ResCTC: Resilience in Wireless Networks through Cross-Technology Communication

Anatolij Zubow, Isabel von Stebut, Sascha Rösler and Falko Dressler
School of Electrical Engineering and Computer Science, TU Berlin, Germany
{zubow,roesler,dressler}@ccs-labs.org

***Abstract*—Resilient wireless networks ensure that the network maintains functionality despite adverse conditions like hardware and software failures, adversarial jamming attacks, or environmental changes like wireless channel fading which can disrupt connectivity. We show that Cross-Technology Communication (CTC), which was developed to enable direct communication between otherwise incompatible radio technologies, can be utilized to improve the resilience in wireless networks. This is achieved by increasing the number of independent wireless links between adjacent wireless nodes as well as by the increase in communication distance resulting in increased path diversity. Results from our analysis reveal that the same level of resilience can be achieved with reduced number of radio interfaces per node while tolerating an order of magnitude higher node failure rate. Moreover, such CTC-enabled networks are more resilient to advanced technology-specific jamming attacks.**

I. Introduction

In our increasingly interconnected world, the demand for wireless networks that go beyond mere connectivity has never been more pressing [1]. Resilient wireless networks are the cornerstone of our modern society's critical infrastructure, supporting everything from healthcare systems and emergency services to industrial automation and smart cities [2]. These networks must withstand unpredictable challenges, from natural disasters to deliberate attacks, while maintaining uninterrupted connectivity and reliability. The objectives for resilient and ultra-reliable wireless networking are centered around ensuring continuous, dependable, and robust connectivity in various scenarios, especially in mission-critical applications like industrial automation, healthcare, or emergency services. Resilience means ensuring the network maintains functional despite adverse conditions like hardware and software failures, adversarial jamming attacks, or environmental changes like wireless channel fading which can disrupt connectivity [3].

In this paper we show that the possibilities of Cross-Technology Communication (CTC) can be utilized in order to make wireless networks more resilient. With CTC it is possible to directly communicate between otherwise incompatible radio technologies by means of waveform emulation, e.g., CTC between WiFi and LoRa [4], WiFi and Bluetooth (BT) [5], and WiFi and ZigBee [6]. As an example Fig. 1 shows a CTC-enabled IoT showcase. Here a node *SRC*, e.g., smartphone with only support for WiFi technology, requires the help from a multi-technology gateway (*MTGW*) for communication with a node *DST*, e.g., door handle supporting only Bluetooth low energy (BTLE). Here the *MTGW* translates between the two wireless technologies, i.e., from WiFi to BTLE and vice versa. The resilience of such a communication network is highly affected by the robustness of the *MTGW* as the failure of the node itself or any of its two wireless interfaces results in communication outage. In addition, channel fading and jamming attacks on the wireless communication channel (WiFi or BTLE), may disrupt connectivity. However, the resilience of our network can be dramatically increased by utilizing CTC to create an additional direct communication link between the *SRC* and *DST* nodes bypassing the *MTGW* node in case of node or interface failures. Moreover, an attack from a technology-specific jammer, here on the WiFi communication, can be circumvent. Finally, the additional link diversity helps to counter outage due to channel fading and attenuation.

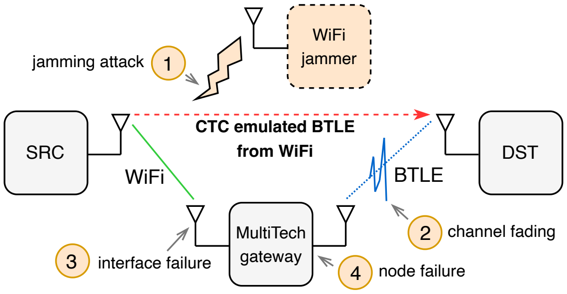


Figure 1. IoT showcase with communication over multi-technology gateway translating from WiFi to Bluetooth low energy (BTLE) technology.

Contributions: We show for the first time that the degrees of freedom provided by CTC can be utilized to improve the resilience in wireless networks. We present closed-form solutions for the end-to-end success probability taking into account node and interface failures as well as outage due to channel fading and malicious jamming attacks. Results from analysis in single hop as well multi-hop networks reveal that the same level of resilience can be achieved with less number of interfaces per node. Moreover, we show how CTC-enabled transmissions can be made resilient to advanced technology-specific jamming attacks.

