IEEE P802.11
Wireless LANs

|  |
| --- |
| TGaz November-January 2020 telecon meeting minutes |
| Date: 2020-11-18 |
| Author(s): |
| Name | Affiliation | Address | Phone | email |
| Assaf Kasher | Qualcomm |  |  | akasher@qti.qualcomm.com |
|  |  |  |  |  |

Abstract

This document contains telecon minutes for the TGaz telecons between the November 2-10, 2020, cancelled plenary and the January 2021 interim.

1. **TGaz – November 18th 2020**
	1. Called to order by TGaz Chair, Jonathan Segev (Intel Corporation) and Vice Chair and secretary (active), Assaf Kasher (Qualcomm), at **10:02am PDT,**
	2. Agenda Doc. **IEEE 802.11-20/01570r12 (in progress - slide 31)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, duty to inform, the guideline for IEEE WG meetings and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped forward.
		3. Chair reminded participants to register their attendance using imat.
		4. Chair reviewed other guidelines for IEEE meetings, asked if any clarifications are requested, no one stepped forward.
		5. Chair reviewed IEEE copyright policy, – no clarification requested
		6. Chair reviewed IEEE code of ethics and WG participation as an individual professional. – no clarification requested
		7. Chair reviewed IEEE 802 ground rules
		8. Recorded Participation requirement
		Headcount: ~33 present
	4. Agenda
		1. Review Telecon Schedule
		2. Submission:
			1. 11-20-1817 Proposed resolution to 111az lb249 CID 3900 (Qi Wang) – 15min
			2. 11-20-1097 Secure LTF using DFT precoded OFDM (Christian Berger) – 35min
			3. 11-20-1373 Attacks to Full Radom OFDM sounding Signal (Qinghua Li) – as time permits
		3. AOB
	5. Submission pipline:
		1. Slide 81 of 1570r12
	6. Telecon Schedule
		1. 3 telecons added
	7. Qi Wang Presented 11-20-1817
		1. CID 3900
		2. Requires further discussion – will be brought again
	8. Christian Berger presented 11-20-1097
		1. Secure LTF using DFT precoded OFDM
		2. Q: can you provide the window function
		3. R: \betta defines the area , the rest raised cosine
		4. Q: attack analysis is missing
		5. R: I have not come with any attacker than can predict the second half based on the first half.
		6. Q: is it the same has having gaussian signal in the frequency domain
		7. R:
	9. Attendance:

|  |  |  |  |
| --- | --- | --- | --- |
| TGaz | 11/18 | Agrawal, abhishek | ON Semiconductor |
| TGaz | 11/18 | Au, Kwok Shum | Huawei Technologies Co.,  Ltd |
| TGaz | 11/18 | Bahn, Christy | IEEE STAFF |
| TGaz | 11/18 | Batra, Anuj | Apple, Inc. |
| TGaz | 11/18 | Berger, Christian | NXP Semiconductors |
| TGaz | 11/18 | Bhandaru, Nehru | Broadcom Corporation |
| TGaz | 11/18 | Cheng, Xilin | NXP Semiconductors |
| TGaz | 11/18 | Grandhe, Niranjan | NXP Semiconductors |
| TGaz | 11/18 | Harkins, Daniel | Hewlett Packard Enterprise |
| TGaz | 11/18 | Henry, Jerome | Cisco Systems, Inc. |
| TGaz | 11/18 | Kasher, Assaf | Qualcomm Incorporated |
| TGaz | 11/18 | Kim, Youhan | Qualcomm Incorporated |
| TGaz | 11/18 | Li, Qinghua | Intel Corporation |
| TGaz | 11/18 | Lindskog, Erik | SAMSUNG |
| TGaz | 11/18 | Lou, Hui-Ling | NXP Semiconductors |
| TGaz | 11/18 | Mirfakhraei, Khashayar | Cisco Systems, Inc. |
| TGaz | 11/18 | NANDAGOPALAN, SAI SHANKAR | Cypress Semiconductor Corporation |
