committed acts of infringement in this district and has a regular and established place of business in this district at least at 6625 Excellence Way, Plano, Texas 75023. Accordingly, SEA may be sued in this district under 28 U.S.C. § 1400(b).

22. On information and belief, SEC and SEA each have significant ties to, and presence in, the State of Texas and the Eastern District of Texas, making venue in this judicial district both proper and convenient for this action.

THE ASSERTED PATENTS AND TECHNOLOGY

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

24. 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.

25. 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.

26. 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.

27. 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.

28. Upon information and belief, a significant portion of the operating revenue of Defendants is derived from the manufacture, distribute, sale, and use of IoT and smart home devices, which are imported into the United States, distributed, and ultimately sold to and used by U.S. consumers. For example, Defendant SEC utilizes its U.S.-based subsidiaries, including Defendant SEA and wholly-owned subsidiary STI, distributors, customers, partners, and retailers to provide the IoT and smart home devices to consumers. SEC’s worldwide net revenue for the IM division in 2019, from which some of Defendants’ IoT and smart home devices are developed and sold, was reported at 1,072,662 (KRW 100mil or 107.2662 trillion), which is 46.6% of SEC’s total revenue. *See 2019 Business Report* at 41/261. SEA, which operates in the U.S., reported 33,859,423 (in millions of Korean won) in sales. *See 2019 Business Report* at 86/261. SEC states

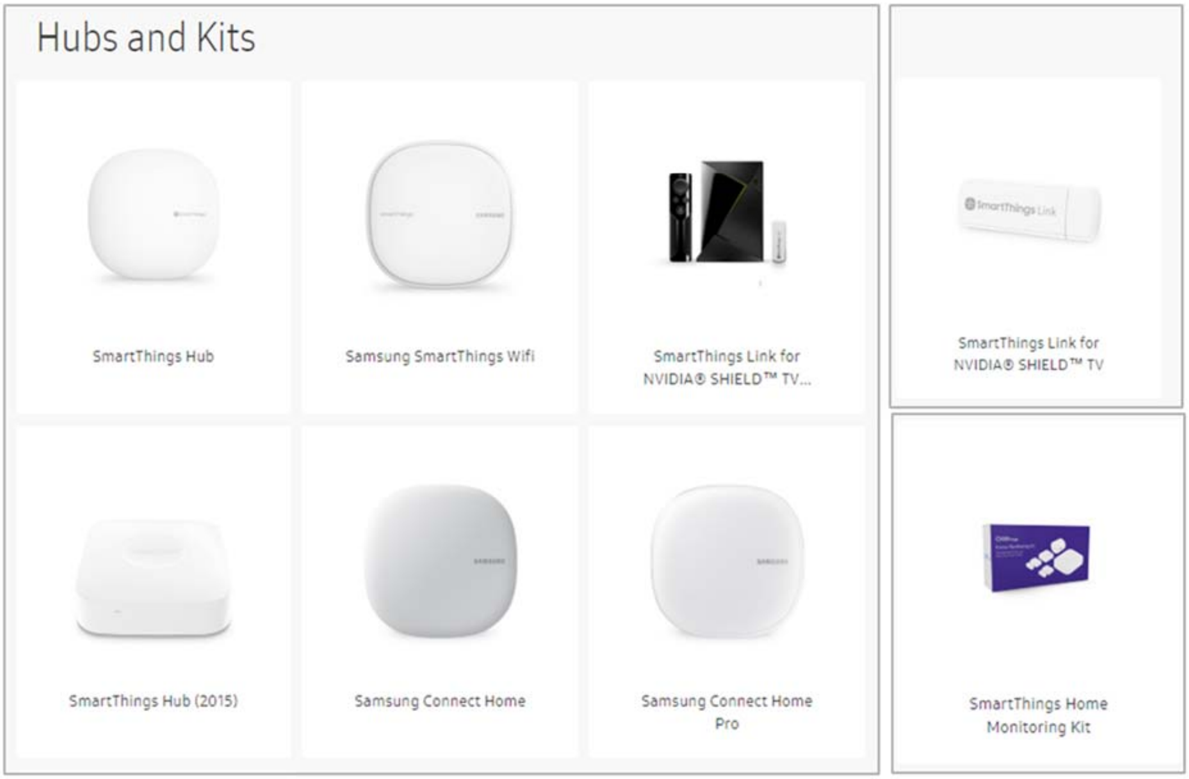
that its sales strategy includes "[e]xpand[ing] market leadership based on premium products such as smart devices." *See 2019 Business Report* at 43/261.

29. The Asserted Patents cover Defendants' IoT and smart home devices, components, software, services, and processes related to same that generally connect to other devices in a network or other networks (including in IoT and cloud networks) using a wireless protocol, such as ZigBee, WiFi, or Z-Wave, including, but not limited to, Defendants' SmartThings Hub, SmartThings WiFi, SmartThings Link for NVIDIA SHIELD^{TM}, Samsung Connect Home, Samsung Connect Home Pro, SmartThings Home Monitoring Kit, SmartThings Water Leak Sensor, SmartThings Arrival Sensor, SmartThings Motion Sensor, SmartThings Multipurpose Sensor, SmartThings Smart Bulb, SmartThings Outlet, SmartThings Button, Harman Amplify, and Harman AMX Devices, Smart TVs, smartphones, home appliances, audio devices, Harman connected devices (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.

30. Examples of Defendant's Accused Products are at least the family of Defendants' SmartThings devices. Examples of the SmartThings hub are shown below:

smartthings.com/products/-/filter/brands/samsung,smartthings

SmartThings



Hubs and Kits

SmartThings Hub

Samsung SmartThings Wifi

SmartThings Link for NVIDIA® SHIELD™ TV...

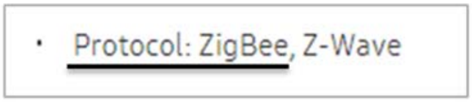
SmartThings Link for NVIDIA® SHIELD™ TV

SmartThings Hub (2015)

Samsung Connect Home

Samsung Connect Home Pro

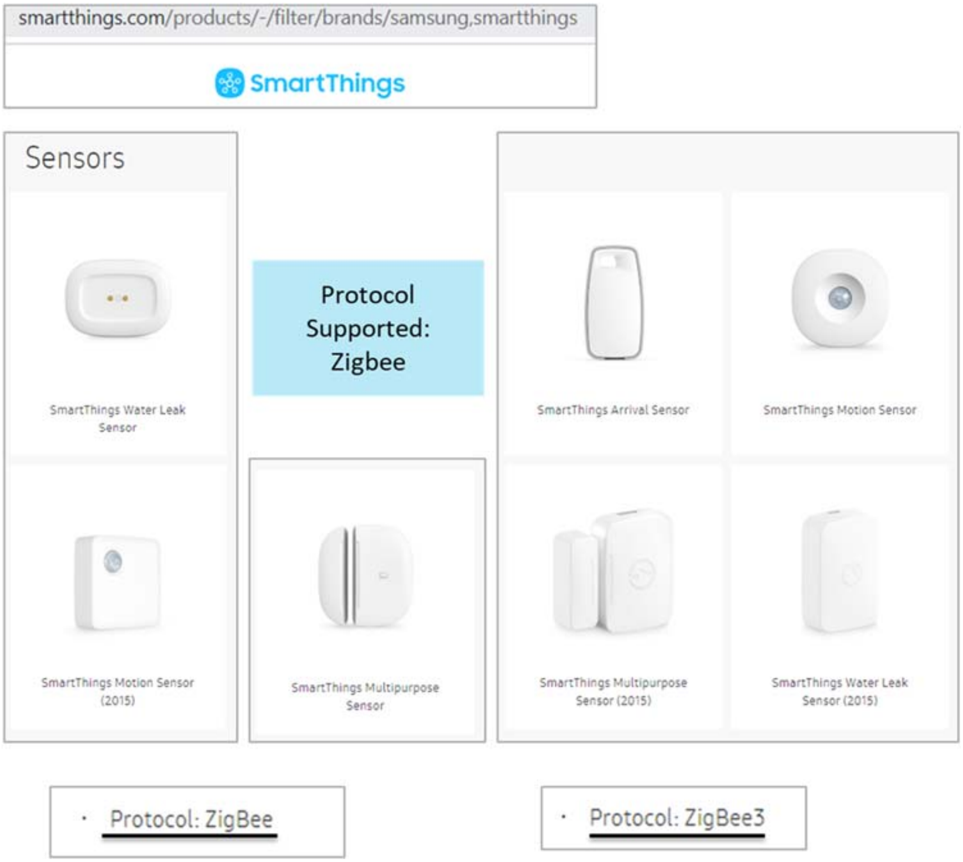
SmartThings Home Monitoring Kit



- Protocol: ZigBee, Z-Wave

Source: https://www.smartthings.com/products/-/filter/brands/samsung,smartthings

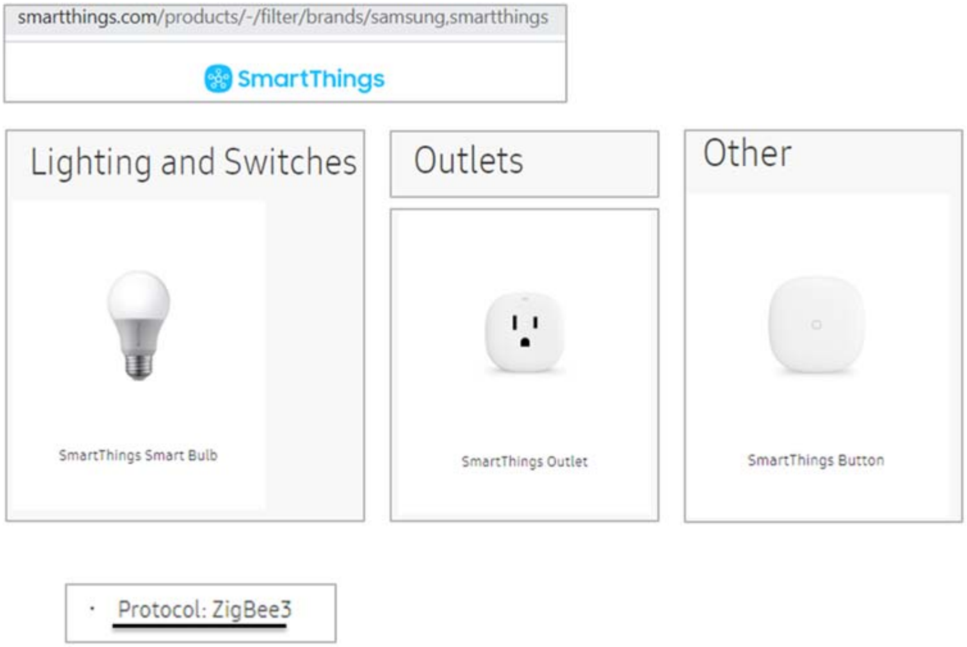
31. The Asserted Patents cover Samsung SmartThings products that use ZigBee protocol to communicate with other devices on the network. ZigBee protocol is based on the IEEE 802.15.4 standard. Such devices include water leak sensors, motion sensors, multi-purpose sensors, and arrival sensors:


smartthings.com/products/-/filter/brands/samsung,smartthings
SmartThings
Sensors
SmartThings Water Leak Sensor
Protocol Supported: Zigbee
SmartThings Arrival Sensor
SmartThings Motion Sensor
SmartThings Motion Sensor (2015)
SmartThings Multipurpose Sensor
SmartThings Multipurpose Sensor (2015)
SmartThings Water Leak Sensor (2015)

- Protocol: ZigBee

- Protocol: ZigBee3

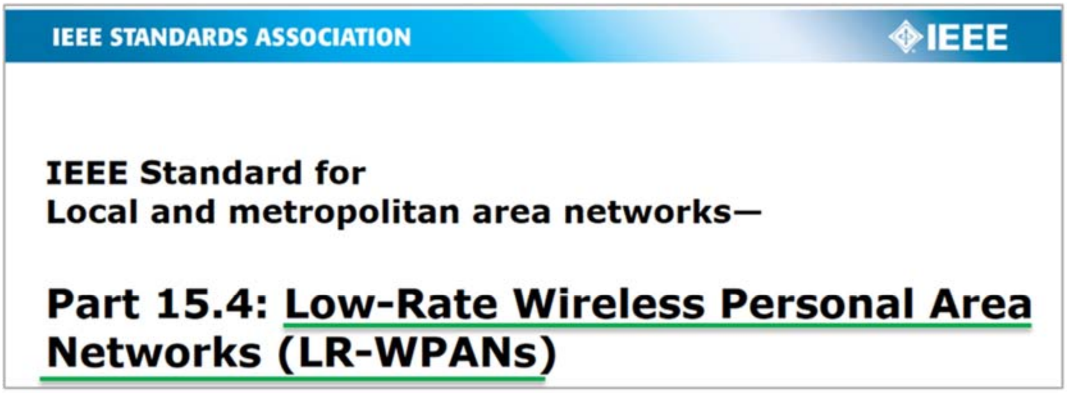
32. Other examples of SmartThings devices, as shown below.