II. Background

A. Cross-Technology Communication

CTC enables direct communication among heterogeneous devices having different incompatible wireless standards, e.g., WiFi with LoRa [7]. Existing CTC techniques can be divided into the packet-level CTC and the physical-level CTC. The packet-level CTC utilizes the packet transmission as the carrier to convey messages to the receiver of another technology. More sophisticated approaches do PHY-level CTC where the waveform of the target technology is emulated. Such signal emulation technique was introduced in a pioneering CTC scheme called WEBee [6], which enabled a WiFi device to transmit a ZigBee waveform by proper selection of its frame payload bits. It operated with the native data rates of ZigBee but suffered from a high packet error rate due to the inherent distortions of the emulated signal. TwinBee [8] and WIDE [9] further improve the quality of signal emulation and hence the reliability of WEBee. Later, the signal emulation enabled CTC between WiFi and BT [5], WiFi and LTE [10], [11]. In [4], we showed that the Complementary Code Keying (CCK)-based modulator of 802.11b WiFi can be used as a PWM generator, that can generate a valid LoRa waveform. Li et al. [12] showed that with CCK-based signal leaves some unique signatures when it flows into the BLE receiver. The authors proposed a technique called symbol transition mapping to convey data between WiFi and BLE. Finally, there are cases where a CTC between a narrow-band technology, e.g., LoRa, and a wideband-technology, e.g., WiFi, needs to be established. A technique termed signal recovery is used on the receiver side to reconstruct the narrow-band transmission.

B. Jamming Resilient CTC

There is a rich body of literature on wireless jamming [13]. Basically it can be said that the more an attacking jammer knows about the victim, the more successful he is. This is because he listens (senses) for victim's transmissions and selectively jam in both time and frequency dimension on detection [14]. The sensing component of such a selective jammer is technology-specific as it has to know some characteristic signal emitted by the victim, e.g., well known PHY preamble.

Although a large number of CTC approaches was developed, they all share the same disadvantages regardless of their designs (physical-level or packet-level CTC). They are very sensitive to technology-specific jamming attacks. This is because some parts of the underlying (native) technology like PHY preamble, header, OFDM pilots, cyclic prefix cannot be modified. So taking the example of Wi-Lo [4], where the LoRa waveform is emulated from a WiFi transmission, there is still a valid WiFi frame that is transmitted with an 802.11b compliant PHY preamble and header. Such a signature can be easily detected and jammed with technology-specific sensing targeting WiFi transmissions. Hence, such a LoRa emulated transmission will be prone to both a WiFi and a LoRa specific jammer.

In order to make CTC emulated transmissions robust against jamming of the underlying technology we propose the following approach (Fig. 2). Our key idea is to send the immutable parts of the underlying technology like physical layer preamble and header at extreme low transmission power while the variable part of the frame used for the actual emulation with high power. This would make the signal detection of a technology-specific jammer much more difficult. From a practical point of view, a fine-grained power control would be needed.

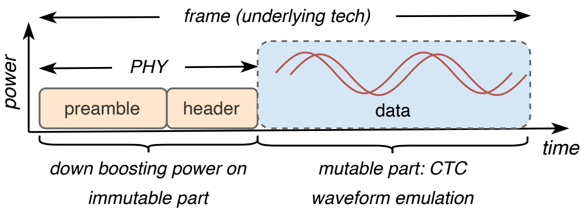


Figure 2. Making CTC resilient to technology-specific jamming by down boosting the TX power on the immutable part of the underlying technology.

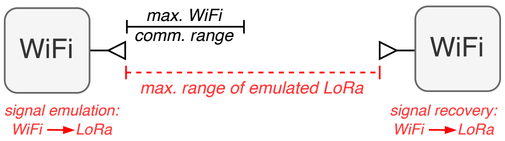


Figure 3. Enabling long-range comm with CTC.

C. CTC for Long-Range Communication

There is another advantage of CTC. CTC can be utilized to enable long range communication (Fig. 3). The limited communication range of the native technology, here WiFi, can be overcome by transmission of an emulated LoRa waveform from the WiFi transmitter which is received by a WiFi node from which the LoRa signal is recovered and its payload demodulated [4]. Based on literature, Fig. 4 shows the minimum sensitivity of different radio technologies from the 2.4 GHz ISM band together with the corresponding data rates. Here we see that both parameters are highly correlated and that we can trade data rate for increased sensitivity and distance. This is very beneficial as it increases the node degree, i.e., the number of neighboring nodes increases, making the network more resilient to node/interface/link failures.

III. Problem Statement

In this section, we first highlight the main system assumptions we use in our analysis. Then we present our system model together with the strategies under investigation.

A. Failure Models

The following issues affect the resilience, i.e., end-to-end (E2E) success probability, of a communication network:

- Node failures, e.g., hardware or software malfunction,
- Interface failures, i.e., outage of a network interface card due to hardware or software failure (failed driver updates),
- Link outage due to wireless channel fading,
- Link failure due to technology-specific jamming attacks.

