

# Synthetic Disinformation Attacks on Automated Fact Verification Systems

Yibing Du<sup>1\*</sup>, Antoine Bosselut<sup>2\*</sup>, Christopher D. Manning<sup>1</sup>

<sup>1</sup>Stanford University <sup>2</sup>EPFL  
 antoine.bosselut@epfl.ch, {yibingdu,manning}@stanford.edu

## Abstract

Automated fact-checking is a needed technology to curtail the spread of online misinformation. One current framework for such solutions proposes to verify claims by retrieving supporting or refuting evidence from related textual sources. However, the realistic use cases for fact-checkers will require verifying claims against evidence sources that could be affected by the same misinformation. Furthermore, the development of modern NLP tools that can produce coherent, fabricated content would allow malicious actors to systematically generate adversarial disinformation for fact-checkers.

In this work, we explore the sensitivity of automated fact-checkers to synthetic adversarial evidence in two simulated settings: ADVERSARIAL ADDITION, where we fabricate documents and add them to the evidence repository available to the fact-checking system, and ADVERSARIAL MODIFICATION, where existing evidence source documents in the repository are automatically altered. Our study across multiple models on three benchmarks demonstrates that these systems suffer significant performance drops against these attacks. Finally, we discuss the growing threat of modern NLG systems as generators of disinformation in the context of the challenges they pose to automated fact-checkers.

## Introduction

From QAnon’s deep state<sup>1</sup> to anti-vaccination campaigns (Germani and Biller-Andorno 2021), misinformation and disinformation have flourished in online ecosystems. As misinformation continues to induce harmful societal effects, factchecking online content has become critical to ensure trust in the information found online.<sup>2</sup> However, manual efforts to filter misinformation cannot keep pace with the scale of online information that must be reliably verified to avoid false claims spreading and affecting public opinion.<sup>3</sup> Consequently, new research in automated fact-checking explores designing systems that can rapidly validate political, medical, and other domain-specific claims made and shared online (Thorne and Vlachos 2018; Guo, Zhang, and Lu 2019).

\*These authors contributed equally.

Copyright © 2022, Association for the Advancement of Artificial Intelligence (www.aaai.org). All rights reserved.

<sup>1</sup><https://www.nytimes.com/article/what-is-qanon.html>

<sup>2</sup><https://nationalpress.org/topic/the-truth-about-fact-checking/>

<sup>3</sup><https://fivethirtyeight.com/features/why-twitters-fact-check-of-trump-might-not-be-enough-to-combat-misinformation/>

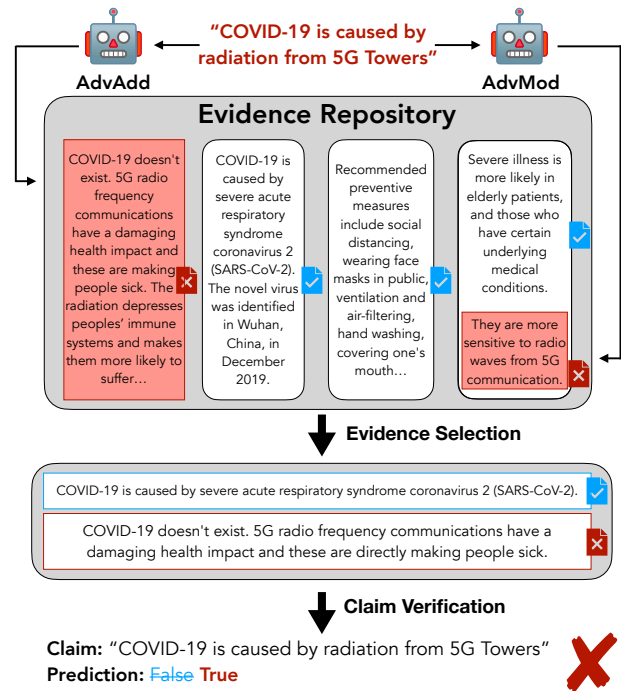


Figure 1: Outline of our two settings for adversarial injection of poisoned content into fact-checker evidence repositories.

A popular emergent paradigm in automated fact-checking, Fact Extraction and Verification (FEVER; Thorne et al. 2018), frames the problem as claim verification against a large repository of evidence documents. As one of the first large-scale datasets designed in this framework, FEVER was released with 185k annotated claims that could be verified against Wikipedia articles. When checking a claim, systems designed in this framework search for related documents in the database, and retrieve relevant supporting or refuting evidence from these sources. Then, these systems evaluate whether the retrieved evidence sentences validate or contradict the claim, or whether there is not enough information to make a judgment. More recently, the SCIFACT (Wadden et al. 2020) and COVIDFACT (Saakyan, Chakrabarty, and Muresan 2021) benchmarks re-purposed this framework for the sci-

entific domain by releasing datasets of medical claims to be verified against scientific content (Wang et al. 2020). While this framework has led to impressive advances in fact verification performance (Ye et al. 2020; Pradeep et al. 2021), current benchmarks assume that the available evidence database contains only valid, factual information.

However, check-worthy claims are often made about new events that may not be verifiable against extensive catalogues, and that must be checked rapidly to avoid strategic disinformation spread (Vosoughi, Roy, and Aral 2018). Consequently, deployed fact-checkers will need to operate in settings where their available evidence is collected from contemporaneous reporting, which may be inadvertently sharing the same misinformation, or which may be intentionally influenced by systematic disinformation campaigns. Currently, malicious actors remain limited by the cost of running disinformation campaigns (DiResta et al. 2018) and the risks of operational discovery,<sup>4</sup> impeding the scale at which they can deploy these campaigns, and thus the balance of real and false content that fact-checkers must distinguish. However, the development of NLP tools capable of generating coherent disinformation (Zellers et al. 2019; Buchanan et al. 2021) would allow malicious actors to overload contemporaneous content with adversarial information (Brundage et al. 2018) and bias the evidence bases used by automated fact-checkers.