- Protocol: ZigBee3

Source: https://www.smartthings.com/products/-/filter/brands/samsung,smartthings

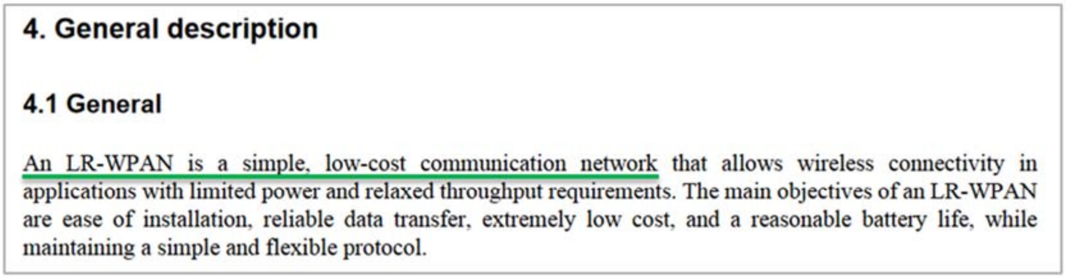
33. The IEEE 802.15.4 standard based mobile ad-hoc network, utilized by the Accused Products, is a type of Low-Rate Wireless Personal Area Network (LR-WPAN) that allows transmission of data between plurality of network nodes.



IEEE STANDARDS ASSOCIATION IEEE

IEEE Standard for
Local and metropolitan area networks—

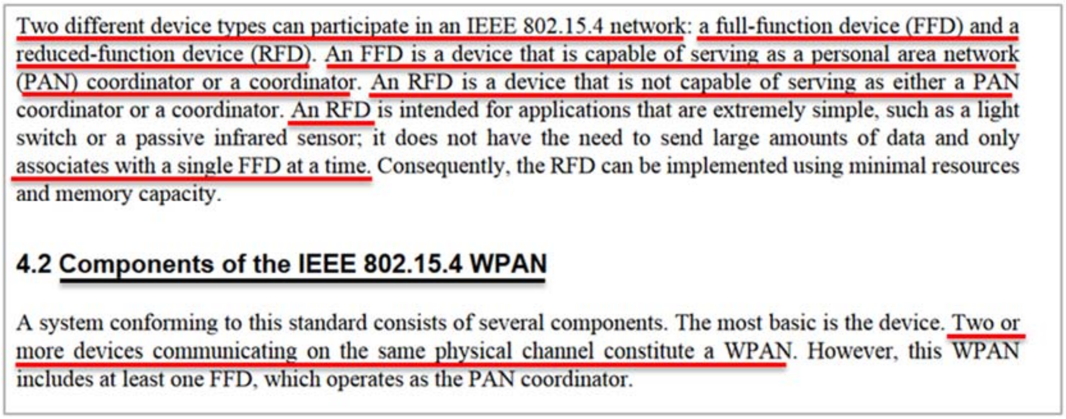
Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)



4. General description

4.1 General

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



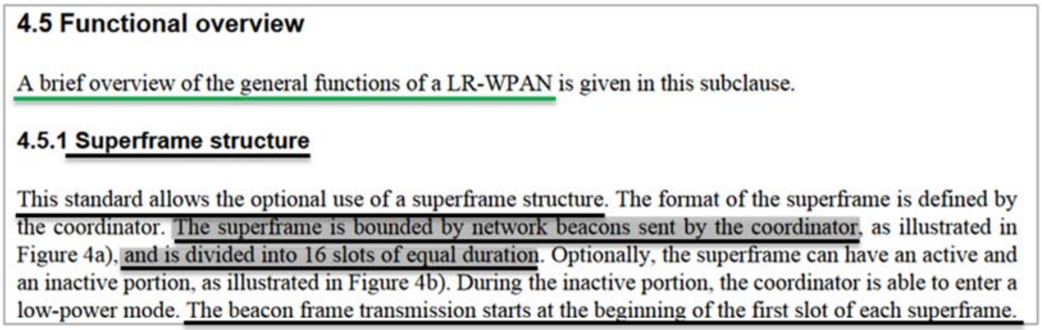
Two different device types can participate in an IEEE 802.15.4 network: a full-function device (FFD) and a reduced-function device (RFD). An FFD is a device that is capable of serving as a personal area network (PAN) coordinator or a coordinator. An RFD is a device that is not capable of serving as either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

4.2 Components of the IEEE 802.15.4 WPAN

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

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

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

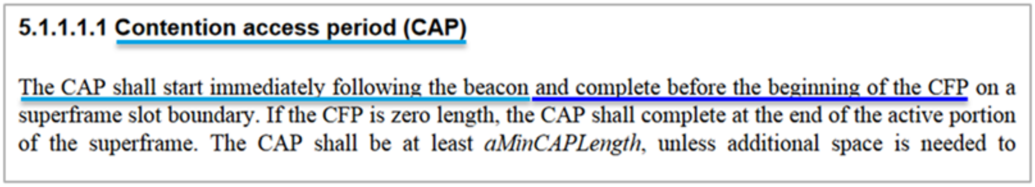


4.5 Functional overview

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

4.5.1 Superframe structure

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



5.1.1.1.1 Contention access period (CAP)

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

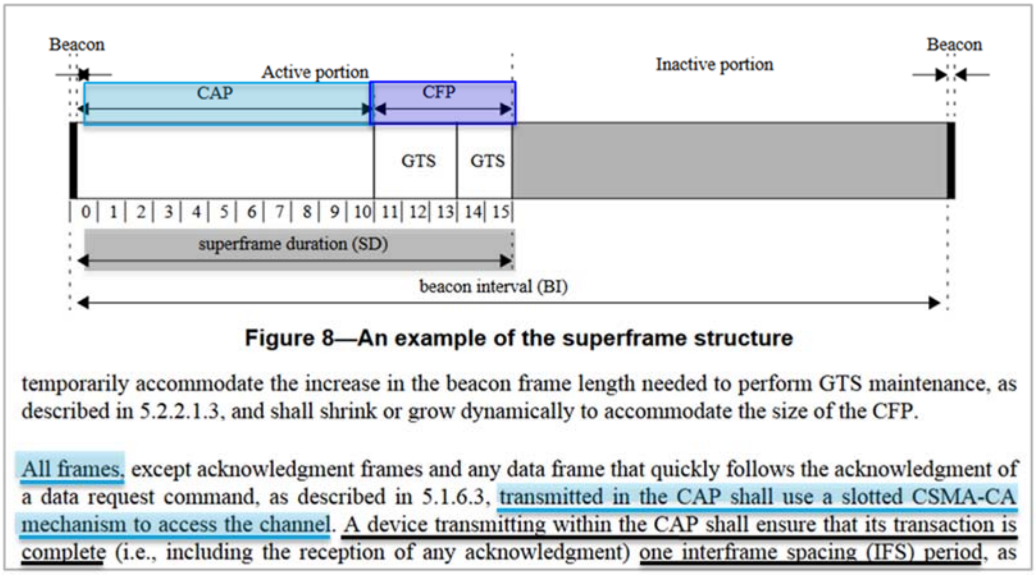
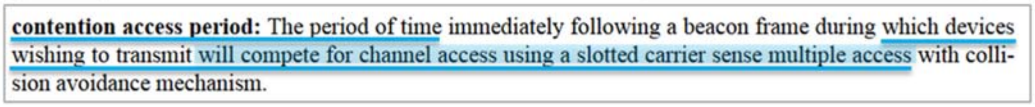


Figure 8—An example of the superframe structure

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

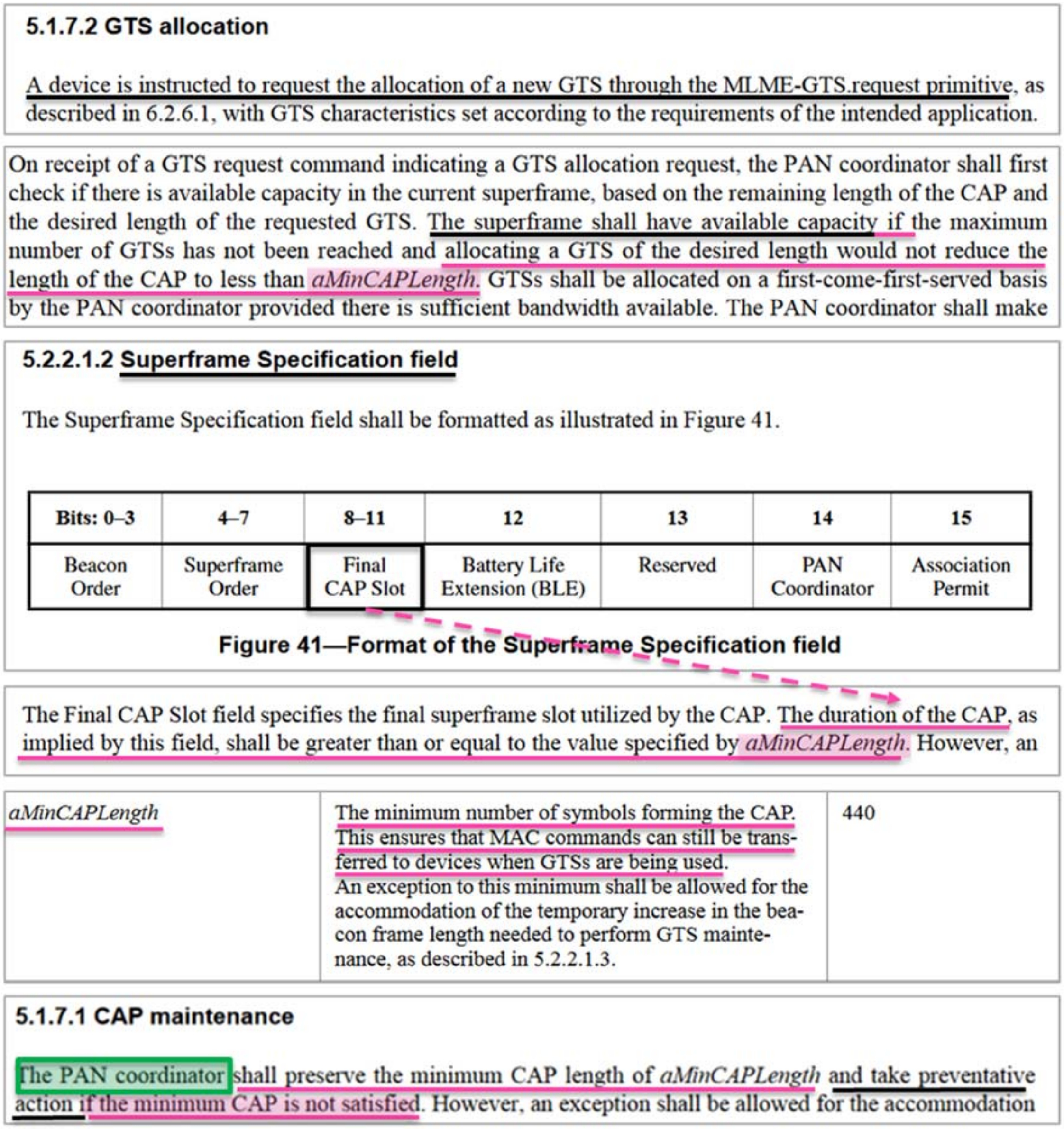
All frames, except acknowledgment frames and any data frame that quickly follows the acknowledgment of a data request command, as described in 5.1.6.3, transmitted in the CAP shall use a slotted CSMA-CA mechanism to access the channel. A device transmitting within the CAP shall ensure that its transaction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