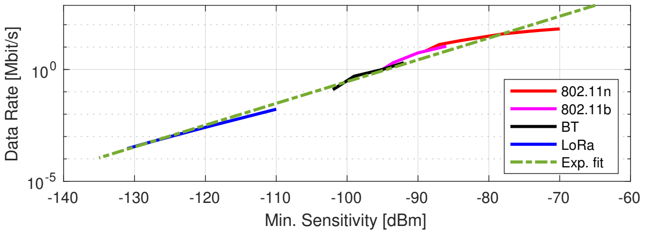


Figure 4. Min. sensitivity vs. data rate for selected radio technologies in 2.4 GHz ISM band with exponential fit: $f(x) = 10^{0.1x+9.2}$.

All four types of errors are modeled as stochastic processes for which we made the following assumptions:

- Node failures are independent,
- Interface failures due to hardware malfunction are independent but software-related failures are dependent,
- Link failures due to channel fading are independent,
- Link disruptions due to jamming attacks are dependent if same link technology is being used.

First, the network nodes themselves can fail with a probability of p_n, preventing any communication to and from that node. For interfaces, we consider both hardware and software failures. We assume interface hardware failures to be independent of each other, since faults like defective electronics in one interface usually do not impact any other interface. The probability for such a failure is p_h. In contrast, we model software-based interface failures to be dependent on the same node as long as the same technology is being used. This is because a faulty software driver update would make all associated interfaces unusable, e.g., failed WiFi driver makes all WiFi interfaces unusable. If no other interface of the same technology has failed due to software-related issues, the probability for failure is p_s. However, as soon as one interface fails, all other interfaces of the same technology have a higher error probability of $p_{s,c}$.

Similarly, link outage, due to channel fading and technology-specific jamming, is modeled as independent and dependent, respectively. For channel fading, it is reasonable to assume that the outage of two links is uncorrelated as they are sufficiently physically separated. So the probability is p_f. In contrast, technology-specific jamming is modeled as dependent if the same wireless technology is being used. This is because such a jammer is able to recognize the transmission using signal patterns from physical layer preamble or pilots. Hence, as soon as the jammer is able to successfully jam a particular link with p_j, all other links of the same technology have a higher jamming probability of $p_{j,c}$.

For our communication system to be not in outage, the following must be fulfilled. First, there exists at least one working path from source to destination node. Second, for each hop along that path at least one interface pair as well as the corresponding link has to be functional.

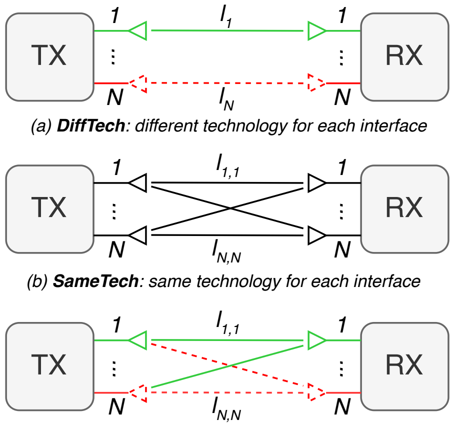
B. Network Model

We consider a wireless network with N devices (nodes). Each device is equipped with K wireless interfaces. We assume the existence of K-many different wireless technologies. Each interface uses a specific wireless technology. We consider two network topologies. First, a *single-hop* scenario with $N = 2$ devices being in direct wireless communication range regardless of the used wireless technology. Second, a *multi-hop* scenario where the $N > 2$ nodes are arranged in a string topology with the first and last nodes being source and destination.

C. Approaches under Study

We will study the following three approaches (Fig .5):

- *DiffTech*: each interface uses a different wireless technology resulting in K links between adjacent nodes;



(a) ***DiffTech**: different technology for each interface*

(b) ***SameTech**: same technology for each interface*

(c) ***FullCTC**: different technology for each interface*

Figure 5. Approaches under study: baselines (a+b) vs. proposed approach (c).

- *SameTech*: all K interfaces use the same wireless technology resulting in K^2-many links between adjacent nodes;
- *FullCTC*: each interface uses a different wireless technology but emulation via CTC of any of the K technologies is possible. The total number of links is K^2.

Note, the difference between the three approaches w.r.t. link failures. In case of channel fading and absence of jamming attacks, the approaches *SameTech* and *FullCTC* offer the highest resilience due to the larger number of links, i.e., K^2 instead of just K for *DiffTech*. However, under intense jamming attacks *DiffTech* as well as *FullCTC* are more resilient than *SameTech* due to our assumption that failures due to jamming are dependent in case the same wireless technology is being used. Hence, in an environment with both channel fading and jamming attacks our proposed *FullCTC* approach is expected to achieve a higher level of resilience, i.e., higher E2E success rate (SR).