| TGaz | 11/18 | Raissinia, Alireza | Qualcomm Incorporated |
| TGaz | 11/18 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGaz | 11/18 | Segev, Jonathan | Intel Corporation |
| TGaz | 11/18 | Shellhammer, Stephen | Qualcomm Incorporated |
| TGaz | 11/18 | Shor, Gadi | Intel Corporation |
| TGaz | 11/18 | Stacey, Robert | Intel Corporation |
| TGaz | 11/18 | SUH, JUNG HOON | Huawei Technologies Co. Ltd |
| TGaz | 11/18 | Tian, Bin | Qualcomm Incorporated |
| TGaz | 11/18 | Wang, Qi | Apple, Inc. |
| TGaz | 11/18 | Wang, Yi-Hsiu | Zeku |
| TGaz | 11/18 | Want, Roy | Google |
| TGaz | 11/18 | Wu, Tianyu | Apple, Inc. |
| TGaz | 11/18 | Yee, Peter | NSA-CSD |
| TGaz | 11/18 | Zeng, Ruochen | NXP Semiconductors |

1. **TGaz – December 2nd 2020**
	1. Called to order by TGaz Chair, Jonathan Segev (Intel Corporation) and Vice Chair and secretary (active), Assaf Kasher (Qualcomm), at **10:02am PDT,**
	2. Agenda Doc. **IEEE 802.11-20/01570r12 (in progress - slide 31)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, duty to inform, the guideline for IEEE WG meetings and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped forward.
		3. Chair reminded participants to register their attendance using imat.
		4. Chair reviewed other guidelines for IEEE meetings, asked if any clarifications are requested, no one stepped forward.
		5. Chair reviewed IEEE copyright policy, – no clarification requested
		6. Chair reviewed IEEE code of ethics and WG participation as an individual professional. – no clarification requested
		7. Chair reviewed IEEE 802 ground rules
		8. Recorded Participation requirement
		Headcount: ~33 present
	4. Agenda
		1. Review Telecon Schedule
		2. Draft 2.6 status
		3. Submission:
			1. 11-20-1373 Attacks to fully radndom OFDM soundisingal (Qinghua Li) – for completeion
			2. 11-20-1855 – further updates on 11az sedure LTF design (Anuj Batra) – 45 minutes
			3. Seure LTFs: additional Design details (Steve Shellhammer) – as time permits
	5. Roy Want reviewed D2.6
		1. D2.6 includes all changes motioned up to and including the November plenary.
	6. Qinghua Li presented 11-20-1373
		1. Q: The table is misleading – the complexity of FD attack – FFT complexity is NxlogN ,
		2. Q: I also think slide 39 is misleading. 1) Time domain attack has more security correlation 2) The fundemental TD is the ICI . – FD attack generates less correlation. 3) complexity does show the full story. In time domain, its only FR filter. In the frequency domain it is the FFT.
		3. Q: FD attack limiting factor is complexity. TD: attack has no complexity issue but has the issue of transmit and receiver on the same time.
		4. Q: FD attack is very complex. TD attack is stronger.
		5. Q: FD attack is complexity. In TD do we need to transmit and receiver simultaneously
	7. Anuj Batra presented 11-20-1855
		1. Q: for concurrent Tx and Rx getting 40dB SNR is difficult.
		2. Q: Can you explain the benefit of the 4-PSK addition – R: minimum distance becomes small – will make sphere decoding harder and creates error propagation
		3. Q: what is the advantage of 64-QAm +4-PSK : R: this is a balance between complexity and security which is reasonable for implementation
		4. Q: this 4x4 for 64-QAM, what will happen if 6x6 will be used? R: I don’t believe it will work, I need to look at data.