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

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

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



5.1.7.2 GTS allocation

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

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

5.2.2.1.2 Superframe Specification field

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

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

Figure 41—Format of the Superframe Specification field

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

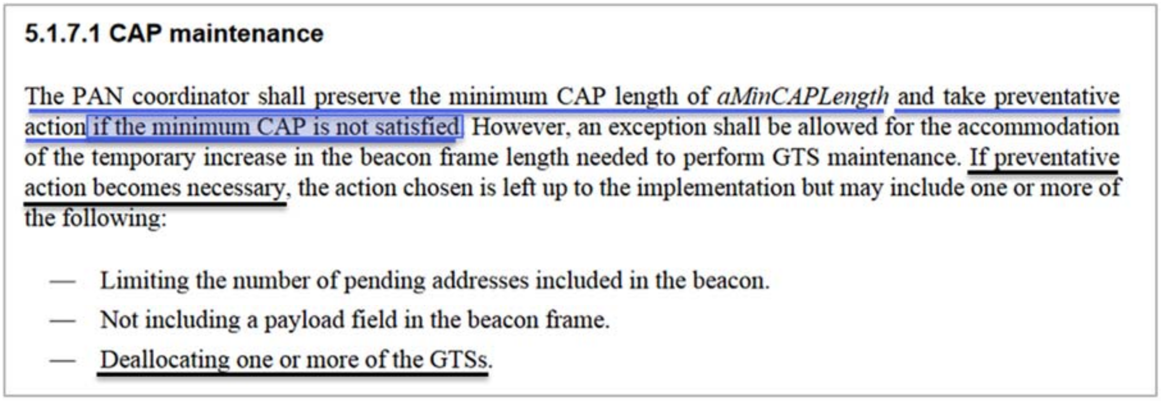
aMinCAPLength	The minimum number of symbols forming the CAP. This ensures that MAC commands can still be transferred to devices when GTSs are being used. An exception to this minimum shall be allowed for the accommodation of the temporary increase in the beacon frame length needed to perform GTS maintenance,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

5.1.7.1 CAP maintenance

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

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

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



5.1.7.1 CAP maintenance

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

— Limiting the number of pending addresses included in the beacon.

— Not including a payload field in the beacon frame.

— Deallocating one or more of the GTSs.

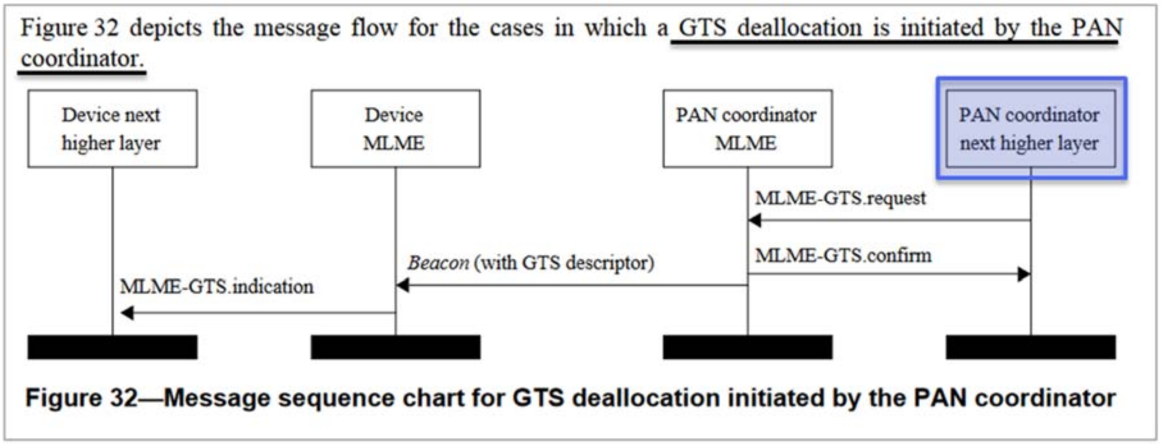


Figure 32 depicts the message flow for the cases in which a GTS deallocation is initiated by the PAN coordinator.

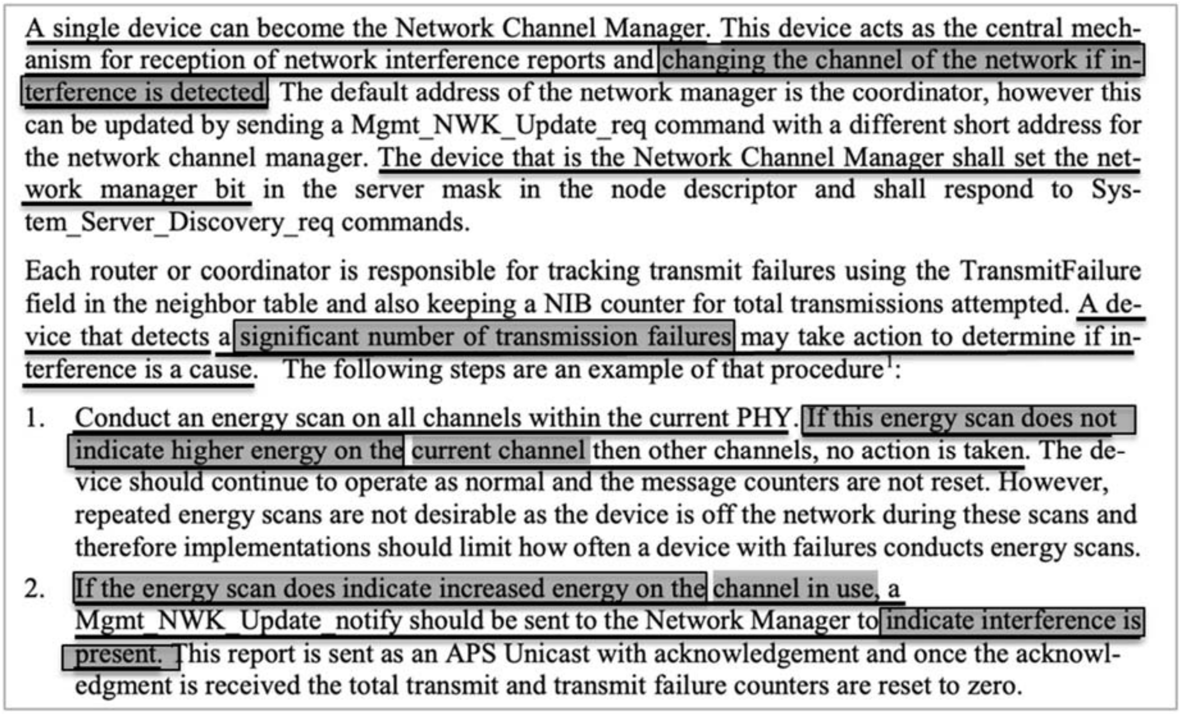
Figure 32—Message sequence chart for GTS deallocation initiated by the PAN coordinator

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

37. The Accused Products, including the SmartThings devices shown as examples below, also practice a method for dynamic channel allocation in a mobile ad hoc network. As indicated below, "[a] single device can become the Network Channel Manager."

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

ZigBee Control your world



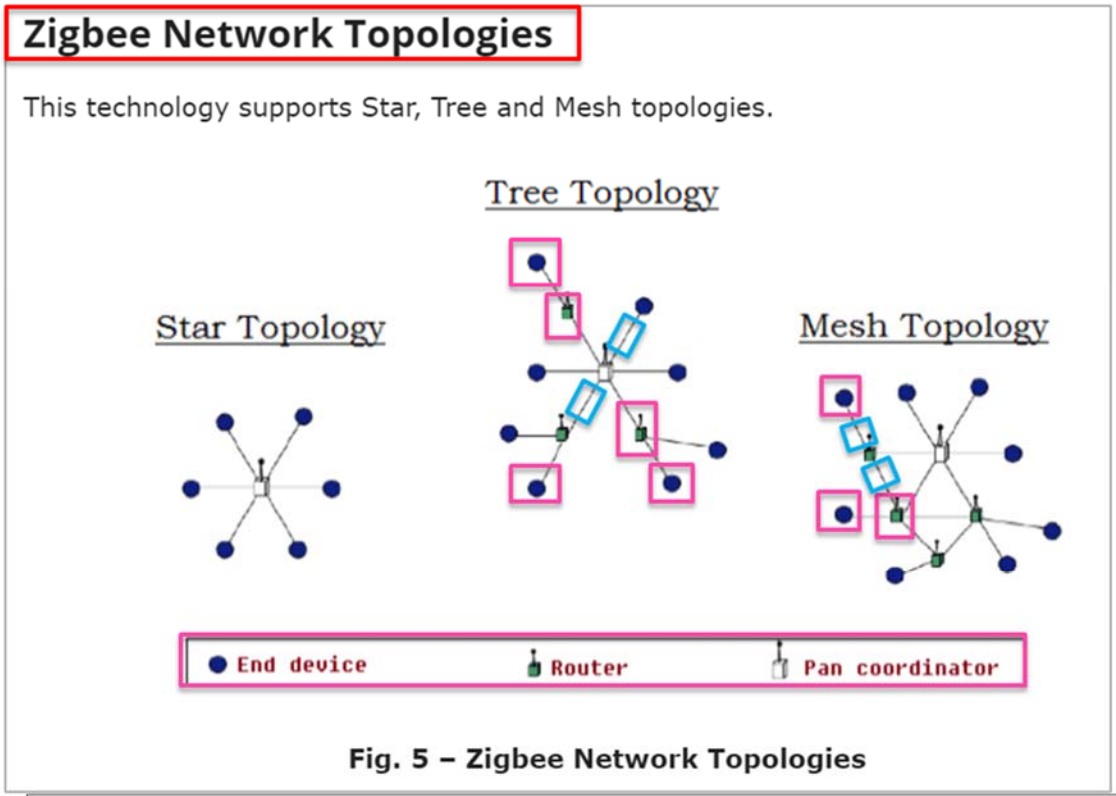
A single device can become the Network Channel Manager. This device acts as the central mechanism for reception of network interference reports and changing the channel of the network if interference is detected. The default address of the network manager is the coordinator, however this can be updated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