D. Analytical Solution

In this section, we present closed-form solutions of the end-to-end success rate for the three approaches under study. All the used terms are summarized in Table I.

1) Difftech: The E2E SR $p_\mathrm{sr}^\mathrm{dt}$ for *DiffTech* is computed as:

$$p_\mathrm{sr}^\mathrm{dt} = (1-p_n)^2 \cdot \Big(1 - \big(1 - (1-p_h)^2 (1-p_s)^2 (1-p_f)\,(1-p_j)\big)^K\Big) \quad (1)$$

2) SameTech: E2E SR $p_\mathrm{sr}^\mathrm{st}$ for *SameTech* is computed as:

$$p_\mathrm{sr}^\mathrm{st} = (1-p_n)^2 \Big(1 - \Big(\sum_{n=0}^{K}\sum_{m=0}^{K} P_\mathrm{st}(X_n) P_\mathrm{st}(Y_m) P(Z_0|X_n \cap Y_m)\Big)\Big) \quad (2)$$

where $P_\mathrm{st}(X_k)$ is the probability of k failure-free interfaces at one node, $P_\mathrm{st}(X_{k,s})$ is the probability of k free of software failure interfaces at one node, $P(Z_0|X_n \cap Y_m)$ the probability of all links jammed or faded conditional n failure-free interfaces at the transmitter and m failure-free interfaces at the receiver and $P(Z_{l,j}|X_n \cap Y_m)$ is the probability of l no jammed links:

$$P_\mathrm{st}(X_k) = \sum_{i=k}^{K} {p_h}^{i-k} (1-p_h)^k P_\mathrm{st}(X_{i,s}) \binom{i}{k} \quad (3)$$

$$P_\mathrm{st}(X_{k,s}) = \begin{cases} (1-p_s)^K, & k = K \\ \sum_{i=k}^{K-1} {p_s}^{K-i} (1-p_s)^i \binom{K}{i} {\tilde{p_s}}^{i-k} (1-\tilde{p_s})^k \binom{i}{k}, & k \neq K \end{cases} \quad (4)$$

Table I
TERMS IN EQUATIONS

p_n	probability of node failure
p_h	probability of interface hardware failure
p_s	probability of interface software failure given no other interface has a software failure
$p_{s,c}$	probability of interface software failure given another interface has a software failure
p_f	probability of a link is faded
p_j	probability of a link is jammed given no other link of same technology is jammed
$p_{j,c}$	probability of a link is jammed given another link of same technology is jammed
K	number of installed interfaces on each node
L	number of links
n	number of fault free interfaces on TX
m	number of fault free interfaces on RX
l	links without fault
X_n	n interfaces are without fault on TX
Y_m	m interfaces are without fault on RX
Z_l	l links are not broken

$$P(Z_l|X_n \cap Y_m, L = nm) = \sum_{i=l}^{L} {p_f}^{i-l}(1-p_f)^l P(Z_{i,j}|L)\binom{i}{l} \tag{5}$$

$$P(Z_{l,j}|X_n \cap Y_m, L = nm) = \begin{cases} (1-p_j)^L, & l = L \\ \sum_{i=l}^{L-1} {p_j}^{L-i}(1-p_j)^i\binom{L}{i}{\tilde{p_j}}^{i-l}(1-\tilde{p_j})^l\binom{i}{l}, & l \neq L \end{cases} \tag{6}$$

using the probabilities

$$\tilde{p_s} = \frac{p_{s,c} - p_s}{1 - p_s} \tag{7}$$

$$\tilde{p_j} = \frac{p_{j,c} - p_j}{1 - p_j} \tag{8}$$

3) FullCTC: Finally, the E2E SR $p_{\mathrm{sr}}^{\mathrm{fc}}$ for our proposed *FullCTC* is computed as:

$$p_{\mathrm{sr}}^{\mathrm{fc}} = (1-p_n)^2\Bigg(1 - \bigg(P_{\mathrm{fc}}(Y_0) + \sum_{m=1}^{K} P_{\mathrm{fc}}(Y_m)\cdot\big(p_s + p_h - p_s p_h \\ + (1-p_s)\,(1-p_h)p_{\mathrm{fc}}(Z_0|X_1 \cap Y_m)\big)^K\bigg)\Bigg) \tag{9}$$

with the probability of k failure-free interfaces at one node $P_{\mathrm{fc}}(X_k)$

$$p_{\mathrm{fc}}(X_k) = \sum_{i=k}^{K} {p_s}^{K-i}(1-p_s)^i {p_h}^{i-k}(1-p_h)^k\binom{K}{i}\binom{i}{k} \tag{10}$$