	8. Meeting ended abruptly (webex technical issue at 12:00PM PST)
	9. Attendance

|  |  |  |  |
| --- | --- | --- | --- |
| TGaz | 12/2 | Agrawal, abhishek | ON Semiconductor |
| TGaz | 12/2 | Aldana, Carlos | Facebook |
| TGaz | 12/2 | Au, Kwok Shum | Huawei Technologies Co.,  Ltd |
| TGaz | 12/2 | Batra, Anuj | Apple, Inc. |
| TGaz | 12/2 | Berger, Christian | NXP Semiconductors |
| TGaz | 12/2 | Bhandaru, Nehru | Broadcom Corporation |
| TGaz | 12/2 | Boldy, David | Broadcom Corporation |
| TGaz | 12/2 | Cepni, Gurkan | Apple, Inc. |
| TGaz | 12/2 | Grandhe, Niranjan | NXP Semiconductors |
| TGaz | 12/2 | Henry, Jerome | Cisco Systems, Inc. |
| TGaz | 12/2 | Kasher, Assaf | Qualcomm Incorporated |
| TGaz | 12/2 | Kim, Youhan | Qualcomm Incorporated |
| TGaz | 12/2 | Lindskog, Erik | SAMSUNG |
| TGaz | 12/2 | Liu, Jianhan | MediaTek Inc. |
| TGaz | 12/2 | Montreuil, Leo | Broadcom Corporation |
| TGaz | 12/2 | NANDAGOPALAN, SAI SHANKAR | Cypress Semiconductor Corporation |
| TGaz | 12/2 | Palm, Stephen | Broadcom Corporation |
| TGaz | 12/2 | Pare, Thomas | MediaTek Inc. |
| TGaz | 12/2 | Petry, Brian | Broadcom Corporation |
| TGaz | 12/2 | Raissinia, Alireza | Qualcomm Incorporated |
| TGaz | 12/2 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGaz | 12/2 | Segev, Jonathan | Intel Corporation |
| TGaz | 12/2 | Shellhammer, Stephen | Qualcomm Incorporated |
| TGaz | 12/2 | Shor, Gadi | Intel Corporation |
| TGaz | 12/2 | Sosack, Robert | Molex Incorporated |
| TGaz | 12/2 | Stacey, Robert | Intel Corporation |
| TGaz | 12/2 | Tian, Bin | Qualcomm Incorporated |
| TGaz | 12/2 | Verma, Sindhu | Broadcom Corporation |
| TGaz | 12/2 | Wang, Chao Chun | MediaTek Inc. |
| TGaz | 12/2 | Wang, Qi | Apple, Inc. |
| TGaz | 12/2 | Wang, Yi-Hsiu | Zeku |
| TGaz | 12/2 | Want, Roy | Google |
| TGaz | 12/2 | Wu, Tianyu | Apple, Inc. |
| TGaz | 12/2 | Yee, Peter | NSA-CSD |
| TGaz | 12/2 | Young, Christopher | Broadcom Corporation |
| TGaz | 12/2 | Zhang, Hongyuan | Marvell Semiconductor, Inc. |

1. **TGaz – December 9th d 2020**
	1. Called to order by TGaz Chair, Jonathan Segev (Intel Corporation) and Vice Chair and secretary (active), Assaf Kasher (Qualcomm), at **10:02am PDT,**
	2. Agenda Doc. **IEEE 802.11-20/01570r16 (in progress - slide 31)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, duty to inform, the guideline for IEEE WG meetings and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped forward.
		3. Chair reminded participants to register their attendance using imat.
		4. Chair reviewed other guidelines for IEEE meetings, asked if any clarifications are requested, no one stepped forward.
		5. Chair reviewed IEEE copyright policy, – no clarification requested
		6. Chair reviewed IEEE code of ethics and WG participation as an individual professional. – no clarification requested
		7. Chair reviewed IEEE 802 ground rules
		8. Recorded Participation requirement
		Headcount: ~60 present
	4. Agenda
		1. Submissions:
			1. 11-20-1863 Seure LTFs: additional Design details (Steve Shellhammer) – 90 minutes
			2. 11-20-1951-00-00az-Discussion Frequency and Time Domain Attack (Christian Berger) – as time permits
		2. Review submission pipeine
		3. Review Telecon Schedule
	5. Steve Shellhammer presented 11-20-1963
		1. Title: Seure LTFs additional Desing Details
		2. Q: are all sptial streams rotated with the same angle R: there is a different phase per each steram as in slide 9.
		3. Q: for one spatial stream? R: no change between repetitios, the per stream rotation is not needed because unintentional BF is not a problem
		4. Q: if you rotate the between stream doesn’t that cancel the other rotation. R: in each repetition it the phase. Q: is there a 1/16 probablity to get a null. R: there is some chance. Q: avoiding a repeat allows the attacker to predict or increase the chance. R: all the sequences that generate the phase shifts and modulation are random and cannot be predicted.