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

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

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

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



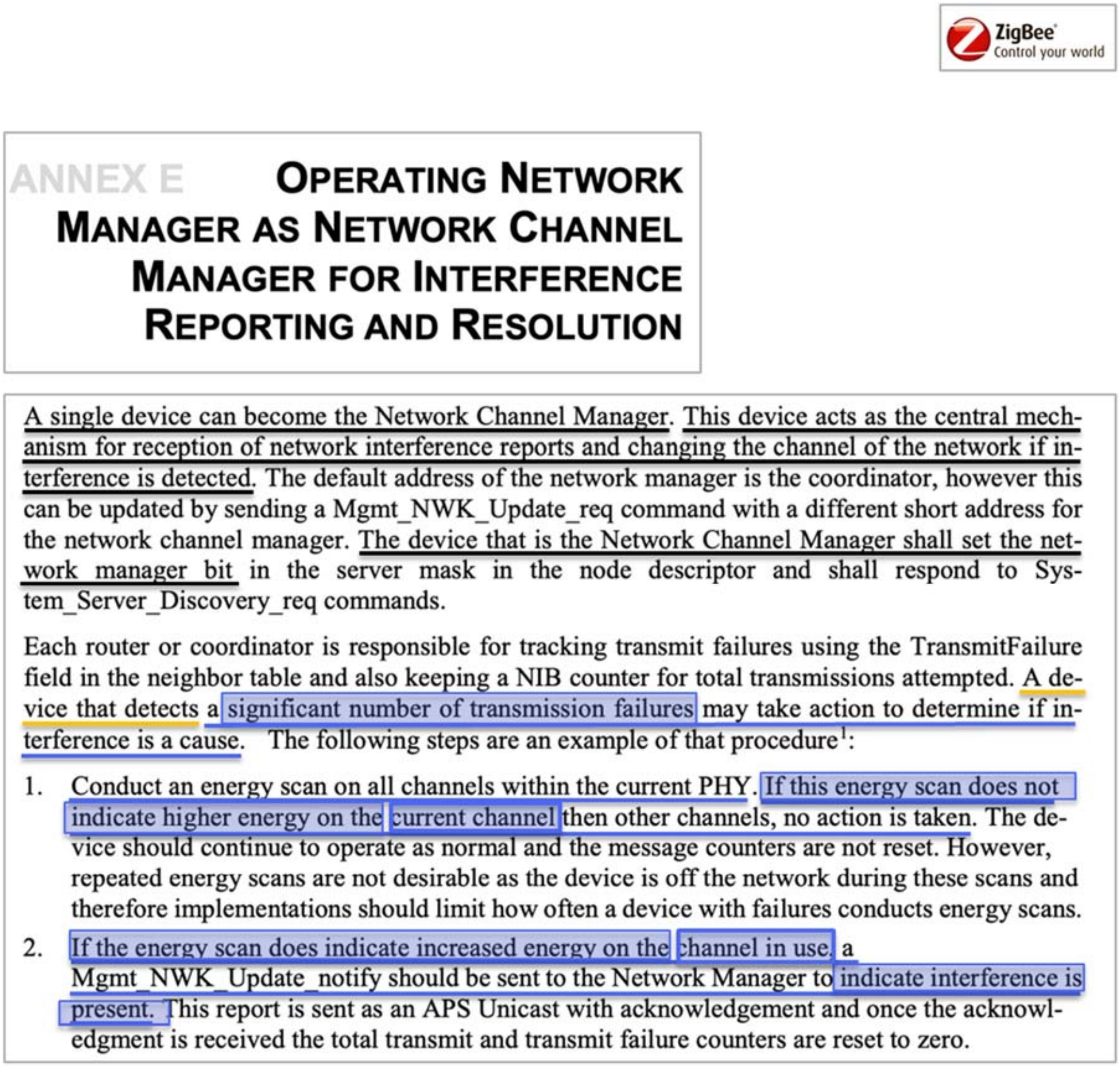
Zigbee Network Topologies

This technology supports Star, Tree and Mesh topologies.

Fig. 5 – Zigbee Network Topologies

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

39. In the ZigBee network of the Accused Products, a network device/node is configured to monitor the performance of a channel-in-use based on its energy measurement. As described below, if the measurement value is higher than the value on other channels (threshold), it indicates interference is present on the channel, consequently resulting in transmission failures.


ZigBee
Control your world

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

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

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

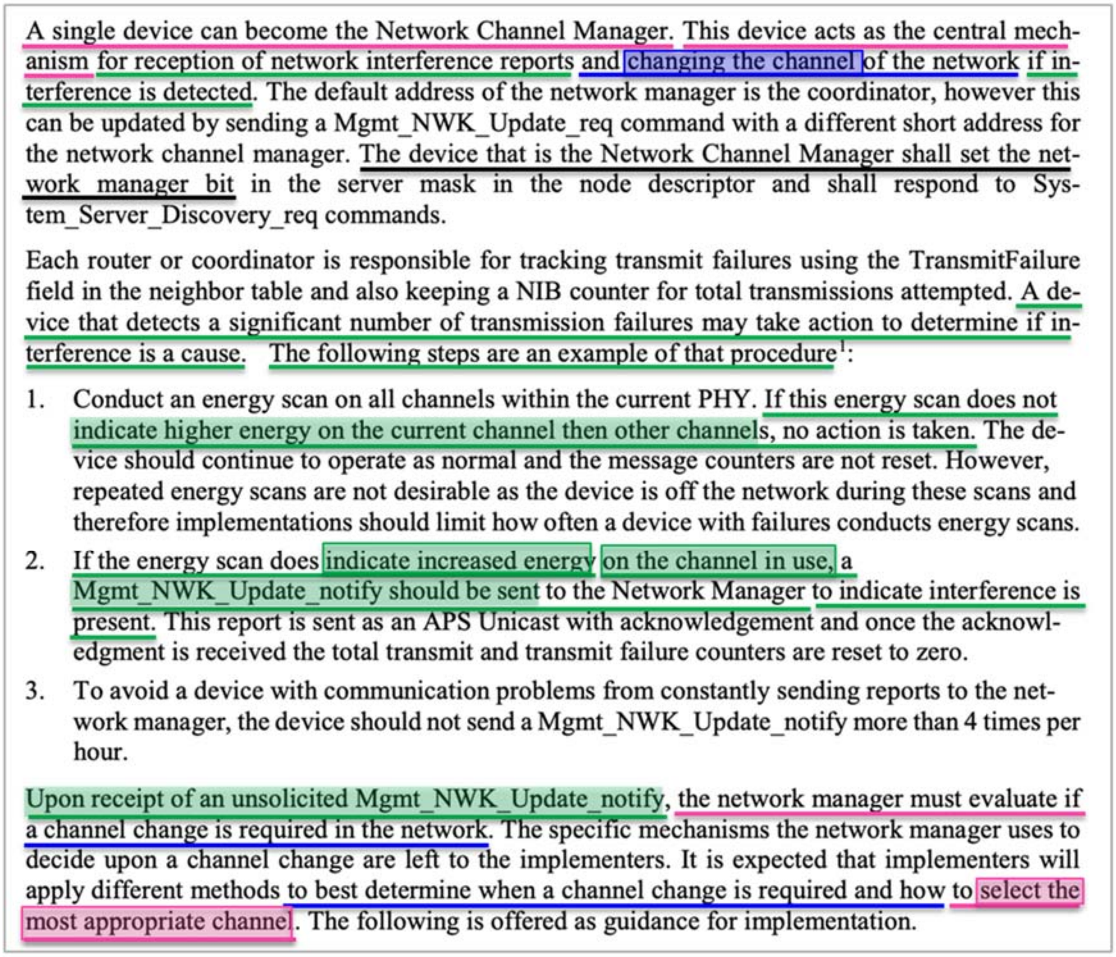
1. Conduct an energy scan on all channels within the current PHY. If this energy scan does not indicate higher energy on the current channel then other channels, no action is taken. The device should continue to operate as normal and the message counters are not reset. However, repeated energy scans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

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

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

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

ZigBee
Control your world



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

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

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

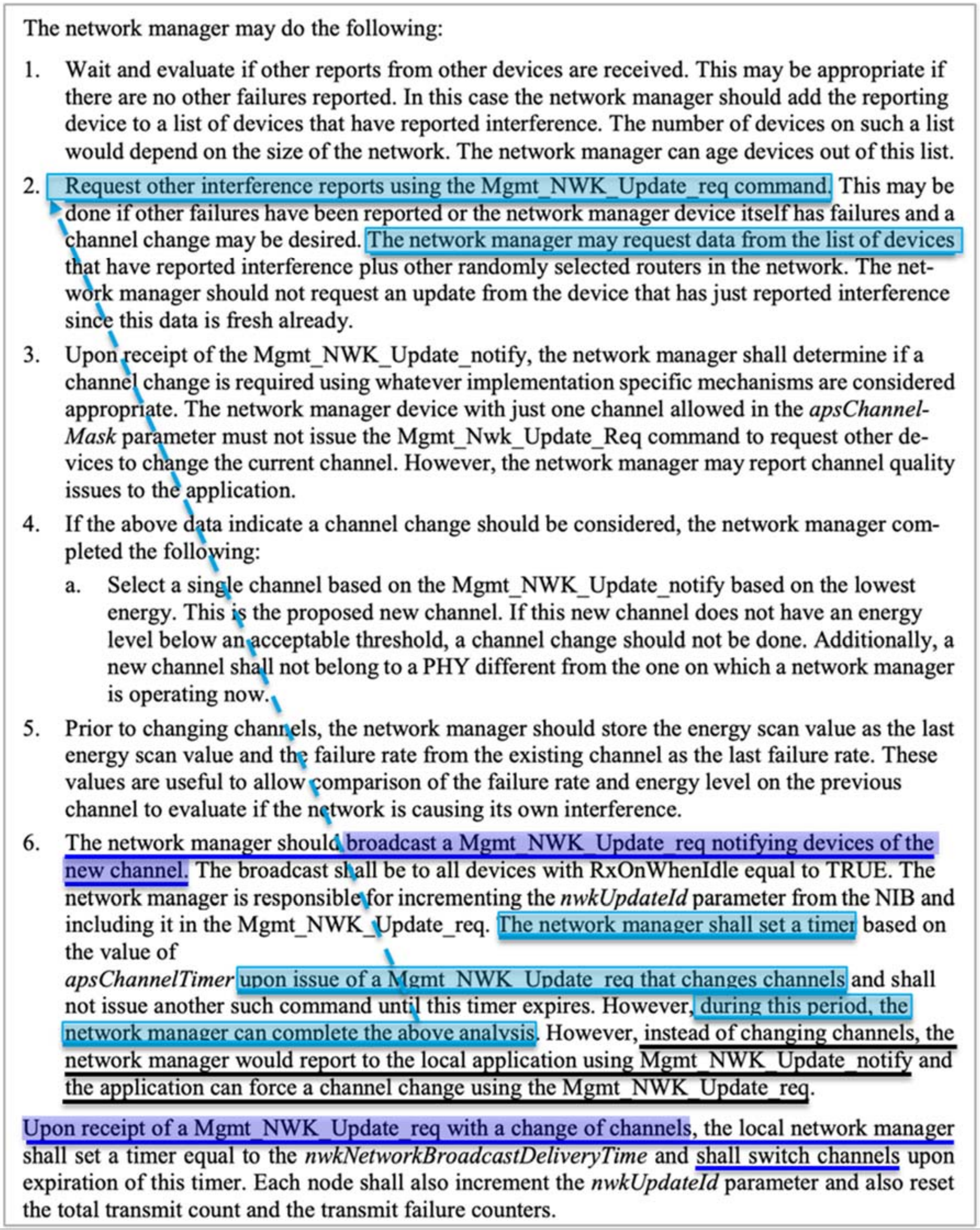
Upon receipt of an unsolicited Mgmt_NWK_Update_notify, the network manager must evaluate if a channel change is required in the network. The specific mechanisms the network manager uses to decide upon a channel change are left to the implementers. It is expected that implementers will apply different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

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

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

41. 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.