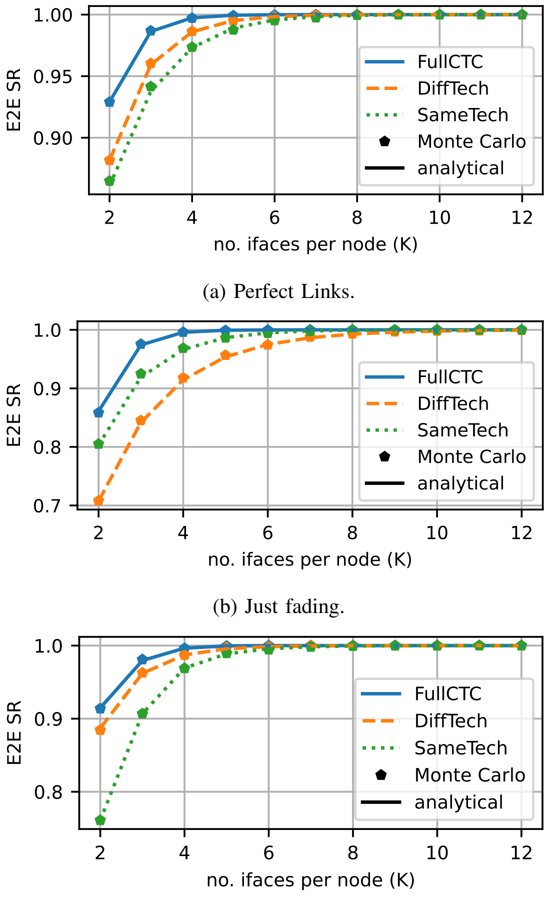
and the other probabilities as defined for the derived equations for *SameTech* (§III-D2).

IV. EVALUATION

We evaluated the different approaches in two scenarios. First, a *single-hop* scenario with source and destination nodes in direct wireless communication range to analyze the impact of interface and channel failures as well as from jamming. Second, a *multi-hop* scenario to investigate the impact from node failures.

A. Single-Hop Scenario

We consider a *single-hop* scenario with source and destination nodes in direct wireless communication range (regardless of the used wireless technology). Both the source and destination nodes are equipped with K interfaces.



(a) Perfect Links.

(b) Just fading.

(c) Fading + Jamming.

Figure 6. Performance in single-hop scenario.

1) Perfect Links: We start with an analysis with completely reliable wireless links, i.e., no fading ($p_f = 0$) and absence of jamming attacks, i.e., ($p_j = 0$). However, we consider the possibility that the interfaces might fail due to hardware or software failures, i.e., $p_h = 0.1$, $p_s = 0.1$, $p_{s,c} = 0.3$. Note the correlation of software failures.

The results are shown in Fig. 6a together with the curves from our analytic evaluation. We see that *FullCTC* is able to achieve an E2E SR of > 0.999 with much lower number of interfaces, i.e., 3 instead of 5 when compared with *DiffTech*. *SameTech* performs worst and requires 6 interfaces. This can be justified by the fact that *SameTech* suffers the most from interface software failures due to the use of same wireless technology on each interface.

2) Just Fading: Next, we consider a scenario with channel fading ($p_f = 0.3$) but no jamming ($p_j = 0$). The remaining parameter were set to: $p_h = 0.1$, $p_s = 0.1$, $p_{s,c} = 0.3$.

The results are shown in Fig. 6b. We see that *FullCTC* is able to achieve an E2E SR of > 0.999 with much less number of interfaces, i.e., 3 instead of 5 when using *SameTech*. The *DiffTech* performs worst and requires 3× more interfaces to achieve the same level of resilience as *FullCTC*. This is because both *SameTech* and *FullCTC* have a much larger number of available wireless links, i.e., K^2 instead of just K, which makes those approaches much more resilient to channel fading.

3) Fading & Jamming: Finally, we consider a scenario with both channel fading ($p_f = 0.1$) and active jamming attacks ($p_j = 0.2, p_{j,c} = 0.7$). Note that the jamming is highly correlated. Therefore, a successful attack on a link that uses a particular technology will most likely disrupt other links that use the same technology. The other parameters were set to $p_h = 0.01$, $p_s = 0.03$, $p_{s,c} = 0.3$.