		5. Q: A null may destroy a repetition, which in some cases will cause loosing the packet/measurement because in some cases all repetition may need to be received. R: in most cases the dynamic range allows you to receive sequence, and the method should allow for loosing one sequence.
		6. StrawPoll (slide 25) – discussion on strawpoll
		7. Q: I would like more time to review and reach Concensus: R: I would like to go through it today.
		8. Q: Generaly this is good work. I would also support deferring the question until other presentations are reviewed.
		9. Q: We are OK with SP, but we think the 4-psk is not needed. The complexity at the TX is too high.
		10. C: This is not new, we have presented most of that 4 months ago. We just add the 4-PSK to solve a security issue.
		11. **Strawpoll**:
		Slide 25 of submission on 11-20-1863r0
		**Results**: (Y/N/A) (67/28/4)
		12. I would like time to have the other presenation (two voices)
		13. Steve: I would like to have more time to break it down.
		14. **Strawpoll**Modified straw poll in slide 93 of 11-20-1570r17
		**Results**: 63/28/2
		15. Q: what would convice the 28 who were against: R: We don’t want any modualtio that is not part of what we already have. Securiyt should not be that important. R: Some people want more security.
		16. Chair: please continue the discussion offline
	6. Submission pipeline: 11-20-1951
	7. Telecon schedule Dec 16th, Jan 6th
	8. AOB?
	9. Adjourned at 11:57PDT.
	10. Attendance:

|  |  |  |  |
| --- | --- | --- | --- |
| TGaz | 12/9 | Adhikari, Shubhodeep | Broadcom Corporation |
| TGaz | 12/9 | Akhmetov, Dmitry | Intel Corporation |
| TGaz | 12/9 | Anwyl, Gary | MediaTek Inc. |
| TGaz | 12/9 | Asterjadhi, Alfred | Qualcomm Incorporated |
| TGaz | 12/9 | Awater, Geert | Qualcomm Incorporated |
| TGaz | 12/9 | B, Hari Ram | NXP Semiconductors |
| TGaz | 12/9 | Bahn, Christy | IEEE STAFF |
| TGaz | 12/9 | Baik, Eugene | Qualcomm Incorporated |
| TGaz | 12/9 | Batra, Anuj | Apple, Inc. |
| TGaz | 12/9 | Batra, Arun | Broadcom Corporation |
| TGaz | 12/9 | Bei, Jianwei | NXP Semiconductors |
| TGaz | 12/9 | Berger, Christian | NXP Semiconductors |
| TGaz | 12/9 | Bhandaru, Nehru | Broadcom Corporation |
| TGaz | 12/9 | Bravo, Daniel | Intel Corporation |
| TGaz | 12/9 | Cao, Rui | NXP Semiconductors |
| TGaz | 12/9 | Cepni, Gurkan | Apple, Inc. |
| TGaz | 12/9 | Cheng, Xilin | NXP Semiconductors |
| TGaz | 12/9 | Dash, Debashis | Apple, Inc. |
| TGaz | 12/9 | da Silva, Claudio | Intel Corporation |
| TGaz | 12/9 | Dave, Brajesh | Apple, Inc. |
| TGaz | 12/9 | de Vegt, Rolf | Qualcomm Incorporated |
| TGaz | 12/9 | DOAN, DUNG | Qualcomm Incorporated |
| TGaz | 12/9 | Erceg, Vinko | Broadcom Corporation |
| TGaz | 12/9 | Garg, Lalit | Broadcom Corporation |
| TGaz | 12/9 | Ghaderipoor, Alireza | MediaTek Inc. |
| TGaz | 12/9 | Grandhe, Niranjan | NXP Semiconductors |
| TGaz | 12/9 | Henry, Jerome | Cisco Systems, Inc. |
| TGaz | 12/9 | jiang, feng | Apple, Inc. |
| TGaz | 12/9 | Jiang, Jinjing | Apple, Inc. |