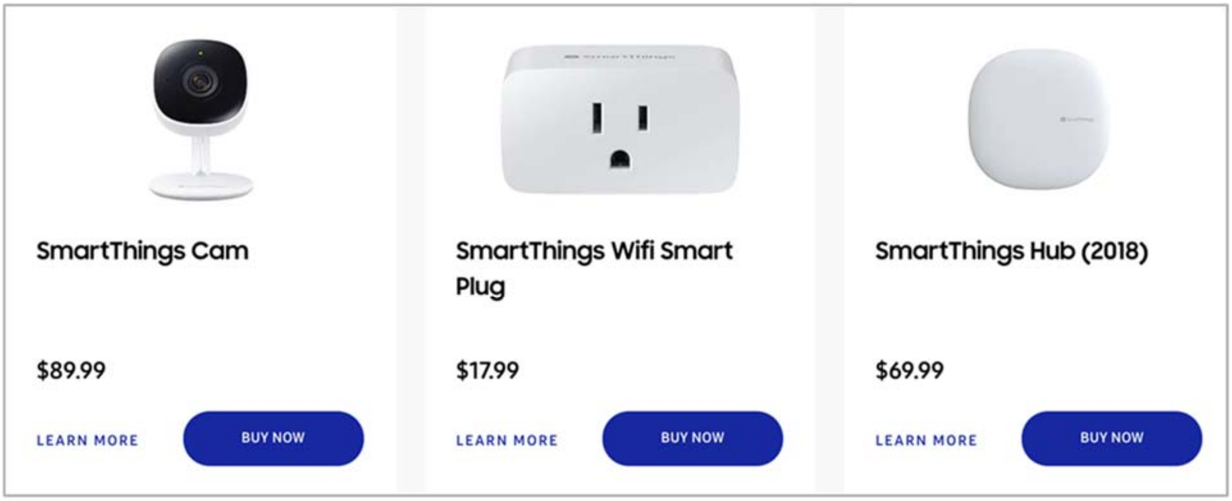
The network manager may do the following:

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

42. The Asserted Patents also cover SmartThings hubs, Smart TVs, smartphones, home appliances, audio devices, Harman connected devices, sensors, electrical outlets, and home security devices that are Wi-Fi (IEEE 802.11) compliant. For example, SmartThings devices, such as the SmartThings Camera, Smart Plug, Hub, and Tracker, are shown below.



SmartThings Cam

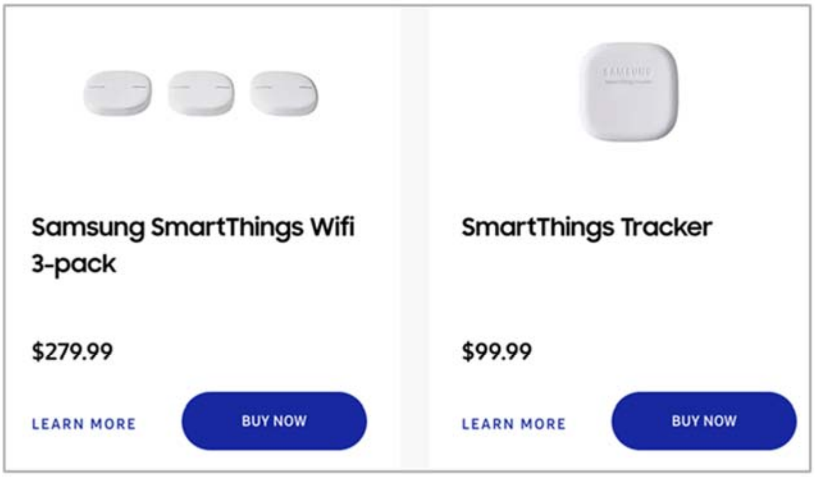
$89.99

SmartThings Wifi Smart Plug

$17.99

SmartThings Hub (2018)

$69.99

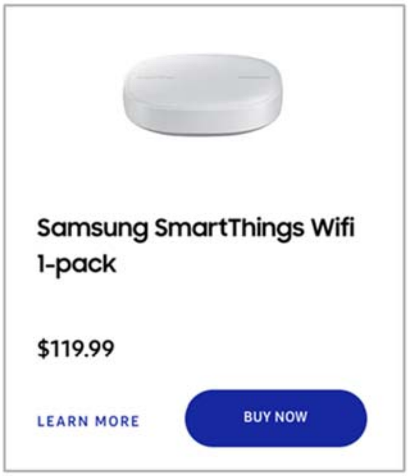


Samsung SmartThings Wifi 3-pack

$279.99

SmartThings Tracker

$99.99

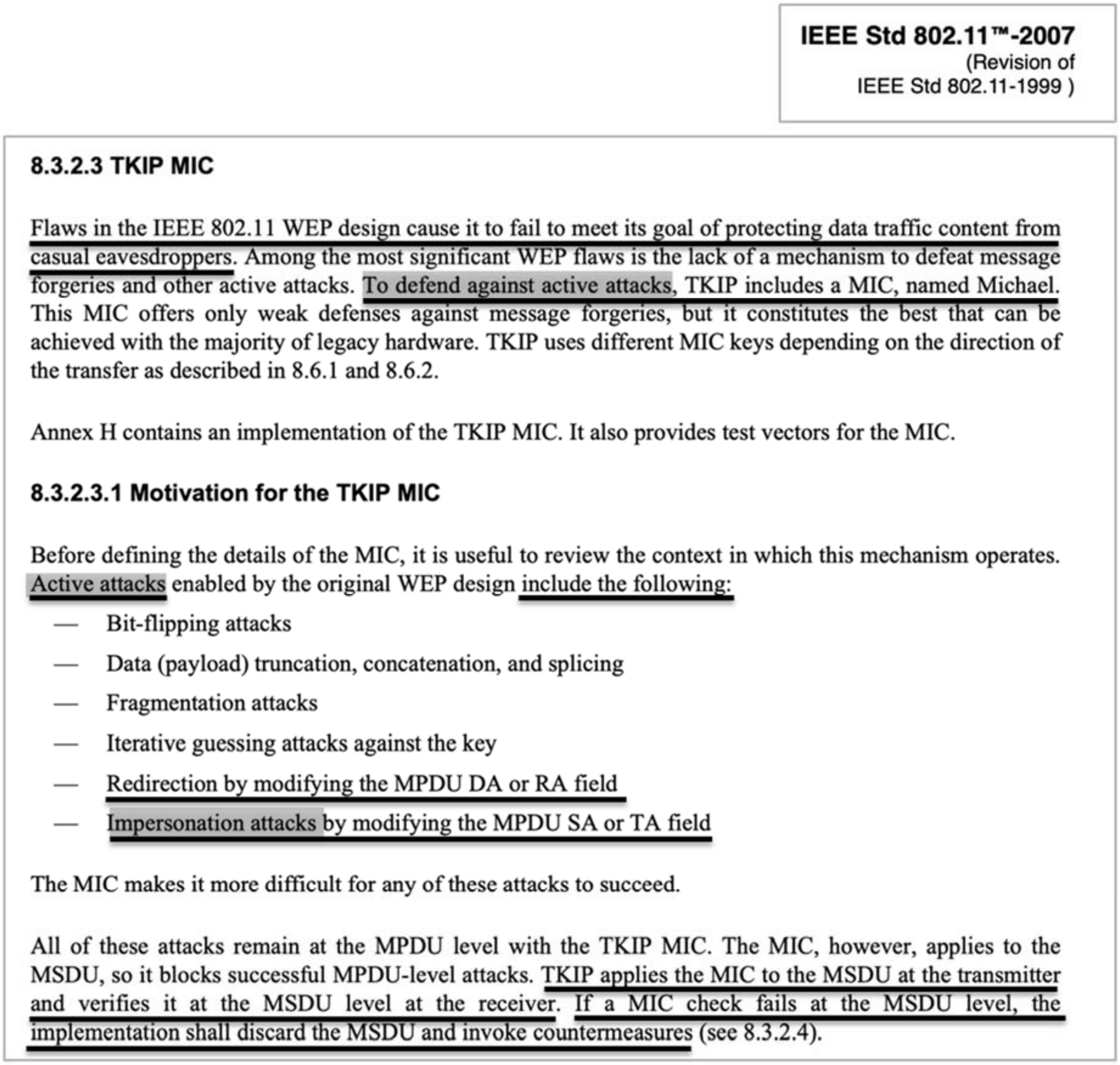


Samsung SmartThings Wifi 1-pack

$119.99

https://www.samsung.com/us/smart-home/smartthings/all-smartthings/

43. 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

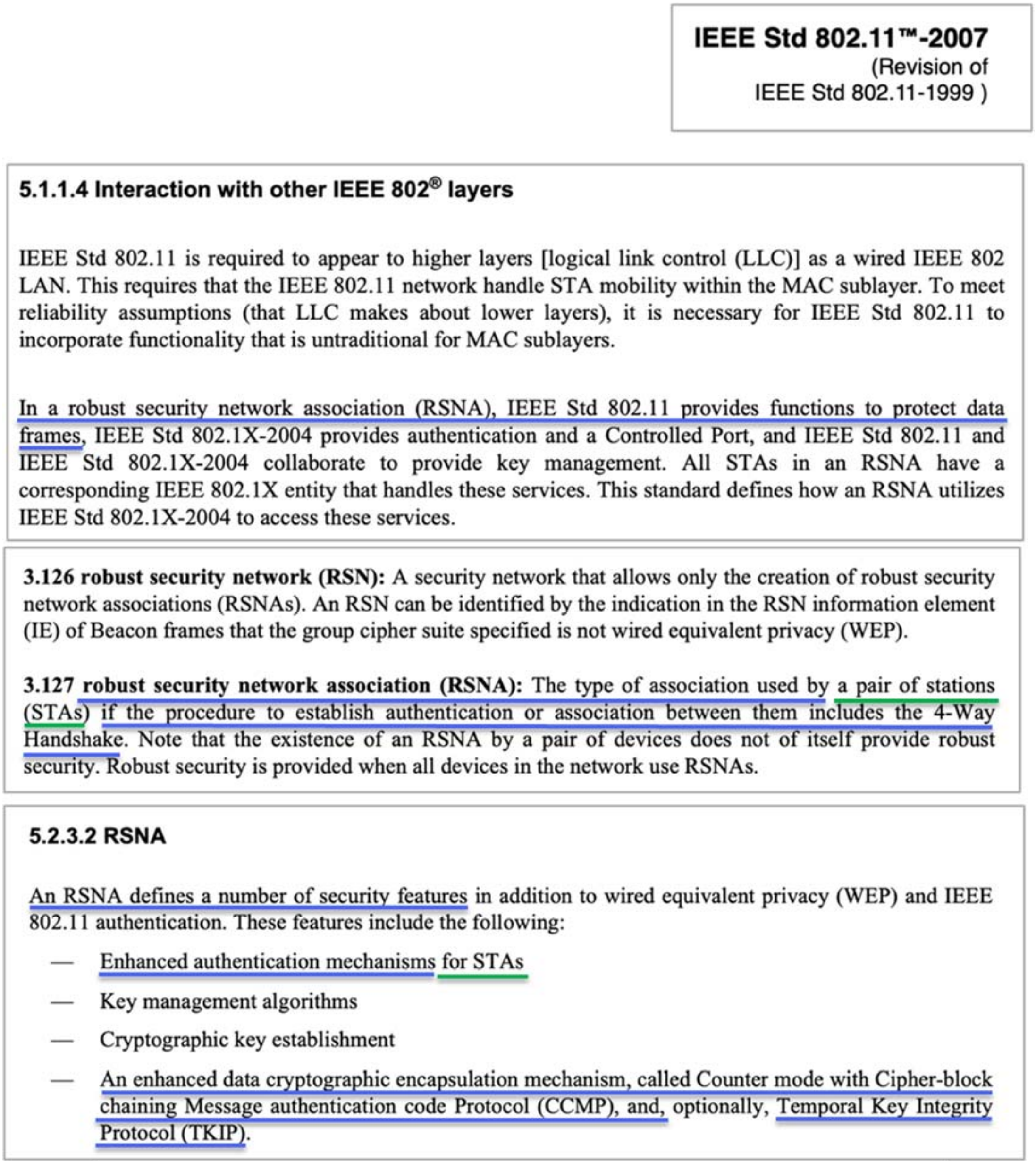
The MIC makes it more difficult for any of these attacks to succeed.