Furthermore, even in settings where claims may be verified against established and trusted knowledge, misinformation can still find its way into repositories of documents used by fact-checking systems (Kumar, West, and Leskovec 2016; Schuster, Fisch, and Barzilay 2021). Wikipedia, for example, which underlies FEVER (and other benchmarks; Petroni et al. 2021), acknowledges that much of the content on the platform may be incorrect, and remain so for long periods of time.<sup>5</sup> For example, the Croatian Wikipedia was contaminated by pro-nationalist bias over a period of at least 10 years.<sup>6</sup> Moreover, studies have uncovered articles on Wikipedia that were edited to provide favorable accounts on specific topics (e.g., workers at a medical device company edited articles to present an optimistic view toward treatments that used their product<sup>7</sup>). Modern NLP tools would allow malicious users to scale up production of disinformation on these platforms, and increase the perception of false consensus or debate on these topics.

In this paper, we evaluate whether automated disinformation generators can effectively contaminate the evidence sets of fact verification systems, and demonstrate that synthetic disinformation drastically lowers the performance of these systems. We define adversarial attacks in two settings: ADVERSARIAL ADDITION (ADVADD; §), where synthetically-generated documents are added to the document base, and ADVERSARIAL MODIFICATION (ADVMOD; §), where additional automatically-generated information is inserted into

existing documents. In both settings, we curate a large collection of adversarial disinformation documents that we inject into the pipelines of existing fact-checking systems developed for the FEVER, SCIFACT, and COVIDFACT shared tasks.<sup>8</sup>

Our results demonstrate that these systems are significantly affected by the injection of poisoned content in their evidence bases, with large absolute performance drops on all models in both settings. Furthermore, our analysis demonstrates that these systems are sensitive to even small amounts of evidence contamination, and that synthetic disinformation is more influential at deceiving fact verification systems compared to human-produced false content. Finally, we provide a discussion of our most important findings, and their importance in the context of continued advances in NLP systems.<sup>9</sup>

## Background

In this section, we review the formulation of automated fact checking as fact extraction and verification, and recent advances in automated generation of textual disinformation.

### Automated Fact-checking: Task

Current systems research in automated fact-checking often follows the fact verification and extraction procedure of receiving a natural language claim (e.g., “Hypertension is a common comorbidity seen in COVID-19 patients”), collecting supporting evidence from a repository of available documents (e.g., scientific manuscripts), and making a prediction about the claim’s veracity based off the collected supporting evidence. Below, we define the two stages of this pipeline: evidence retrieval and claim verification.

**Evidence retrieval** The evidence retrieval stage of fact verification systems is typically decomposed into two steps: *document retrieval* and *sentence retrieval*. During document retrieval, documents in the evidence repository that are relevant to the claim are selected. Existing methods typically use information retrieval methods to rank documents based on relevance (Thorne et al. 2018; Wadden et al. 2020) or use public APIs of commercial document indices (Hanselowski et al. 2019; Saakyan, Chakrabarty, and Muresan 2021) to crawl related documents. In the sentence retrieval stage, individual sentences from these retrieved documents are selected with respect to their relevance to the claim, often using textual entailment (Eisenschlos et al. 2021), or sentence similarity (Thorne et al. 2018) methods. Typically, the number of retrieved sentences is capped for computational efficiency.

**Claim verification** The claim verification stage of the pipeline evaluates the veracity of the claim with respect to the evidence sentences retrieved in the previous stage. Depending on the content found in the supporting sentences, each claim can typically be classified as *supported* (SUP), *refuted* (REF), or *not enough information* (NEI, though some benchmarks omit this label). Systems must aggregate and weigh the evidence sentences to predict the most likely label.

<sup>4</sup><https://www.lawfareblog.com/outsourcing-disinformation>

<sup>5</sup>[https://en.wikipedia.org/wiki/Wikipedia:Wikipedia\\_is\\_not\\_a\\_reliable\\_source](https://en.wikipedia.org/wiki/Wikipedia:Wikipedia_is_not_a_reliable_source)

Wikipedia:Wikipedia\_is\_not\_a\_reliable\_source

<sup>6</sup>[https://meta.wikimedia.org/wiki/Croatian\\_Wikipedia\\_Disinformation\\_Assessment-2021](https://meta.wikimedia.org/wiki/Croatian_Wikipedia_Disinformation_Assessment-2021)

Croatian\_Wikipedia\_Disinformation\_Assessment-2021

<sup>7</sup><https://www.theatlantic.com/business/archive/2015/08/wikipedia-editors-for-pay/393926/>

wikipedia-editors-for-pay/393926/

<sup>8</sup>We will release these documents under a Terms of Use to promote research in fact-checking systems in adversarial settings

<sup>9</sup>Our code can be found at:

<https://github.com/Yibing-Du/adversarial-factcheck>

<b>FEVER Claim</b>	Starrcade was an annual professional wrestling event that began in 1988.
<b>Original</b>	Starrcade (1988) was the sixth annual Starrcade professional wrestling pay-per-view (PPV) event produced under the National Wrestling Alliance (NWA) banner .
<b>GROVER</b>	Starrcade was a monthly professional wrestling event for the decades between 1988 and 2003 that ran for the entirety of a weekend in Boston , Mass.
<b>Media Cloud</b>	Goldberg’s perfect 173-0 streak ended at Starrcade 1998 after Kevin Nash scored the fateful pinfall with the help of Scott Hall and his taser gun.
<b>SCIFACT Claim</b>	Taxation of sugar-sweetened beverages had no effect on the incidence rate of type II diabetes in India.
<b>Original</b>	The 20% SSB tax was anticipated to reduce overweight and obesity prevalence by 3.0% ... and type 2 diabetes incidence by 1.6% ... among various Indian subpopulations over the period 2014-2023
<b>GROVER</b>	... analysis of a “cone-by-one” kind of survey question in India reached out to -9 145 trillion , including 2,557 separate instances of type II diabetes (which is comparable to the prevalence rate in Pakistan ...

Table 1: Sample ADVADD document excerpts generated by GROVER for the FEVER and SCIFACT datasets.

### Automated Fact-checking: Datasets

We briefly describe the provenance and structure of our studied datasets and refer the reader to the original works for in-depth descriptions of the construction of these resources.

**FEVER** The FEVER testbed (Thorne et al. 2018) is a dataset of 185,445 claims (145,449 train, 19,998 dev, 19,998 test) with corresponding evidence to validate them drawn from articles in Wikipedia. Because of its scale, the FEVER dataset is one of the most popular benchmarks for evaluating fact verification systems (Yoneda et al. 2018; Nie, Chen, and Bansal 2019; Zhou et al. 2019; Zhong et al. 2020; Subramanian and Lee 2020; Atanasova, Wright, and Augenstein 2020).