| TGaz | 12/9 | Jones, Vincent Knowles IV | Qualcomm Incorporated |
| TGaz | 12/9 | Kadampot, Ishaque Ashar | Qualcomm Incorporated |
| TGaz | 12/9 | Kakani, Naveen | Qualcomm Incorporated |
| TGaz | 12/9 | Kang, Sugbong | Apple, Inc. |
| TGaz | 12/9 | Kasher, Assaf | Qualcomm Incorporated |
| TGaz | 12/9 | Kneckt, Jarkko | Apple, Inc. |
| TGaz | 12/9 | Kumar, Manish | Marvell Semiconductor, Inc. |
| TGaz | 12/9 | Kwon, Young Hoon | NXP Semiconductors |
| TGaz | 12/9 | Latif, Imran | Apple, Inc. |
| TGaz | 12/9 | Li, Jialing | Qualcomm Incorporated |
| TGaz | 12/9 | Lindskog, Erik | SAMSUNG |
| TGaz | 12/9 | Liu, Ying | NXP Semiconductors |
| TGaz | 12/9 | Lou, Hui-Ling | NXP Semiconductors |
| TGaz | 12/9 | Ma, Li | MediaTek Inc. |
| TGaz | 12/9 | Mohanty, Bibhu | Qualcomm Incorporated |
| TGaz | 12/9 | Montreuil, Leo | Broadcom Corporation |
| TGaz | 12/9 | Nam, Junyoung | Qualcomm Incorporated |
| TGaz | 12/9 | NANDAGOPALAN, SAI SHANKAR | Cypress Semiconductor Corporation |
| TGaz | 12/9 | Nurani Krishnan, Neelakantan | Qualcomm Incorporated |
| TGaz | 12/9 | Palm, Stephen | Broadcom Corporation |
| TGaz | 12/9 | Pare, Thomas | MediaTek Inc. |
| TGaz | 12/9 | Patil, Abhishek | Qualcomm Incorporated |
| TGaz | 12/9 | Petry, Brian | Broadcom Corporation |
| TGaz | 12/9 | Puducheri, Srinath | Broadcom Corporation |
| TGaz | 12/9 | Qi, Emily | Intel Corporation |
| TGaz | 12/9 | Raissinia, Alireza | Qualcomm Incorporated |
| TGaz | 12/9 | Reshef, Ehud | Intel Corporation |
| TGaz | 12/9 | Rosdahl, Jon | Qualcomm Technologies, Inc. |
| TGaz | 12/9 | Sandhu, Shivraj | Qualcomm Incorporated |
| TGaz | 12/9 | Segev, Jonathan | Intel Corporation |
| TGaz | 12/9 | Shah, Tushar | Apple, Inc. |
| TGaz | 12/9 | Shellhammer, Stephen | Qualcomm Incorporated |
| TGaz | 12/9 | Shor, Gadi | Intel Corporation |
| TGaz | 12/9 | Sosack, Robert | Molex Incorporated |
| TGaz | 12/9 | Srinivasa, Sudhir | NXP Semiconductors |
| TGaz | 12/9 | Srinivasan, Shree Raman | Qualcomm Incorporated |
| TGaz | 12/9 | Stacey, Robert | Intel Corporation |
| TGaz | 12/9 | Strauch, Paul | Qualcomm Incorporated |
| TGaz | 12/9 | Sun, Yanjun | Qualcomm Incorporated |
| TGaz | 12/9 | Thakur, Sidharth | Apple, Inc. |
| TGaz | 12/9 | Tian, Bin | Qualcomm Incorporated |
| TGaz | 12/9 | Trainin, Solomon | Qualcomm Incorporated |
| TGaz | 12/9 | Verma, Lochan | Apple, Inc. |
| TGaz | 12/9 | Verma, Sindhu | Broadcom Corporation |
| TGaz | 12/9 | Vermani, Sameer | Qualcomm Incorporated |
| TGaz | 12/9 | Wang, Chao Chun | MediaTek Inc. |
| TGaz | 12/9 | Wang, Qi | Apple, Inc. |
| TGaz | 12/9 | Wang, Yi-Hsiu | Zeku |
| TGaz | 12/9 | Want, Roy | Google |
| TGaz | 12/9 | Wentink, Menzo | Qualcomm |
| TGaz | 12/9 | Wu, Kanke | Qualcomm Incorporated |
| TGaz | 12/9 | Wu, Tianyu | Apple, Inc. |
| TGaz | 12/9 | Yang, Lin | Qualcomm Incorporated |
| TGaz | 12/9 | Yee, Peter | NSA-CSD |
| TGaz | 12/9 | Yong, Su Khiong | Apple, Inc. |
| TGaz | 12/9 | Young, Christopher | Broadcom Corporation |