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

44. 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

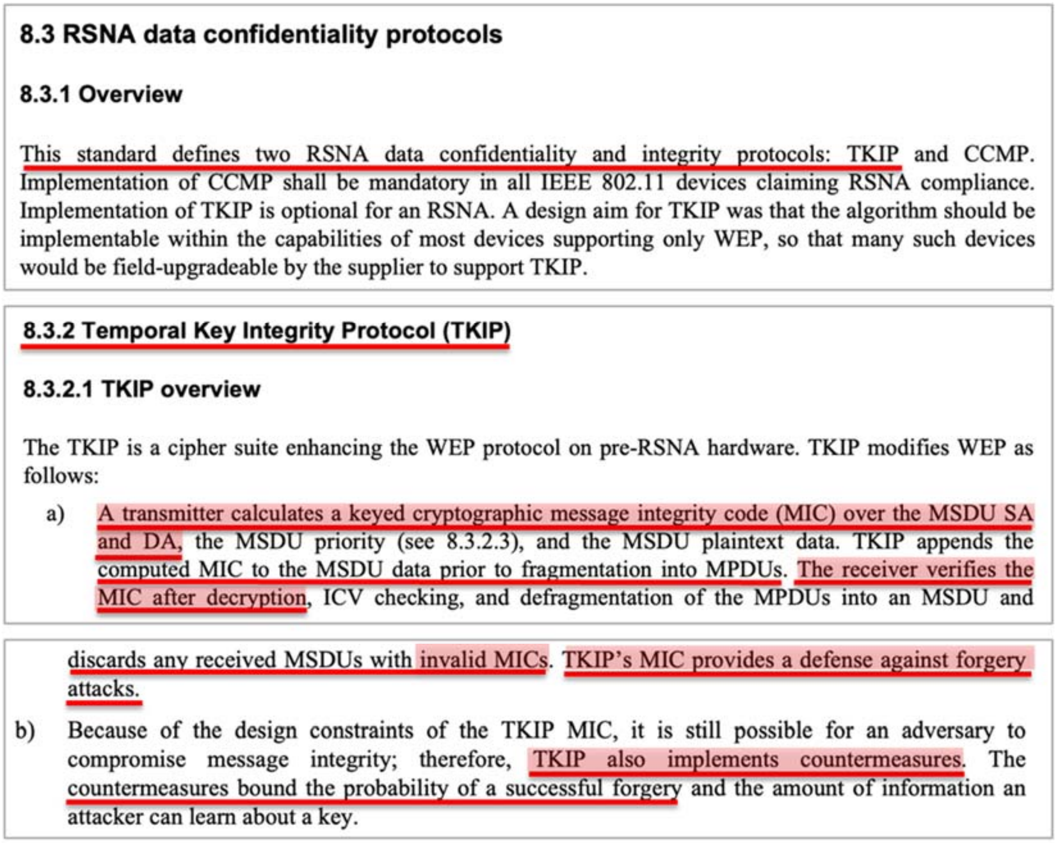
An RSNA defines a number of security features in addition to wired equivalent privacy (WEP) and IEEE 802.11 authentication. These features include the following:

- 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

45. 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

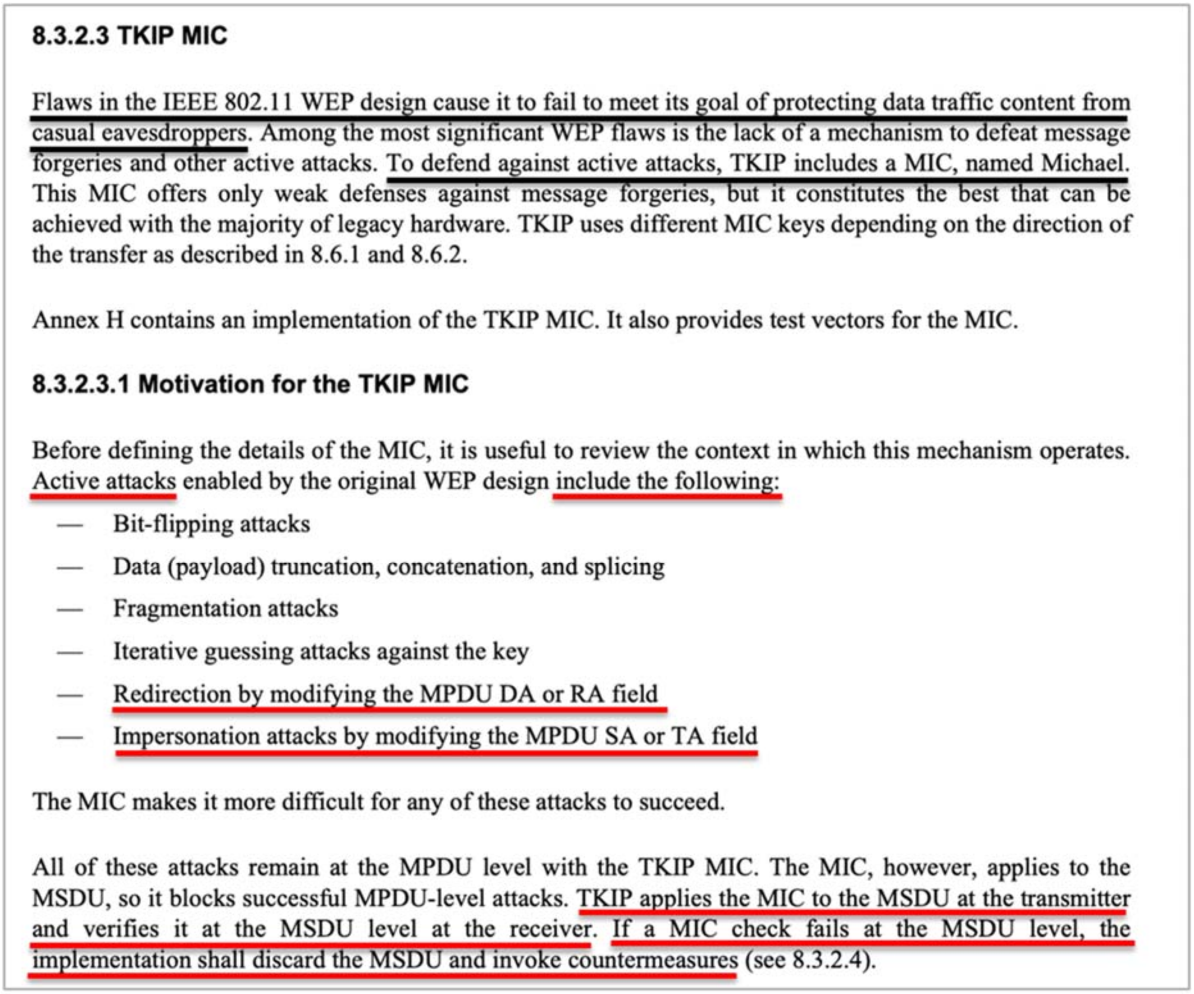
The TKIP is a cipher suite enhancing the WEP protocol on pre-RSNA hardware. TKIP modifies WEP as follows:

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

46. 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

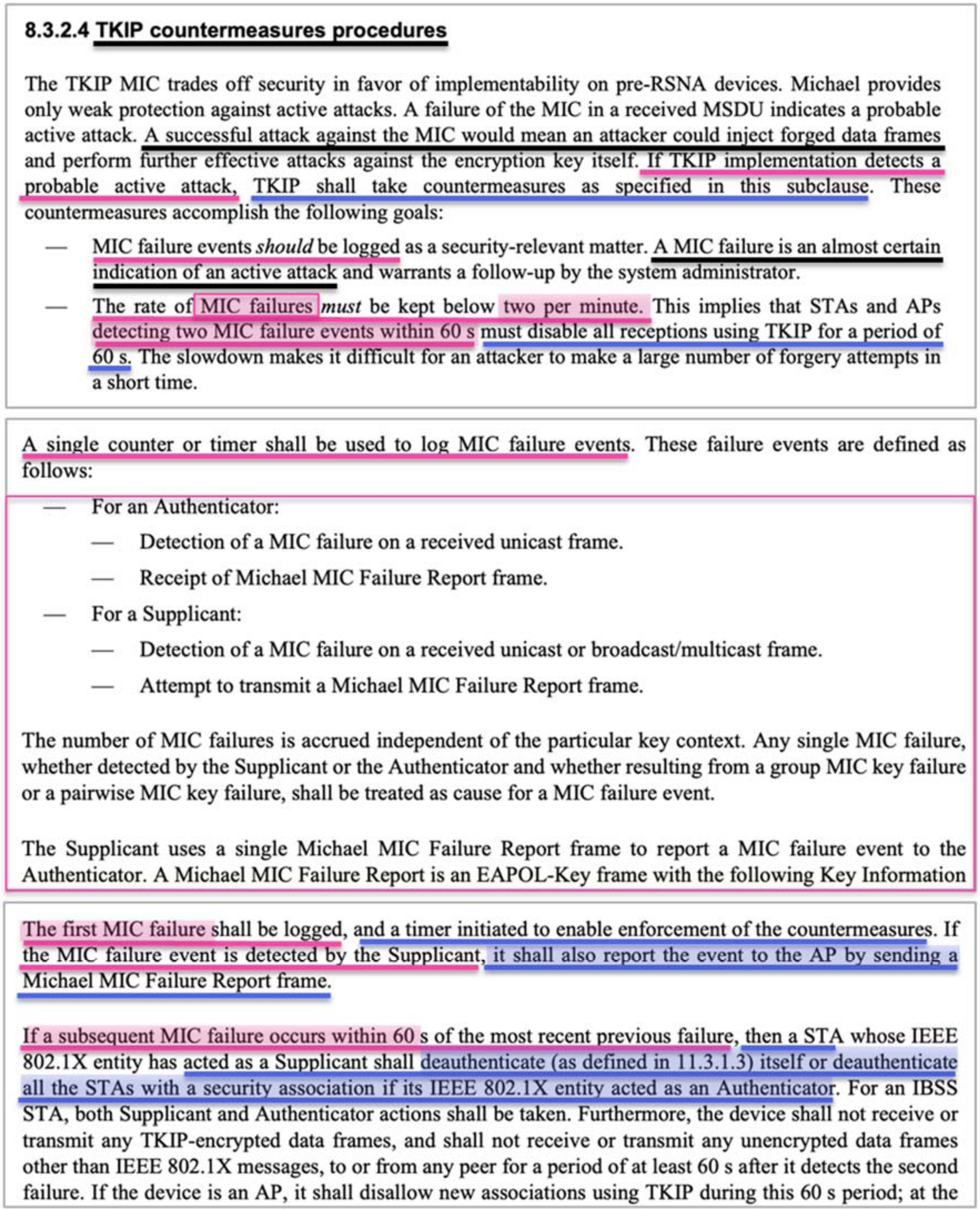
— Impersonation attacks by modifying the MPDU SA or TA field

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

47. 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

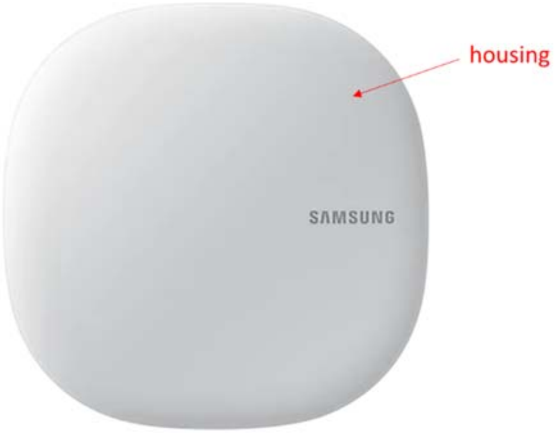
The first MIC failure shall be logged, and a timer initiated to enable enforcement of the countermeasures. If the MIC failure event is detected by the Supplicant, it shall also report the event to the AP by sending a Michael MIC Failure Report frame.