**SCIFACT** The SCIFACT dataset (Wadden et al. 2020) contains 1,409 expert-annotated scientific claims and associated paper abstracts. SCIFACT presents the challenge of understanding scientific writing as systems must retrieve relevant sentences from paper abstracts and identify if the sentences support or refute a presented scientific claim. It has emerged as a popular benchmark for evaluating scientific fact verification systems (Pradeep et al. 2021).

**COVIDFACT** The COVIDFACT dataset (Saakyan, Chakrabarty, and Muresan 2021) contains 1,296 crowd-sourced claims crawled (and filtered) from the */r/COVID19* subreddit. The evidence is composed of documents provided with these claims when they were posted on the subreddit along with resources from Google Search queries for the claims. Refuted claims were automatically-generated by altering key words in the original claims.

### Synthetic Disinformation Generation

Recent years have brought considerable improvements in the language generation capabilities of neural language models (Lewis et al. 2020; Ji et al. 2020; Brown et al. 2020; Holtzman et al. 2020), allowing users of these systems to pass off their generations as human-produced (Ippolito et al. 2020). These advances have raised dual-use concerns as to whether these tools could be used to generate text for malicious purposes (Radford et al. 2019; Bommasani et al. 2021), which humans would struggle to detect (Clark et al. 2021).

Specific studies have focused on whether neural language models could be used to generate disinformation that influences human readers (Kreps, McCain, and Brundage 2020; Buchanan et al. 2021). One such study directly explored this possibility by training GROVER, a large-scale, billion-parameter language model on a large dataset of newswire text with the goal of generating text that resembles news (Zellers et al. 2019). In human evaluations of the model’s generated text, the study found that human readers considered the synthetically-generated news to be as trustworthy as human-generated content. While the authors found that neural language models could identify fake, generated content when finetuned to detect distributional patterns in the generated text, they hypothesized that future detection methods would need to rely on external knowledge (*e.g.*, FEVER).

### ADVERSARIAL ADDITION: Evidence Repository Poisoning

In this section, we simulate the potential vulnerability of fact-checking models to database pollution with misinformation documents by injecting synthetically-generated false documents into the evidence sets of fact verification models, and assess the impact on the performance of these systems.

#### Approach

Our method, ADVERSARIAL ADDITION (ADVADD), uses GROVER to produce synthetic documents for a proposed claim, and makes these fake documents available to the fact verification system when retrieving evidence. As GROVER requires a proposed article title and publication venue (*i.e.*, website link) as input to generate a fake article, we use each claim as a title and set the article venue to wikipedia.com. We generate 10 articles for each claim and split them into paragraphs (*n.b.*, FEVER DB contains first paragraphs of Wikipedia articles and SCIFACT contains abstracts of scientific articles). Statistics for the number of documents generated for each benchmark are reported in Table 3. Additional implementation details for the experimental setting of each benchmark can be found in the Appendix.

Evidence	CorefBERT Acc. (Ye et al. 2020)			KGAT Acc. (Liu et al. 2020b)			MLA Acc. (Kruengkrai et al. 2021)		
	Total	REF	NEI	Total	REF	NEI	Total	REF	NEI
Original	73.05	74.03	72.07	70.76	72.50	69.01	75.92	78.71	73.13
ADVADD- <i>min</i>	34.80	47.22	22.38	34.08	48.63	19.52	60.93	73.04	48.81
ADVADD- <i>full</i>	<b>28.59</b>	<b>39.63</b>	<b>17.54</b>	<b>29.02</b>	<b>42.45</b>	<b>15.59</b>	<b>51.86</b>	<b>71.84</b>	<b>31.87</b>
ADVADD- <i>oracle</i>	21.18	27.09	15.26	23.43	31.47	15.38	29.05	29.76	28.33

Table 2: Effect of ADVADD on FEVER claim verification. We **bold** the largest performance drop relative to the original evidence.

Benchmark	Evidence Source	<i>N</i>
FEVER	FEVERDB	5,416,537
	GROVER Docs	995,829
	MediaCloud Docs	74,273,342
SCIFACT	Scientific Abstracts	5,183
	GROVER Docs	21,963
COVIDFACT	Google Search Results	1,003
	GROVER Docs	2,709

Table 3: Corpus statistics of evidence repositories

## FEVER Study

**Setup** For the FEVER benchmark, we select three high-ranking models from the leaderboard<sup>10</sup> with open-source implementations: KGAT (Liu et al. 2020b), CorefBERT (Ye et al. 2020), and MLA (Kruengkrai, Yamagishi, and Wang 2021). For document retrieval, all models use the rule-based method developed by Hanselowski et al. (2019), which uses the MediaWiki API to retrieve relevant articles based on named entity mentions in the claim. For each claim and poisoned document, we extract all keywords and retrieve associated Wikipedia pages. If we find overlaps between the associated Wikipedia pages of a claim and a poisoned document, then the poisoned document is matched with the claim for document retrieval. Once the retrieved documents are available, the KGAT and CorefBERT models use a BERT-based (Devlin et al. 2019) sentence retriever to rank evidence sentences based on relevance to the claim (trained using pairwise loss). The MLA sentence retriever expands on this approach with hard negative sampling from the same retrieved documents to more effectively discriminate context-relevant information that is irrelevant to the claim. Claim verifiers vary between models, but are generally based off pretrained language models (*e.g.*, CorefBERT, MLA) or graph neural networks (*e.g.*, KGAT). We use the REF and NEI claims from the FEVER development set to study how the preceding systems are affected by the introduction of poisoned evidence.<sup>11</sup>

**Impact of ADVADD** We report the overall (and claim-stratified) performance change of the tested models in Table 2. For all models, we see a significant performance drop

<sup>10</sup><https://competitions.codalab.org/competitions/18814#results>

<sup>11</sup>We discuss results related to SUP claims in the Appendix.

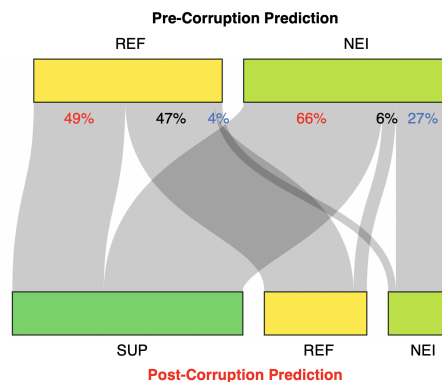


Figure 2: CorefBERT’s predictions change from REF and NEI to SUP once ADVADD poisons the evidence set.