| TGaz | 12/9 | Yu, Mao | NXP Semiconductors |
| TGaz | 12/9 | Zeng, Ruochen | NXP Semiconductors |
| TGaz | 12/9 | Zhang, Hongyuan | Marvell Semiconductor, Inc. |
| TGaz | 12/9 | Zhang, Yan | NXP Semiconductors |
| TGaz | 12/9 | Zou, Tristan | Qualcomm Incorporated |

1. **TGaz – December 9th d 2020**
	1. Called to order by TGaz Chair, Jonathan Segev (Intel Corporation) and Vice Chair and secretary (active), Assaf Kasher (Qualcomm), at **10:02am PDT,**
	2. Agenda Doc. **IEEE 802.11-20/01570r16 (in progress - slide 31)**
	3. Review Patent Policy and logistics
		1. Chair reviewed the IEEE-SA Patent Policy, duty to inform, the guideline for IEEE WG meetings and logistics – no clarifications requested.
		2. Chair called for any potentially essential patents, no one stepped forward.
		3. Chair reminded participants to register their attendance using imat.
		4. Chair reviewed other guidelines for IEEE meetings, asked if any clarifications are requested, no one stepped forward.
		5. Chair reviewed IEEE copyright policy, – no clarification requested
		6. Chair reviewed IEEE code of ethics and WG participation as an individual professional. – no clarification requested
		7. Chair reviewed IEEE 802 ground rules
		8. Recorded Participation requirement
		Headcount: ~60 present
	4. Agenda
		1. Submissions:
		2. 11-20-1951- Discussion Frequency and Time Domain Attack - (Christian Berger) – 45min
		3. 11-20-1956 - Ranging PHY Security (Erik Lindskog) – 40 min
		4. 11-20-1863 - Secure LTF Additional Design details (Steve Shellhammer) –20 min follow up/as time permits.
		5. 11-20-1959 - Tx FD Window Design for Secure LTF (Anuj Batra) – as time permits
	5. Christian Berger Presented 11-20-1951
		1. Title: Discussion Frequency and Time Domain Attack
	6. Erik Lindskog Presented 11-20-1956
		1. Title: Ranging PHY Security
	7. Steve Shellhammer Presented 11-20-1863
		1. Secure LTF Additional Design details – followup and strawpoll
		2. **Strawpoll
		*Do you agree to replace the existing 802.11az secure LTF design parameters with the following changes***Using secure pseudo random 64QAM modulation
		***Security LTF value is pseudo randomized per tone and per OFDM symbol and is the same across all streams***Using AES-128 Counter (CTR) Mode as a pseudo random bit generator for the sounding NDP sequence
		***A 256-bit sequence from KDF is used to initialize AES128-CTR by using the first 128 bits as the Key and second 128 bits as IV, at the beginning of the NDP***Using per-stream phase rotation which is updated every secure LTF Repetition
		***Per-stream phase rotation angles are the same for all the tones and all the LTFs in one repetition
		Pseudo random phase rotation is generated at the beginning of the NDP using bits from the AES-128 Counter Mode
		An additional deterministic per-stream phase rotation is applied in each Repetition*
		Results (50/1/5)**
	8. Anuj Batra Presented 11-20-1959
		1. Title: Tx FD Window Design for Secure LTF
	9. Review Future Telecons
	10. AOB
	11. Attendance