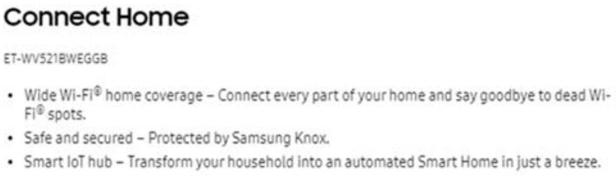
If a subsequent MIC failure occurs within 60 s of the most recent previous failure, then a STA whose IEEE 802.1X entity has acted as a Supplicant shall deauthenticate (as defined in 11.3.1.3) itself or deauthenticate all the STAs with a security association if its IEEE 802.1X entity acted as an Authenticator. 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

48. The Asserted Patents also cover SmartThings Wi-Fi compliant devices, which support WPA and WPA2-AES security mechanisms, as described below. Of the WPA and WPA2 security mechanism used by the Accused Products, such as SmartThings Wi-Fi devices, the WPA

is based on Temporal Key Integrity Protocol (TKIP), while, as described below, the WPA2-AES is based on Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP). Shown below is an exemplary IEEE 802.11 complaint SmartThings device/station (STA) from Samsung—model no. ET-WV521. The device has a housing.





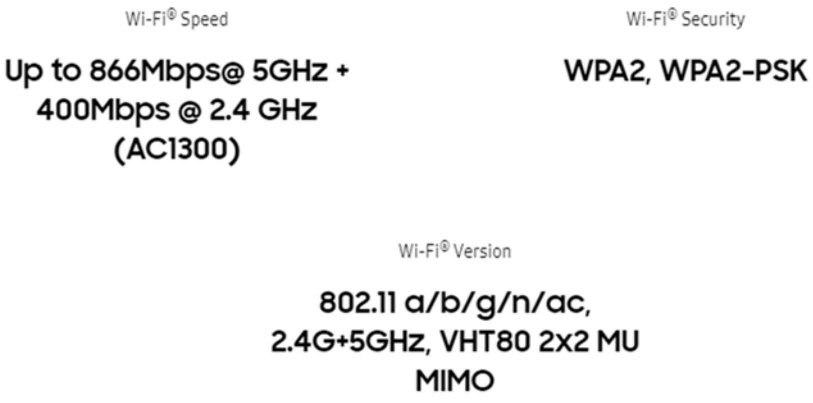
Connect Home

ET-WV521BWEGGB

- Wide Wi-Fi® home coverage – Connect every part of your home and say goodbye to dead Wi-Fi® spots.
- Safe and secured – Protected by Samsung Knox.
- Smart IoT hub – Transform your household into an automated Smart Home in just a breeze.

https://www.samsung.com/sg/smartthings/hub/samsung-connect-home-et-wv521bweggb/

49. 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.



Wi-Fi® Speed

Up to 866Mbps@ 5GHz + 400Mbps @ 2.4 GHz (AC1300)

Wi-Fi® Security

WPA2, WPA2-PSK

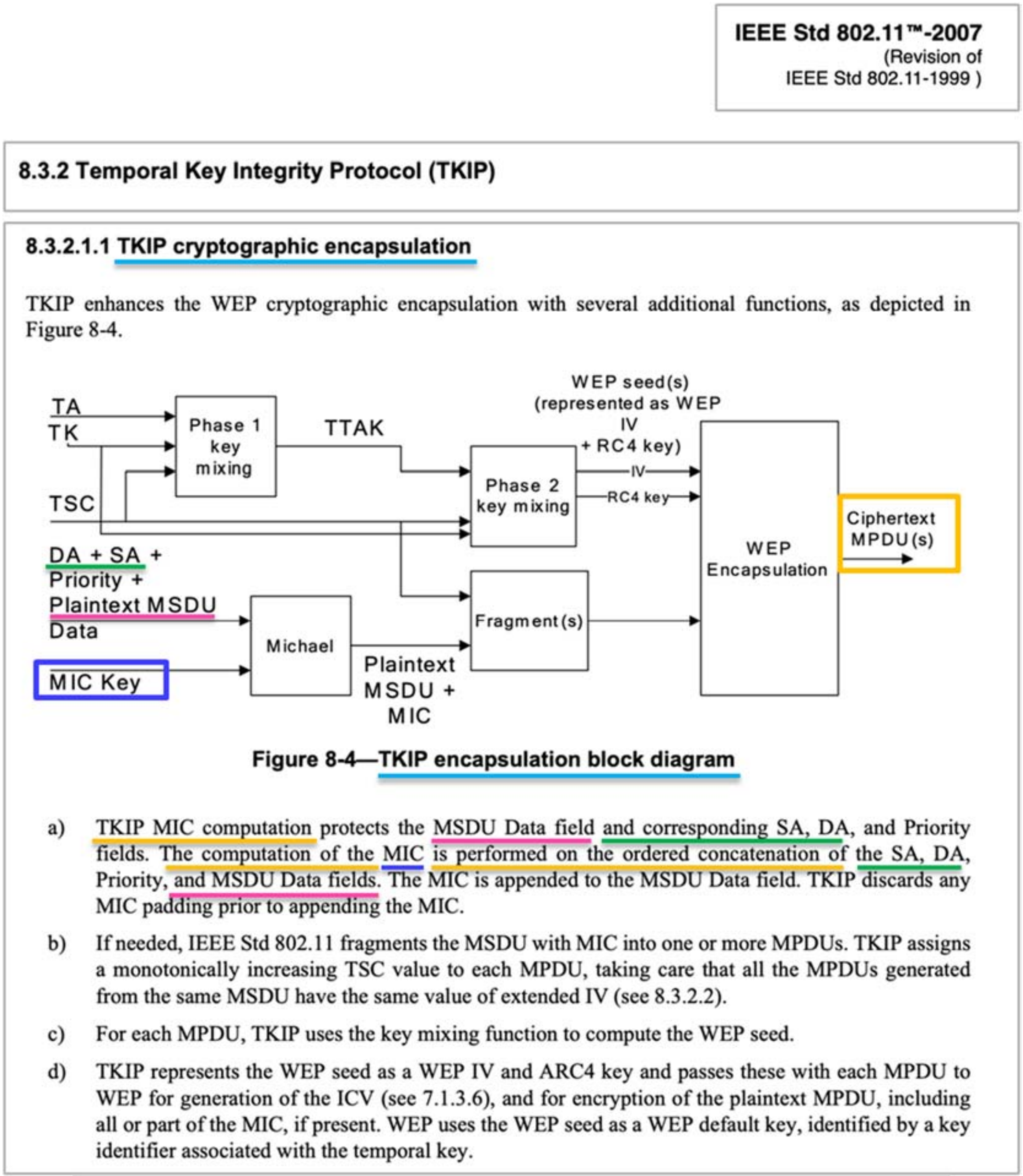
Wi-Fi® Version

802.11 a/b/g/n/ac, 2.4G+5GHz, VHT80 2x2 MU MIMO

https://www.samsung.com/sg/smartthings/hub/samsung-connect-home-et-wv521bweggb/

50. 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.

TA
TK
Phase 1 key mixing
TTAK
WEP seed(s) (represented as WEP IV + RC4 key)
IV
RC4 key
Phase 2 key mixing
TSC
WEP Encapsulation
Ciphertext MPDU(s)
DA + SA + Priority + Plaintext MSDU Data
Fragment(s)
Michael
MIC Key
Plaintext MSDU + MIC

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)

51. Plaintiff incorporates paragraphs 1 through 50 herein by reference.

52. 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.

53. 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.

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

55. Upon information and belief, Samsung designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via SEC's subsidiaries, such as Defendant SEA and STI, partners, distributors, retails, customers, and consumers.

56. Defendants SEC and SEA (i.e., "Samsung") 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, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants SEC and SEA make and sell the Accused Products outside of the United States, deliver those products to their customers, distributors, and/or subsidiaries in the United States, or in the case that they deliver the Accused Products outside of the United States they do so intending and/or knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby directly infringing the '117 patent. *See, e.g., Lake Cherokee Hard*

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

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

58. For example, Samsung infringes claim 24 of the '117 patent via the Accused Products that use ZigBee protocol to communicate with each other, such as, for example, Samsung IoT and smart home devices. 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.

59. At a minimum, Samsung has known of the ’117 patent at least as early as the filing date of the complaint. In addition, Samsung has known about the ’117 patent since at least April 10, 2018, when Samsung received a letter regarding infringement of the patent portfolio including the ’117 patent related to wireless communication network products, which specifically referenced the infringing use of IEEE 802 and ZigBee standards, as well as Samsung’s SmartThings products. Additionally, on August 28, 2018, as a continuation of the previous correspondence, Samsung received a licensing proposal regarding, *inter alia*, the ’117 patent.

60. Upon information and belief, since at least the above-mentioned date when Samsung was on notice of its infringement, Defendants SEC and SEA have each actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, 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 SEC and SEA each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’117 patent. Upon information and belief, Defendants SEC and SEA each intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these

products to purchasers and prospective buyers, testing 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.*, *SmartThings Enabled Hubs*, SMARTTHINGS, https://support.smartthings.com/hc/en-us/articles/360052390151-SmartThings-Enabled-Hubs (last visited January 14, 2021) (Under subheading "Control your SmartThings Enabled Hub": "These settings will control Zigbee and Z-Wave functions in your hub…To access the Zigbee settings of your SmartThings enabled hub, follow these steps"); *Samsung Connect Home User Manual*, revision 1.1 at 15, SAMSUNG, https://downloadcenter.samsung.com/content/UM/201803/20180302135432816/ET-WV530_UM_USA_Type_Rev.1.1_180302.pdf (March 2018) ("Register the Internet of Things (IoT) devices that support Z-Wave, zigbee (sic), LAN, or Cloud-to-Cloud to the SmartThings app and control them"). Furthermore, Samsung markets SmartThings devices and its application software as working with 100s of compatible devices that function within the same networks as the SmartThings devices. Such compatibility provides convenience and added functionality that induces consumers to use the SmartThings devices and thus further infringe the '117 patent. *See SmartThings*, SAMSUNG, https://www.samsung.com/us/smart-home/#compatibility (listing third-party manufacturers of compatible devices, including Google Assistant, Philips Hue, Amazon Alexa, Schlage, Arlo, Ecobee, Ring and Honeywell, among others, and stating "Control it all through the SmartThings app").

61. Upon 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, Samsung has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Samsung's infringing activities relative to the '117 patent have been,

and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

62. Plaintiff Stingray has been damaged as a result of Samsung's infringing conduct described in this Count. Samsung is thus liable to Stingray in an amount that adequately compensates Stingray for Samsung'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)

63. Plaintiff incorporates paragraphs 1 through 62 herein by reference.

64. 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.

65. 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.

66. Samsung has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the '678 patent in this judicial district and elsewhere in Texas and the United States.

67. Upon information and belief, Samsung designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via SEC's subsidiaries, such as Defendant SEA and STI, partners, distributors, retails, customers, and consumers.

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

69. Furthermore, Defendant SEC directly infringes the '678 patent through its direct involvement in the activities of its subsidiaries, including Defendant SEA and STI, including by selling and offering for sale the Accused Products directly to SEA and importing the Accused Products into the United States for SEA. Upon information and belief, SEA conducts activities that constitutes direct infringement of the '678 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products. SEC is vicariously liable

for this infringing conduct of SEA, STI, and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and belief, Defendants SEC and SEA are essentially the same company, and Samsung has the right and ability to control SEA's infringing acts and receives a direct financial benefit from SEA's infringement.

70. For example, Samsung infringes claim 51 of the '678 patent via the Accused Products that use IEEE 802.11 protocol to communicate with each other, such as, for example, Samsung SmartThings products. 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.