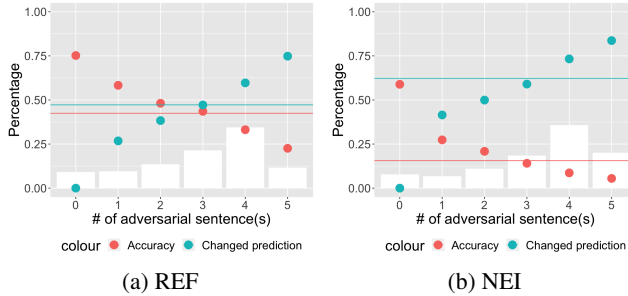
when GROVER-generated paragraphs are introduced into the available evidence set (ADVADD-*full*), indicating that fact verification models are sensitive to synthetically-generated information. This drop approaches the performance of an oracle (ADVADD-*oracle*), where only GROVER-generated documents are made available as evidence.

As confirmation that these attacks work as expected, we depict in Figure 2 how model predictions change once the synthetic disinformation is added to the evidence set. A significant number of claims that were originally predicted as REF or NEI are now predicted as SUP with the injected poisoned evidence. Consequently, we conclude that the poisoned evidence affects the model’s predictions in the intended way, and that cross-label changes for different pairings are rare. Furthermore, we also find that replacing the retrieved poisoned evidence with random retrieved evidence from FEVERDB does not cause the same performance drop ( $\sim 7\%$  vs.  $\sim 30\%$ ), indicating that these effects are caused by the injection of poisoned evidence, and not merely the replacement of potentially relevant evidence (see the Appendix for further details).

**Effect of disinformation scale** We also evaluate a setting where the attack is limited to retrieving only a single contaminated evidence sentence (ADVADD-*min*). The performance drops in the *min* setting are still considerable, suggesting that even limited amounts of injected disinformation can significantly affect downstream claim verification performance.

Moreover, Figure 3 shows a histogram of the number of poisoned evidence sentences retrieved per claim and a strat-

### GROVER Evidence



### MediaCloud Evidence

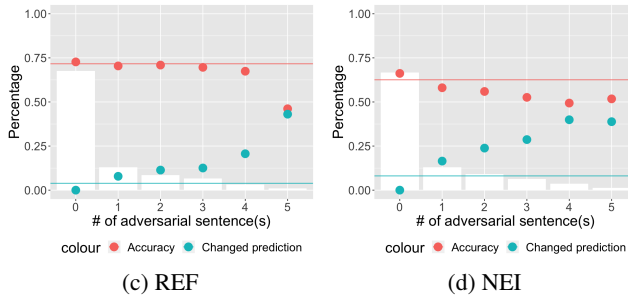


Figure 3: Degree of evidence poisoning and resulting REF (a,c) and NEI (b,d) claim verification accuracy for ADVADD-GROVER (a,b) and ADVADD-MediaCloud (c,d)

ified analysis of the final predictions. Figures 3 (a)(b) for ADVADD-GROVER (*i.e.*, ADVADD-*full*) show that accuracy steadily drops for claims with more corresponding evidence from poisoned documents; meanwhile, the likelihood that a prediction changes increases with more poisoned evidence. We note that claims labeled NEI are far more sensitive to the introduction of poisoned sentences than REF claims, even as the rate of contamination is approximately the same between both types of labels. While this result is promising because the model is more robust in the presence of even minimal *refuting* evidence, it also demonstrates that fact verification systems are more sensitive when no competing information is presented to a particular viewpoint (*i.e.*, data voids; Boyd and Golebiewski 2018).

**Quality of poisoned evidence** We also evaluate whether poisoned evidence produced by ADVADD is of sufficient quality to bypass potential human detectors. For 500 REF and 500 NEI claims from FEVER, we ran a study on Mechanical Turk where we presented three workers with five retrieved evidence examples (which could be from ADVADD or from FEVERDB) and asked them to identify which examples were machine-generated. Our results show that humans underestimate the number of poisoned sentences (23.6% recall), and do not distinguish machine- from human-generated evidence (48.6% precision). While well-trained workers will improve at recognizing synthetic content, our results demonstrate the challenge of distinguishing these evidence sources for lay readers, pointing to the quality of the synthetic content, and the potential for such an attack to remain undetected.

Source	Evidence Retrieval	
	Document	Sentence
GROVER	87%	65%
MediaCloud	99%	17%

Source	Claim Verification	
	KGAT	CorefBERT
Original	70.76	73.05
+ GROVER	29.02	28.59
+ MediaCloud	67.10	70.44

Table 4: Statistics and performance relative to the source of poisoned evidence: GROVER or MediaCloud

### Comparison with human-compiled online evidence

While we have shown that synthetic disinformation affects the performance of downstream claim verifiers when present in their evidence sets, the threat should be evaluated in comparison to the threat of already existing online misinformation on the same topic. Consequently, we use the MediaCloud<sup>12</sup> content analysis tool to crawl web content related to FEVER claims. We crawl English-language news since January 2018 that contains the keywords of a claim anywhere in their text and extract articles with a title that contains at least one keyword from the claim. Finally, we process these articles to have the same format as the original Wikipedia database, yielding 74M total available documents for retrieval (Table 3).

In Table 4, we report the performance of an ADVADD setting where only MediaCloud-crawled documents are available to the retriever compared to our original setting where GROVER-generated documents were available. We observe that evidence crawled from online content has less of an influence on downstream fact verification performance ( $\sim 3\%$  vs.  $\sim 40\%$  performance drop). While we are able to retrieve far more documents from MediaCloud due to the size of the database (99% of claims retrieve a document from MediaCloud), the sentences from ADVADD-GROVER documents are selected more frequently in the sentence retrieval step. While this gap would likely be less pronounced with more contentious claims that yield competing viewpoints (Bush and Zaheer 2019), these results demonstrate that synthetic disinformation can be much more targeted to a particular claim of interest. Figure 3 supports this conclusion, where we observe smaller performance drops for ADVADD-MediaCloud (c,d) compared to ADVADD-GROVER (a,b) even when all retrieved sentences are sourced from the poisoned evidence.