The results are shown in Fig. 6c. Again, *FullCTC* offers the highest resilience. To achieve an E2E SR of > 0.999 it requires only 3 interfaces whereas the other two approaches need 5 and 6 respectively.

Takeaway: Our proposed *FullCTC* outperforms the other two approaches in all three scenarios. On average, it requires half of the number of interfaces to achieve the same level of resilience.

B. Multi-Hop Scenario

Next, we analyze the advantage of *FullCTC* in a multi-hop scenario. Therefore, we consider a scenario with 19 nodes arranged in a string topology and inter-node distance of 30 m with the source and destination nodes being the outer left and outer right nodes respectively. To consider the influence of node outage p_n on the E2E SR in isolation, we assumed fully reliable interfaces and a perfect channel without fading and jaming. In addition, we assumed the source and destination nodes to be reliable as well, i.e., p_n affected only intermediate nodes. As *Baseline*, we configured the nodes to operate in 802.11n WiFi mode with the sensitivity and data rate values as shown in Fig. 4. Since WiFi only allows short range communication the *Baseline* resulted in 18 hops from source to destination. Hence even a single node failure results in outage, i.e., SR=0.

We compare the baseline with two versions of our proposed approach. In *FullCTC*, we assume that the emulation of the technologies WiFi 802.11b, Bluetooth (BT) and LoRa is perfectly possible without any data rate loss. This results in much higher node degree because of the increased sensitivity and communication range of those technologies (Fig. 3) as compared to 802.11n and hence multiple paths from source to destination node. Because of this path diversity the outage of a single node no longer results in a broken connection. Results for an optimal solution termed as *FullCTC**. Here, we assume that for each receive sensitivity there exists some wireless technology with some data rate according to our curve fit in Fig. 4. As consequence, even for two very far apart nodes, there is always a link but with possibly very low data rate. Hence, *FullCTC** offers the highest node degree and path diversity.

The results are shown in Fig. 7. Looking at the E2E SR first, we can observe the significant improvement for *FullCTC* and *FullCTC** as compared to *Baseline*. When considering a target E2E SR of 0.5 the maximum possible node outage for *Baseline* is just 0.04 as compared to 0.4 and 0.76 for *FullCTC* and *FullCTC**, respectively. For a higher target E2E SR of 0.99 p_n must be nearly zero, whereas *FullCTC* can tolerate a node outage of up to 0.09. The reason for the improved resilience is due to the much higher node degree, i.e., the number of wireless links is 2.8/5.8× larger in *FullCTC/FullCTC** case as compared to *Baseline*, hence increasing the path diversity by that factor. However, the increased resilience comes at the price of a lower data rate. Fig. 7 also shows the average E2E data rate computed over the network configurations being not in outage. For *FullCTC/FullCTC** we can observe a graceful degradation of data rate with an increase in p_n.

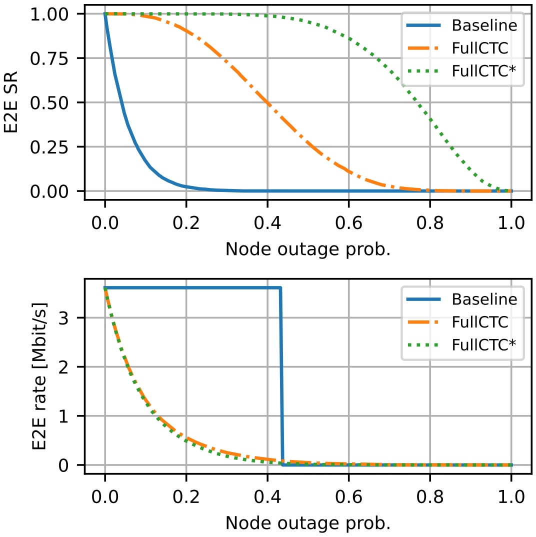


Figure 7. Performance in multi-hop scenario.

Takeaway: Our *FullCTC* approach increases the node degree and hence the path diversity resulting in an order of magnitude higher resilience to node failures as compared to baseline.

V. Related Work

Related work falls into four categories:

Diversity in Communication Technologies: Employing diverse communication technologies (e.g., multi-radio systems, multi-path routing) to enhance reliability and resilience. Nielsen et al. [15] proposed to utilize interface diversity and integrate multiple communication interfaces, each interface based on a different technology. By means of coding the payload and redundancy data is distributed across multiple available communication interfaces. In their analysis they also consider failure correlation among interfaces and technologies. Instead of considering the connectivity between adjacent nodes jamming can be also addressed at the network-level [16]. Here it is possible to restore the end-to-end data delivery through multi-path routing. As long as all paths do not fail concurrently, the end-to-end path availability is maintained. Pu [17] proposed a jamming-resilient multi-path routing for flying ad-hoc networks. In addition to multi-path routing, Cai et al. [18] introduced load balancing to handle multiple disaster zones.