71. At a minimum, Samsung has known of the '678 patent at least as early as the filing date of the complaint. In addition, Samsung has known about the '678 patent since at least April 10, 2018, when Samsung received a letter regarding infringement of the patent portfolio, which includes the '678 patent related to wireless communication network products. The letter specifically referenced the infringing use of IEEE 802 and ZigBee standards, as well as Samsung's SmartThings products. Additionally, on August 28, 2018, as a continuation of the previous correspondence, Samsung received a licensing proposal regarding, *inter alia*, the '678 patent.

72. Upon information and belief, since at least the above-mentioned date when Samsung was on notice of its infringement, Defendants SEC and SEA have each actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, 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 SEC and SEA each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’678 patent. Upon information and belief, Defendants SEC and SEA each intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing 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.*, *SmartThings Enabled Hubs*, SMARTTHINGS, https://support.smartthings.com/hc/en-us/articles/360052390151-SmartThings-Enabled-Hubs (last visited January 14, 2021) (Under subheading “Control your SmartThings Enabled Hub”: “These settings will control Zigbee and Z-Wave functions in your hub…To access the Zigbee settings of your SmartThings enabled hub, follow these steps”); *Samsung Connect Home User Manual*, revision 1.1 at 15, SAMSUNG, https://downloadcenter.samsung.com/content/UM/201803/20180302135432816/ET-

WV530_UM_USA_Type_Rev.1.1_180302.pdf (March 2018) ("Register the Internet of Things (IoT) devices that support Z-Wave, zigbee (sic), LAN, or Cloud-to-Cloud to the SmartThings app and control them"). Furthermore, Samsung markets SmartThings devices and its application software as working with 100s of compatible devices that function within the same networks as the SmartThings devices. Such compatibility provides convenience and added functionality that induces consumers to use the SmartThings devices and thus further infringe the '678 patent. *See SmartThings*, SAMSUNG, https://www.samsung.com/us/smart-home/#compatibility (listing third-party manufacturers of compatible devices, including Google Assistant, Philips Hue, Amazon Alexa, Schlage, Arlo, Ecobee, Ring and Honeywell, among others, and stating "Control it all through the SmartThings app").

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

74. Plaintiff Stingray has been damaged as a result of Samsung's infringing conduct described in this Count. Samsung is thus liable to Stingray in an amount that adequately compensates Stingray for Samsung'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)

75. Plaintiff incorporates paragraphs 1 through 74 herein by reference.

76. 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.

77. 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.

78. Samsung has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’572 patent in this judicial district and elsewhere in Texas and the United States.

79. Upon information and belief, Samsung designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via SEC’s subsidiaries, such as Defendant SEA and STI, partners, distributors, retails, customers, and consumers.

80. Defendants SEC and SEA (i.e., “Samsung”) 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, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants SEC and SEA make and sell the Accused Products outside of the United States, deliver those products to their customers, distributors, and/or subsidiaries in the United States, or in the case that they deliver the Accused Products outside of the United States they do so intending and/or

knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby directly infringing the ’572 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to “whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)”).

81. Furthermore, Defendant SEC directly infringes the ’572 patent through its direct involvement in the activities of its subsidiaries, including Defendant SEA and STI, including by selling and offering for sale the Accused Products directly to SEA and importing the Accused Products into the United States for SEA. Upon information and belief, SEA conducts activities that constitutes direct infringement of the ’572 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products. SEC is vicariously liable for this infringing conduct of SEA, STI, and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and belief, Defendants SEC and SEA are essentially the same company, and Samsung has the right and ability to control SEA’s infringing acts and receives a direct financial benefit from SEA’s infringement.

82. For example, Samsung infringes claim 1 of the ’572 patent via the Accused Products that use IEEE 802.11 protocol to communicate with each other, such as, for example, Samsung SmartThings products. 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.

83. Samsung 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. Upon 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.

84. Samsung 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.

85. At a minimum, Samsung has known of the ’572 patent at least as early as the filing date of the complaint. In addition, Samsung has known about the ’572 patent since at least April 10, 2018, when Samsung received a letter regarding infringement of the patent portfolio including the ’572 patent related to wireless communication network products, which specifically referenced the infringing use of IEEE 802 and ZigBee standards, as well as Samsung’s SmartThings products. Additionally, on August 28, 2018, as a continuation of the previous correspondence, Samsung received a licensing proposal regarding, *inter alia*, the ’572 patent.

86. Upon information and belief, since at least the above-mentioned date when Samsung was on notice of its infringement, Defendants SEC and SEA have each actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, 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 SEC and SEA each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the '572 patent. Upon information and belief, Defendants SEC and SEA each intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing 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.*, *SmartThings Enabled Hubs*, SMARTTHINGS, https://support.smartthings.com/hc/en-us/articles/360052390151-SmartThings-Enabled-Hubs (last visited January 14, 2021) (Under subheading "Control your SmartThings Enabled Hub": "These settings will control Zigbee and Z-Wave functions in your hub…To access the Zigbee settings of your SmartThings enabled hub, follow these steps"); *Samsung Connect Home User Manual*, revision 1.1 at 15, SAMSUNG, https://downloadcenter.samsung.com/content/UM/201803/20180302135432816/ET-

WV530_UM_USA_Type_Rev.1.1_180302.pdf (March 2018) ("Register the Internet of Things (IoT) devices that support Z-Wave, zigbee (sic), LAN, or Cloud-to-Cloud to the SmartThings app and control them"). Furthermore, Samsung markets SmartThings devices and its application software as working with 100s of compatible devices that function within the same networks as the SmartThings devices. Such compatibility provides convenience and added functionality that induces consumers to use the SmartThings devices and thus further infringe the '572 patent. *See SmartThings*, SAMSUNG, https://www.samsung.com/us/smart-home/#compatibility (listing third-party manufacturers of compatible devices, including Google Assistant, Philips Hue, Amazon Alexa, Schlage, Arlo, Ecobee, Ring and Honeywell, among others, and stating "Control it all through the SmartThings app").

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

88. Plaintiff Stingray has been damaged as a result of Samsung's infringing conduct described in this Count. Samsung is thus liable to Stingray in an amount that adequately compensates Stingray for Samsung'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)

89. Plaintiff incorporates paragraphs 1 through 88 herein by reference.

90. 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.

91. 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.

92. Samsung has and continues to directly and/or indirectly infringe (by inducing infringement) one or more claims of the ’961 patent in this judicial district and elsewhere in Texas and the United States.

93. Upon information and belief, Samsung designs, develops, manufactures, imports, distributes, offers to sell, sells, and uses the Accused Products, including via SEC’s subsidiaries, such as Defendant SEA and STI, partners, distributors, retails, customers, and consumers.

94. Defendants SEC and SEA (i.e., “Samsung”) 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, distributors, importers, customers, subsidiaries, and/or consumers. Furthermore, upon information and belief, Defendants SEC and SEA make and sell the Accused Products outside of the United States, deliver those products to their customers, distributors, and/or subsidiaries in the United States, or in the case that they deliver the Accused Products outside of the United States they do so intending and/or

knowing that those products are destined for the United States and/or designing those products for sale in the United States, thereby directly infringing the '961 patent. *See, e.g., Lake Cherokee Hard Drive Techs., L.L.C. v. Marvell Semiconductor, Inc.*, 964 F. Supp. 2d 653, 658 (E.D. Tex. 2013) (denying summary judgment and allowing presentation to jury as to "whether accused products manufactured and delivered abroad but imported into the United States market by downstream customers … constitute an infringing sale under § 271(a)").

95. Furthermore, Defendant SEC directly infringes the '961 patent through its direct involvement in the activities of its subsidiaries, including Defendant SEA and STI, including by selling and offering for sale the Accused Products directly to SEA and importing the Accused Products into the United States for SEA. Upon information and belief, SEA conducts activities that constitutes direct infringement of the '961 patent under 35 U.S.C. § 271(a) by making, importing, offering for sale, selling, and/or using those Accused Products. SEC is vicariously liable for this infringing conduct of SEA, STI, and other subsidiaries (under both the alter ego and agency theories) because, as an example and on information and belief, Defendants SEC and SEA are essentially the same company, and Samsung has the right and ability to control SEA's infringing acts and receives a direct financial benefit from SEA's infringement.

96. For example, Samsung infringes claim 1 of the '961 patent via the Accused Products such as Samsung SmartThings products that use ZigBee protocol to communicate with each other. 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.

97. At a minimum, Samsung has known of the ’961 patent at least as early as the filing date of the complaint. In addition, Samsung has known about the ’961 patent since at least April 10, 2018, when Samsung received a letter regarding infringement of the patent portfolio, which includes the ’961 patent related to wireless communication network products. The letter specifically referenced the infringing use of IEEE 802 and ZigBee standards, as well as Samsung’s SmartThings products. Additionally, on August 28, 2018, as a continuation of the previous correspondence, Samsung received a licensing proposal regarding, *inter alia*, the ’961 patent.

98. Upon information and belief, since at least the above-mentioned date when Samsung was on notice of its infringement, Defendants SEC and SEA have each actively induced, under U.S.C. § 271(b), its distributors, customers, subsidiaries, importers, and/or consumers that import, purchase, 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 SEC and SEA each do so with knowledge, or with willful blindness of the fact, that the induced acts constitute infringement of the ’961 patent. Upon information and belief, Defendants SEC and SEA each intends to cause, and has taken affirmative steps to induce, infringement by distributors, importers, customers, subsidiaries, and/or consumers by at least, *inter alia*, creating advertisements that promote the infringing use of the Accused Products, creating and/or maintaining established distribution channels for the Accused Products into and within the United States, manufacturing the Accused Products in conformity with U.S. laws and regulations, distributing or making available instructions or manuals for these products to purchasers and prospective buyers, testing 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.*, *SmartThings Enabled Hubs*, SMARTTHINGS, https://support.smartthings.com/hc/en-us/articles/360052390151-SmartThings-Enabled-Hubs (last visited January 14, 2021) (Under subheading “Control your SmartThings Enabled Hub”: “These settings will control Zigbee and Z-Wave functions in your hub…To access the Zigbee settings of your SmartThings enabled hub, follow these steps”); *Samsung Connect Home User Manual*, revision 1.1 at 15, SAMSUNG, https://downloadcenter.samsung.com/content/UM/201803/20180302135432816/ET-WV530_UM_USA_Type_Rev.1.1_180302.pdf (March 2018) (“Register the Internet of Things (IoT) devices that support Z-Wave, zigbee (sic), LAN, or Cloud-to-Cloud to the SmartThings app and control them”). Furthermore, Samsung markets SmartThings devices and its application software as working with 100s of compatible devices that function within the same networks as the SmartThings devices. Such compatibility provides convenience and added functionality that induces consumers to use the SmartThings devices and thus further infringe the ’961 patent. *See*

SmartThings, SAMSUNG, https://www.samsung.com/us/smart-home/#compatibility (listing third-party manufacturers of compatible devices, including Google Assistant, Philips Hue, Amazon Alexa, Schlage, Arlo, Ecobee, Ring and Honeywell, among others, and stating "Control it all through the SmartThings app").

99. Upon 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, Samsung has nevertheless continued its infringing conduct and disregarded an objectively high likelihood of infringement. Samsung's infringing activities relative to the '961 patent have been, and continue to be, willful, wanton, malicious, in bad-faith, deliberate, consciously wrongful, flagrant, characteristic of a pirate, and an egregious case of misconduct beyond typical infringement such that Plaintiff is entitled under 35 U.S.C. § 284 to enhanced damages up to three times the amount found or assessed.

100. Plaintiff Stingray has been damaged as a result of Samsung's infringing conduct described in this Count. Samsung is thus liable to Stingray in an amount that adequately compensates Stingray for Samsung'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

101. 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.

102. 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

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

PRAYER FOR RELIEF

104. 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: January 29, 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
BRAGALONE CONROY PC
2200 Ross Avenue
Suite 4500W
Dallas, TX 75201
Tel: (214) 785-6670
Fax: (214) 785-6680
jbragalone@bcpc-law.com
tsaad@bcpc-law.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