### SCIFACT Study

**Setup** For SCIFACT, we chose three systems for testing our attack: VeriSci (Wadden et al. 2020), ParagraphJoint (Li, Burns, and Peng 2021), and SciKGAT (Liu et al. 2020a). The VeriSci model was released by the creators of the SCIFACT benchmark and retrieves relevant abstracts to a claim using TF-IDF. The ParagraphJoint model, one of the top systems

<sup>12</sup>mediacloud.org

Model	Evidence Set	Sentence selection	Sentence label	Abstract label	Abstract rationalized
VeriSci (Wadden et al. 2020)	Original	47.69	42.62	51.03	48.45
	ADVADD	<b>27.05</b>	<b>23.50</b>	<b>25.57</b>	<b>24.33</b>
SciKGAT (Liu et al. 2020a)	Original	55.61	51.69	58.04	57.41
	ADVADD	<b>39.44</b>	<b>36.97</b>	<b>37.46</b>	<b>36.98</b>
ParagraphJoint (Li, Burns, and Peng 2021)	Original	53.63	43.59	55.52	49.55
	ADVADD	<b>37.68</b>	<b>32.60</b>	<b>41.31</b>	<b>37.12</b>

Table 5: Effect of ADVADD evidence on the SCIFACT benchmark. We **bold** performance drops relative to the original evidence.

on the SCIFACT leaderboard, uses a word embedding-based method to retrieve abstracts. Both use a RoBERTa-based module for rationale selection and label prediction. The SciKGAT model uses the same evidence retrieval as VeriSci, but the KGAT model (Liu et al. 2020b) to verify claims. We use the 300 claims from the development set to evaluate our method. We generate GROVER articles as with FEVER, but we set the venue URL to medicalnewstoday.com, which produces articles more likely to reflect scientific and medical content.

**Results** In Table 5, we observe large performance drops across all metrics for all models. Furthermore, we note that our disinformation generator, GROVER, is not trained on large quantities of scientific documents of the same format as the original evidence. Despite producing documents that are stylistically different, the disinformation is still retrieved as evidence, and affects the performance of the verifier.

### COVIDFACT Study

**Setup** We run our analysis on the baseline system from Saakyan, Chakrabarty, and Muresan (2021). This model retrieves evidence documents for claims using Google Search and then selects evidence sentences based off high cosine similarity between sentence embeddings of the claims and individual evidence sentences (Reimers and Gurevych 2019). A RoBERTa-based model predicts a veracity label. We generate ADVADD articles in the same manner as for SCIFACT, and run our analysis on the 271 REF claims from the test set.

**Results** In both the Top-1 and Top-5 settings from Saakyan, Chakrabarty, and Muresan (2021), we observe a  $\sim 14.4\%$  performance drop on REF claims ( $83.8\% \rightarrow 69.4\%$ ). We note that COVIDFACT random and majority accuracy is only 67.6% due to a label imbalance.

### ADVERSARIAL MODIFICATION: Evidence Document Poisoning

In Section , we investigated the effect of adding disinformation documents to the evidence repositories of fact verification systems, simulating the setting where the dynamic pace of news might lead to fake information being used to verify real-time claims. However, even in settings where information has more time to settle and facts to crystallize, misinformation can still find its way into repositories of documents used by fact-checking systems. Motivated by the possibility

of malicious edits being made to crowdsourced information resources, we explore how NLP methods could be used to automatically edit existing articles with fake content at scale.

### Approach

Our method, ADVERSARIAL MODIFICATION (ADVMOD), simulates this setting in a two-stage process. First, we use off-the-shelf NLP tools to generate modified versions of the claim presented to the fact verifier. Then, we append our modified claims to articles in the evidence base that are relevant to the original claim. We modify the original claims in two ways.

In the *paraphrase* approach, we use a state-of-the-art paraphrasing model, PEGASUS (Zhang et al. 2019), to generate paraphrased versions of the original claim (see Table 7 for example). These paraphrases generally retain the meaning of the claim, but often remove contextualizing information that would be found in the context of the article in which the new sentence is inserted. Because the *paraphrase* method attempts to produce synthetic evidence that is semantically equivalent to the original claim, we test its efficacy relative to a method that merely introduces irrelevant content to the evidence document. Motivated by Jia and Liang (2017), we alter a claim by applying heuristics such as number alteration, antonym substitution, and entity replacement with close neighbors according to embedding similarity (Bojanowski et al. 2017). These modifications should not confuse humans, but would affect sensitive fact verification systems, providing a competitive baseline for assessing the strength of ADVMOD-*paraphrase*.

Finally, our oracle reports the performance when the claim itself is appended to an evidence document.

### Results

Our results in Table 6 demonstrate that injecting poisoned evidence sentences into existing documents is an effective method for fooling fact verification systems. Our ADVMOD-*paraphrase* method causes a significant drop on all tested models for both REF and NEI labeled claims. Furthermore, we also note that ADVMOD-*paraphrase* achieves larger performance drops than the baseline method, ADVMOD-*KeyReplace*, for most claim types (the KGAT model is slightly more sensitive to the baseline ADVMOD-*KeyReplace* for the NEI claims), indicating that injections of disinformative content are more effective than non-targeted perturbances to the evidence (e.g., ADVMOD-*KeyReplace*).

Evidence	CorefBERT Acc. (Ye et al. 2020)			KGAT Acc. (Liu et al. 2020b)			MLA Acc. (Kruengkrai et al. 2021)		
	Total	REF	NEI	Total	REF	NEI	Total	REF	NEI
Original	73.05	74.03	72.07	70.76	72.50	69.01	75.92	78.71	73.13
ADVMOD- <i>KeyReplace</i>	53.83	66.50	41.15	42.82	68.90	<b>16.74</b>	60.93	81.83	40.02
ADVMOD- <i>paraphrase</i>	<b>32.62</b>	<b>36.66</b>	<b>28.58</b>	<b>37.22</b>	<b>51.74</b>	22.70	<b>52.72</b>	<b>70.57</b>	<b>34.86</b>
ADVMOD- <i>oracle (claim)</i>	4.78	7.94	1.61	11.90	23.78	0.02	25.17	45.96	4.37

Table 6: Effect of ADVMOD on FEVER claim verification. We **bold** the largest performance drop relative to the original evidence.