Redundancy and Reliability Protocols: The objective is to jointly implement redundancy and reliability protocols such as Hybrid Automatic Repeat reQuest (HARQ) to mitigate packet loss and ensure data integrity. Khosravirad et al. [19] proposed a transmission scheme that performs channel-aware rate adaptation, link scheduling and also exploits multi-user diversity through cooperation on demand. Swamy et al. [20]

proposed the usage of network coding in conjunction with cooperative communication techniques. With CLARQ, Han et al. [21] introduced a closed loop ARQ for high reliability. They use reallocation of resources in a TDMA scheme to improve the resilience against Rayleigh fading.

Advanced Antenna Technologies: The usage of (massive) multiple antennas (MIMO) is a significant contributor in achieving resilience as it enables to create high SNR, quasi-deterministic links being quasi-immune to fading and interference [22]. Akhlaghpasand et al. [23] showed how a MIMO system can be protected from jamming attacks. Do et al. [24] also uses optimal power distribution and RX filters based on jamming estimation. They exploit the high spatial resolution of missive MIMO systems.

Dynamic Spectrum Access: When operating in unlicensed bands, co-existence need to be assured as there may be other wireless systems working on the same bands resulting in cross-technology interference. Xu et al. [25] proposed to employ the basic idea of cognitive radio for dynamic interference-resistant multi-channel access. In particular a multi-channel listen before talk scheme with adaptive channel hopping is proposed. Wang et al. [26] proposed different anti-jamming methods based on cognitive radio technology where the wireless devices learn the dynamic and complex spectrum environment and obtain an optimal communication strategy. They consider both single-user and multiple-user (collaborative) strategies.

VI. Conclusion

In this paper we showed that the degrees of freedom provided by CTC can be utilized to improve the resilience in wireless networks. Specifically, there is an increase in the number of wireless links between adjacent nodes as well as the number of available paths in the network. Furthermore, we showed that CTC transmissions can be more robust against jamming. As future work, we plan a prototype using commodity hardware which would allow us to validate our approach under real channel and jamming conditions.

Acknowledgments

This work was supported by the Federal Ministry of Education and Research (BMBF, Germany) within the 6G Research and Innovation Cluster 6G-RIC under Grant 16KISK020K as well as by the German Research Foundation (DFG) within the projects Resilient Worlds under grant DR 639/30-1 and ZU 235/4-1.

References

[1] F. Dressler, “Physical Layer Resilience through Deep Learning in Software Radios: Technical Perspective,” *Communications of the ACM*, vol. 65, no. 9, pp. 82–82, Sep. 2022.

[2] Bundesnetzagentur, *Strategy paper, Resilience of telecommunications networks*, https://www.bundesnetzagentur.de/SharedDocs/Downloads/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Strategiepapier_Resilienz_eng.pdf, [Accessed 22-01-2024], 2022.

[3] Y. Zou, D. Yu, J. Yu, Y. Zhang, F. Dressler, and X. Cheng, “Distributed Byzantine-Resilient Multiple-Message Dissemination in Wireless Networks,” *IEEE/ACM Transactions on Networking*, vol. 29, no. 4, pp. 1662–1675, Aug. 2021.

[4] P. Gawłowicz, A. Zubow, and F. Dressler, “Wi-Lo: Emulation of LoRa using Commodity 802.11b WiFi Devices,” in *IEEE ICC 2022*, Seoul, South Korea: IEEE, May 2022, pp. 4414–4419.

[5] W. Jiang, Z. Yin, R. Liu, Z. Li, S. M. Kim, and T. He, “BlueBee: A 10,000x Faster Cross-Technology Communication via PHY Emulation,” in *ACM SenSys 2017*, Delft, Netherlands: ACM, Nov. 2017, pp. 1–13.

[6] Z. Li and T. He, “WEBee: Physical-Layer Cross-Technology Communication via Emulation,” in *ACM MobiCom 2017*, Snowbird, UT: ACM, Oct. 2017, pp. 2–14.

[7] Y. Chen, M. Li, P. Chen, and S. Xia, “Survey of cross-technology communication for IoT heterogeneous devices,” *IET Communications*, vol. 13, no. 12, pp. 1709–1720, Jul. 2019.

[8] Y. Chen, Z. Li, and T. He, “TwinBee: Reliable Physical-Layer Cross-Technology Communication with Symbol-Level Coding,” in *IEEE INFOCOM 2018*, Honolulu, HI: IEEE, Apr. 2018, pp. 153–161.