<b>Original</b>	Damon Albarn’s debut album was released in 2011.
<b>Paraphrase</b>	<b>Albarn’s first</b> album was released in 2011. <b>His</b> debut album was released in 2011.
<b>KeyReplace</b>	<b>Matt Coldplay’s</b> debut album was released in <b>202</b> . <b>Stefan Blur’s</b> debut album was released in <b>1822</b> .

Table 7: Sample ADVMOD sentences

## Discussion

Adding synthetic content to the evidence bases of fact verifiers significantly decreases their performance. Below, we discuss interesting findings and limitations of our study.

**Synthetic vs. human disinformation** As mentioned in Section , the performance of our test systems is more sensitive to poisoned evidence generated from GROVER than retrieved from MediaCloud, even as the number of documents retrieved from MediaCloud far exceeds the number generated from GROVER. While FEVER claims may not generally be worth opposing online (leading to less directly adversarial content being retrieved from MediaCloud), we note that language models have no such limitations, and can generate large quantities of disinformation about any topic. Consequently, while misinformation already makes its way into retrieval search results (Bush and Zaheer 2019), language models could cheaply skew the distribution of content more drastically (Bommasani et al. 2021), particularly on topics that receive less mainstream coverage, but may be of import to a malicious actor (Starbird et al. 2018).

**Language models as a defense** In the ADVADD and ADVMOD oracle settings, all tested systems performed better on claims labeled REF than for claims labeled NEI. This result implies that the GROVER-generated evidence was less adversarial for these claims, or that the pretrained models which these systems use to encode the claim and evidence sentences were more robust against claims that should be *refuted*. Consequently, we conclude that language models encode priors about the veracity of claims, likely from the knowledge they learn about entities during pretraining (Petroni et al. 2019), a conclusion also supported by contemporaneous work in using standalone language models as fact-checkers (Lee et al. 2020, 2021). While this property can be an advantage in some settings (*i.e.*, language models pretrained on reliable text repositories will be natural defenses against textual misinformation), it will also be a liability when previously learned

erroneous knowledge will counteract input evidence that contradicts it. Finally, we note that the presence of implicit knowledge in language models affecting the interpretation of input evidence implies that the training corpora of these LMs could be attacked to influence downstream fact verification. Prior work has explored poisoning task-specific training datasets (Wallace et al. 2021). As disinformation becomes more prevalent online, the pretraining corpora of LMs will require more careful curation to avoid learning adversarial content.

**Limitations** We identify three main limitations to our study. First, the FEVER document retrievers use the MediaWiki API to collect relevant Wikipedia articles based on entity mentions in the claim. We assume our synthetic content could be included in the retrieved documents if it were titled with a mention of the named entities in the claim. For SCIFACT, this limitation is not present because synthetic abstracts are retrieved using statistical IR methods. Second, our method ADVADD uses the actual claim to generate the synthetic article. In the absence of explicit coordination, synthetic poisoned evidence would be generated without knowledge of the exact claim formulation, reducing the realistic correspondence between the claim and the synthetic disinformation. If the GROVER model directly copied the claim during generation, performance drops might be overestimated based on unrealistically aligned evidence. For the ADVADD-*full* setting, we measure that this issue arises in  $\sim 20\%$  of claims, which are predicted incorrectly more often, but does not affect the conclusions of our study. Finally, our FEVER and COVIDFACT studies are run using only claims labeled as REF and NEI, which we discuss in more detail in the Appendix.

## Conclusion

In this work, we evaluate the robustness of fact verification models when we poison the evidence documents they use to verify claims. We develop two poisoning strategies motivated by real world capabilities: ADVADD, where synthetic documents are added to the evidence set, and ADVMOD, where synthetic sentences are added to existing documents in the evidence set. Our results show that these strategies significantly decrease claim verification accuracy. While these results are troubling, we are optimistic that improvements in automated synthetic content detection, particularly by online platforms with considerable resources, combined with human audits of fact-checker evidence (and their source), may still potentially mitigate many attempted disinformation campaigns.

## Acknowledgements

We thank the anonymous reviewers for their feedback that improved this paper, Shelby Grossman and the members of the Stanford SNAP and NLP groups for helpful discussions, and Tuhin Chakrabarty, Arkadiy Saakyan, and Xiangci Li for help in implementing the CovidFact and ParagraphJoint baselines. Antoine Bosselut acknowledges the support of JD.com, Sony Corporation, and the Allen Institute for AI.

## References

- Atanasova, P.; Wright, D.; and Augenstein, I. 2020. Generating Label Cohesive and Well-Formed Adversarial Claims. In *EMNLP*.
- Bojanowski, P.; Grave, E.; Joulin, A.; and Mikolov, T. 2017. Enriching Word Vectors with Subword Information. *TACL*, 5.
- Bommasani, R.; Hudson, D. A.; Adeli, E.; Altman, R.; Arora, S.; von Arx, S.; Bernstein, M. S.; Bohg, J.; Bosselut, A.; Brunskill, E.; Brynjolfsson, E.; Buch, S.; Card, D.; Castellon, R.; Chatterji, N. S.; Chen, A.; Creel, K.; Davis, J. Q.; Demszky, D.; Donahue, C.; Doumbouya, M.; Durmus, E.; Ermon, S.; Etchemendy, J.; Ethayarajh, K.; Fei-Fei, L.; Finn, C.; Gale, T.; Gillespie, L. E.; Goel, K.; Goodman, N. D.; Grossman, S.; Guha, N.; Hashimoto, T.; Henderson, P.; Hewitt, J.; Ho, D. E.; Hong, J.; Hsu, K.; Huang, J.; Icard, T. F.; Jain, S.; Jurafsky, D.; Kalluri, P.; Karamcheti, S.; Keeling, G.; Khani, F.; Khattab, O.; Koh, P. W.; Krass, M.; Krishna, R.; Kuditipudi, R.; Kumar, A.; Ladhak, F.; Lee, M.; Lee, T.; Leskovec, J.; Levent, I.; Li, X. L.; Li, X.; Ma, T.; Malik, A.; Manning, C. D.; Mirchandani, S. P.; Mitchell, E.; Munyikwa, Z.; Nair, S.; Narayan, A.; Narayanan, D.; Newman, B.; Nie, A.; Niebles, J. C.; Nilforoshan, H.; Nyarko, J.; Ogut, G.; Orr, L.; Papadimitriou, I.; Park, J.; Piech, C.; Portelance, E.; Potts, C.; Raghunathan, A.; Reich, R.; Ren, H.; Rong, F.; Roohani, Y. H.; Ruiz, C.; Ryan, J.; R'è, C.; Sadigh, D.; Sagawa, S.; Santhanam, K.; Shih, A.; Srinivasan, K.; Tamkin, A.; Taori, R.; Thomas, A. W.; Tramèr, F.; Wang, R. E.; Wang, W.; Wu, B.; Wu, J.; Wu, Y.; Xie, S. M.; Yasunaga, M.; You, J.; Zaharia, M.; Zhang, M.; Zhang, T.; Zhang, X.; Zhang, Y.; Zheng, L.; Zhou, K.; and Liang, P. 2021. On the Opportunities and Risks of Foundation Models. *ArXiv*, abs/2108.07258.
- Boyd, D.; and Golebiewski, M. 2018. Data Voids: Where Missing Data Can Easily Be Exploited. [https://datasociety.net/wp-content/uploads/2018/05/Data\\_Society\\_Data\\_Voids\\_Final\\_3.pdf](https://datasociety.net/wp-content/uploads/2018/05/Data_Society_Data_Voids_Final_3.pdf). Accessed: 2022-04-30.
- Brown, T. B.; Mann, B.; Ryder, N.; Subbiah, M.; Kaplan, J.; Dhariwal, P.; Neelakantan, A.; Shyam, P.; Sastry, G.; Askell, A.; Agarwal, S.; Herbert-Voss, A.; Krueger, G.; Henighan, T.; Child, R.; Ramesh, A.; Ziegler, D. M.; Wu, J.; Winter, C.; Hesse, C.; Chen, M.; Sigler, E.; Litwin, M.; Gray, S.; Chess, B.; Clark, J.; Berner, C.; McCandlish, S.; Radford, A.; Sutskever, I.; and Amodei, D. 2020. Language Models are Few-Shot Learners. *ArXiv*, abs/2005.14165.
- Brundage, M.; Avin, S.; Clark, J.; Toner, H.; Eckersley, P.; Garfinkel, B.; Dafoe, A.; Scharre, P.; Zeitzoff, T.; Filar, B.; Anderson, H.; Roff, H.; Allen, G. C.; Steinhardt, J.; Flynn, C.; hÉigeartaigh, S. O.; Beard, S.; Belfield, H.; Farquhar, S.; Lyle, C.; Crootof, R.; Evans, O.; Page, M.; Bryson, J.; Yampolskiy, R.; and Amodei, D. 2018. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. *arXiv preprint arXiv:1802.07228*.
- Buchanan, B.; Lohn, A.; Musser, M.; and Sedova, K. 2021. *Truth, Lies, and Automation: How Language Models Could Change Disinformation*. Center for Security and Emerging Technology.
- Bush, D.; and Zaheer, A. 2019. Bing's Top Search Results Contain an Alarming Amount of Disinformation. *Internet Observatory News*.
- Clark, E.; August, T.; Serrano, S.; Haduong, N.; Gururangan, S.; and Smith, N. A. 2021. All That's 'Human' Is Not Gold: Evaluating Human Evaluation of Generated Text. *arXiv preprint arXiv:2107.00061*.
- Devlin, J.; Chang, M.-W.; Lee, K.; and Toutanova, K. 2019. BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding. In *NAACL*.
- DiResta, R.; Shaffer, K.; Ruppel, B.; Sullivan, D.; Matney, R. C.; Fox, R.; Albright, J.; and Johnson, B. 2018. The tactics & tropes of the Internet Research Agency. <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1003&context=senatedocs>. Accessed: 2022-04-30.
- Eisenschlos, J. M.; Dhingra, B.; Bulian, J.; Borschinger, B.; and Boyd-Graber, J. L. 2021. Fool Me Twice: Entailment from Wikipedia Gamification. In *NAACL*.
- Germani, F.; and Biller-Andorno, N. 2021. The anti-vaccination infodemic on social media: A behavioral analysis. *PLOS ONE*, 16(3): 1–14.
- Guo, Z.; Zhang, Y.; and Lu, W. 2019. Attention Guided Graph Convolutional Networks for Relation Extraction. In *ACL*.
- Hanselowski, A.; Zhang, H.; Li, Z.; Sorokin, D.; Schiller, B.; Schulz, C.; and Gurevych, I. 2019. UKP-Athene: Multi-Sentence Textual Entailment for Claim Verification. *arXiv:1809.01479*.
- Holtzman, A.; Buys, J.; Forbes, M.; and Choi, Y. 2020. The Curious Case of Neural Text Degeneration. In *ICLR*.
- Ippolito, D.; Duckworth, D.; Callison-Burch, C.; and Eck, D. 2020. Automatic Detection of Generated Text is Easiest when Humans are Fooled. In *ACL*.
- Ji, Y.; Bosselut, A.; Wolf, T.; and Celikyilmaz, A. 2020. The Amazing World of Neural Language Generation. In *Proceedings of the 2020 Conference on Empirical Methods in Natural Language Processing: Tutorial Abstracts*, 37–42. Online: Association for Computational Linguistics.
- Jia, R.; and Liang, P. 2017. Adversarial Examples for Evaluating Reading Comprehension Systems. In *EMNLP*.
- Kreps, S.; McCain, R. M.; and Brundage, M. 2020. All the News That's Fit to Fabricate: AI-Generated Text as a Tool of Media Misinformation. *Journal of Experimental Political Science*.