[9] X. Guo, Y. He, J. Zhang, and H. Jiang, “WIDE: Physical-level CTC via Digital Emulation,” in *ACM/IEEE IPSN 2019*, Montreal, Canada: ACM, Apr. 2019, pp. 49–60.

[10] P. Gawłowicz, A. Zubow, and A. Wolisz, “Enabling Cross-technology Communication between LTE Unlicensed and WiFi,” in *IEEE INFOCOM 2018*, Honolulu, HI: IEEE, Apr. 2018.

[11] P. Gawłowicz, A. Zubow, S. Bayhan, and A. Wolisz, “Punched Cards over the Air: Cross-Technology Communication Between LTE-U/LAA and WiFi,” in *IEEE WoWMoM 2020*, Virtual Conference: IEEE, Sep. 2020, pp. 297–306.

[12] L. Li, Y. Chen, and Z. Li, “WiBle: Physical-Layer Cross-Technology Communication with Symbol Transition Mapping,” in *IEEE SECON 2021*, Virtual Conference: IEEE, Jul. 2021, pp. 1–9.

[13] K. Grover, A. Lim, and Q. Yang, “Jamming and anti-jamming techniques in wireless networks: a survey,” *International Journal of Ad Hoc, Sensor & Ubiquitous Computing*, vol. 17, no. 4, pp. 197–215, Dec. 2014.

[14] A. Proaño and L. Lazos, “Selective Jamming Attacks in Wireless Networks,” in *IEEE ICC 2010*, Cape Town, South Africa: IEEE, May 2010.

[15] J. J. Nielsen, R. Liu, and P. Popovski, “Ultra-Reliable Low Latency Communication Using Interface Diversity,” *IEEE Transactions on Communications*, vol. 66, no. 3, pp. 1322–1334, Mar. 2018.

[16] H. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, “Jamming-Resilient Multipath Routing,” *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 852–864, Nov. 2012.

[17] C. Pu, “Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks,” *IEEE Access*, vol. 6, pp. 68 472–68 486, May 2018.

[18] S. Cai, F. Zhou, Z. Zhang, and A. Meddahi, “Disaster-Resilient Service Function Chain Embedding Based on Multi-Path Routing,” in *IEEE INFOCOM 2021, ICCN Workshop*, Vancouver, Canada: IEEE, May 2021, pp. 1–7.

[19] S. R. Khosravirad, H. Viswanathan, and W. Yu, “Exploiting Diversity for Ultra-Reliable and Low-Latency Wireless Control,” *IEEE Transactions on Wireless Communications*, vol. 20, no. 1, pp. 316–331, Jan. 2021.

[20] V. N. Swamy, P. Rigge, G. Ranade, A. Sahai, and B. Nikolić, “Network coding for high-reliability low-latency wireless control,” in *IEEE WCNC 2016*, Doha, Qatar: IEEE, Apr. 2016, pp. 1–7.

[21] B. Han, Y. Zhu, M. Sun, V. Sciancalepore, Y. Hu, and H. Schotten, “CLARQ: A Dynamic ARQ Solution for Ultra-High Closed-Loop Reliability,” *IEEE Transactions on Wireless Communications*, vol. 21, no. 1, pp. 280–294, Jan. 2022.

[22] P. Popovski, J. J. Nielsen, C. Stefanovic, et al., “Wireless Access for Ultra-Reliable Low-Latency Communication: Principles and Building Blocks,” *IEEE Network*, vol. 32, no. 2, pp. 16–23, Mar. 2018.

[23] H. Akhlaghpasand, E. Björnson, and S. M. Razavizadeh, “Jamming-Robust Uplink Transmission for Spatially Correlated Massive MIMO Systems,” *IEEE Transactions on Communications*, vol. 68, no. 6, pp. 3495–3504, Jun. 2020.

[24] T. T. Do, E. Björnson, E. G. Larsson, and S. M. Razavizadeh, “Jamming-Resistant Receivers for the Massive MIMO Uplink,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 210–223, Jan. 2018.

[25] C. Xu, P. Zeng, H. Yu, X. Jin, and C. Xia, “WIA-NR: Ultra-Reliable Low-Latency Communication for Industrial Wireless Control Networks over Unlicensed Bands,” *IEEE Network*, vol. 35, no. 1, pp. 258–265, Jan. 2021.

[26] X. Wang, J. Wang, Y. Xu, et al., “Dynamic Spectrum Anti-Jamming Communications: Challenges and Opportunities,” *IEEE Communications Magazine*, vol. 58, no. 2, pp. 79–85, Feb. 2020.