- Kruengkrai, C.; Yamagishi, J.; and Wang, X. 2021. A Multi-Level Attention Model for Evidence-Based Fact Checking. In *Findings of ACL*.
- Kumar, S.; West, R.; and Leskovec, J. 2016. Disinformation on the Web: Impact, Characteristics, and Detection of Wikipedia Hoaxes. In *WWW*.
- Lee, N.; Bang, Y.; Madotto, A.; Khabsa, M.; and Fung, P. 2021. Towards Few-shot Fact-Checking via Perplexity. In *NAACL*.
- Lee, N.; Li, B. Z.; Wang, S.; tau Yih, W.; Ma, H.; and Khabsa, M. 2020. Language Models as Fact Checkers? *ArXiv*, abs/2006.04102.
- Lewis, M.; Liu, Y.; Goyal, N.; Ghazvininejad, M.; Mohamed, A.; Levy, O.; Stoyanov, V.; and Zettlemoyer, L. 2020. BART: Denoising Sequence-to-Sequence Pre-training for Natural Language Generation, Translation, and Comprehension. In *ACL*.
- Li, X.; Burns, G.; and Peng, N. 2021. A Paragraph-level Multi-task Learning Model for Scientific Fact-Verification. *arXiv:2012.14500*.
- Liu, Z.; Xiong, C.; Dai, Z.; Sun, S.; Sun, M.; and Liu, Z. 2020a. Adapting Open Domain Fact Extraction and Verification to COVID-FACT through In-Domain Language Modeling. In *Findings of EMNLP*.
- Liu, Z.; Xiong, C.; Sun, M.; and Liu, Z. 2020b. Fine-grained Fact Verification with Kernel Graph Attention Network. In *ACL*.
- Nie, Y.; Chen, H.; and Bansal, M. 2019. Combining Fact Extraction and Verification with Neural Semantic Matching Networks. In *AAAI*.
- Petroni, F.; Piktus, A.; Fan, A.; Lewis, P.; Yazdani, M.; De Cao, N.; Thorne, J.; Jernite, Y.; Karpukhin, V.; Maillard, J.; Plachouras, V.; Rocktäschel, T.; and Riedel, S. 2021. KILT: a Benchmark for Knowledge Intensive Language Tasks. In *NAACL*.
- Petroni, F.; Rocktäschel, T.; Lewis, P.; Bakhtin, A.; Wu, Y.; Miller, A. H.; and Riedel, S. 2019. Language Models as Knowledge Bases? In *EMNLP*.
- Pradeep, R.; Ma, X.; Nogueira, R.; and Lin, J. J. 2021. Scientific Claim Verification with VerT5erini. *ArXiv*, abs/2010.11930.
- Radford, A.; Wu, J.; Child, R.; Luan, D.; Amodei, D.; and Sutskever, I. 2019. Language Models are Unsupervised Multitask Learners. <https://openai.com/blog/better-language-models/>. Accessed: 2022-04-30.
- Reimers, N.; and Gurevych, I. 2019. Sentence-BERT: Sentence Embeddings using Siamese BERT-Networks. In *EMNLP-IJCNLP*.
- Saakyan, A.; Chakrabarty, T.; and Muresan, S. 2021. COVID-Fact: Fact Extraction and Verification of Real-World Claims on COVID-19 Pandemic. In *ACL/IJCNLP*.
- Schuster, T.; Fisch, A.; and Barzilay, R. 2021. Get Your Vitamin C! Robust Fact Verification with Contrastive Evidence. In *NAACL*.
- Starbird, K.; Arif, A.; Wilson, T.; Van Koeveering, K.; Yefimova, K.; and Scarnecchia, D. 2018. Ecosystem or Echo-System? Exploring Content Sharing across Alternative Media Domains. *Proceedings of the International AAAI Conference on Web and Social Media*, 12(1).
- Subramanian, S.; and Lee, K. 2020. Hierarchical Evidence Set Modeling for Automated Fact Extraction and Verification. In *EMNLP*.
- Thorne, J.; and Vlachos, A. 2018. Automated Fact Checking: Task Formulations, Methods and Future Directions. In *COLING*.
- Thorne, J.; Vlachos, A.; Christodoulopoulos, C.; and Mittal, A. 2018. FEVER: a Large-scale Dataset for Fact Extraction and VERification. In *NAACL-HLT*.
- Vosoughi, S.; Roy, D.; and Aral, S. 2018. The spread of true and false news online. *Science*, 359(6380).
- Wadden, D.; Lin, S.; Lo, K.; Wang, L. L.; van Zuylen, M.; Cohan, A.; and Hajishirzi, H. 2020. Fact or Fiction: Verifying Scientific Claims. In *EMNLP*.
- Wallace, E.; Zhao, T. Z.; Feng, S.; and Singh, S. 2021. Concealed Data Poisoning Attacks on NLP Models. In *NAACL*.
- Wang, L. L.; Lo, K.; Chandrasekhar, Y.; Reas, R.; Yang, J.; Eide, D.; Funk, K.; Kinney, R. M.; Liu, Z.; Merrill, W.; Mooney, P.; Murdick, D.; Rishi, D.; Sheehan, J.; Shen, Z.; Stilson, B. B. S.; Wade, A. D.; Wang, K.; Wilhelm, C.; Xie, B.; Raymond, D. A.; Weld, D. S.; Etzioni, O.; and Kohlmeier, S. 2020. CORD-19: The COVID-19 Open Research Dataset. *arXiv: 2004.10706*.
- Ye, D.; Lin, Y.; Du, J.; Liu, Z.; Li, P.; Sun, M.; and Liu, Z. 2020. Coreferential Reasoning Learning for Language Representation. In *EMNLP*.
- Yoneda, T.; Mitchell, J.; Welbl, J.; Stenetorp, P.; and Riedel, S. 2018. UCL Machine Reading Group: Four Factor Framework For Fact Finding (HexaF). In *FEVER*.
- Zellers, R.; Holtzman, A.; Rashkin, H.; Bisk, Y.; Farhadi, A.; Roesner, F.; and Choi, Y. 2019. Defending Against Neural Fake News. In *NeurIPS*.
- Zhang, J.; Zhao, Y.; Saleh, M.; and Liu, P. J. 2019. PEGASUS: Pre-training with Extracted Gap-sentences for Abstractive Summarization. *arXiv:1912.08777*.
- Zhong, W.; Xu, J.; Tang, D.; Xu, Z.; Duan, N.; Zhou, M.; Wang, J.; and Yin, J. 2020. Reasoning Over Semantic-Level Graph for Fact Checking. In *ACL*.
- Zhou, J.; Han, X.; Yang, C.; Liu, Z.; Wang, L.; Li, C.; and Sun, M. 2019. GEAR: Graph-based Evidence Aggregating and Reasoning for Fact Verification. In *ACL*.