BULLETIN OF THE POLISH ACADEMY OF SCIENCES
TECHNICAL SCIENCES, Vol. 69(4), 2021, Article number: e137724
DOI: 10.24425/bpasts.2021.137724

SPECIAL SECTION

A survey of requirements for COVID-19 mitigation strategies

Wojciech JAMROGA[1, 2*], David MESTEL[1], Peter B. ROENNE[1], Peter Y.A. RYAN[1], and Marjan SKROBOT[1]

[1] Interdisciplinary Centre on Security, Reliability and Trust, SnT, University of Luxembourg
[2] Institute of Computer Science, Polish Academy of Sciences, ul. Jana Kazimierza 5, 01-248 Warsaw, Poland

Abstract. The COVID-19 pandemic has influenced virtually all aspects of our lives. Across the world, countries have applied various mitigation strategies, based on social, political, and technological instruments. We postulate that multi-agent systems can provide a common platform to study (and balance) their essential properties. We also show how to obtain a comprehensive list of the properties by "distilling" them from media snippets. Finally, we present a preliminary take on their formal specification, using ideas from multi-agent logics.

Key words: COVID-19; mitigation strategies; specification; multi-agent logic.

1. INTRODUCTION

COVID-19 has influenced virtually all aspects of our lives. Across the world, countries applied wildly varying mitigation strategies for the epidemic, ranging from minimal intrusion in the hope of obtaining "herd immunity", to imposing severe lockdowns on the other extreme. It seems clear at the first glance what all those measures are trying to achieve, and what the criteria of success are. But is it really that clear? Quoting an oft-repeated phrase, with COVID-19 we fight *an unprecedented threat to health and economic stability* [1]. While fighting it, we must *protect privacy*, *equality and fairness* [2] and *do a coordinated assessment of usefulness*, *effectiveness*, *technological readiness*, *cybersecurity risks and threats to fundamental freedoms and human rights* [3]. Taken together, this is hardly a straightforward set of goals and requirements. Thus, paraphrasing [3], one may ask:

What problem does an anti-COVID strategy solve exactly?

Even a quick survey of news articles, manifestos, and research papers published since the beginning of the pandemic reveals a diverse landscape of postulates and opinions. Some authors focus on medical goals, some on technological requirements; others are concerned by the economic, social, or political impact of a containment strategy. The actual stance is often related to the background of the author (in the case of a researcher) or their information sources (in the case of a journalist). Moreover, the authors advocating a particular aspect of the strategy most often neglect all the other aspects. We propose that the field of multi-agent systems can offer a common platform to study all the relevant properties, due to its interdisciplinary nature [4, 5], well-developed theories of heterogeneous agency [6, 7], and a wealth of formal methods for specification and verification [5, 8, 9].

This still leaves the question of how to gather the *actual* goals and requirements for a COVID-19 mitigation strategy. One way to achieve it is to look at what is considered relevant by the general public, and referred to in the media. To this end, we collected a number of news quotes, ordered them thematically and with respect to the type of concern, and presented in [10], see Section 2 for more details. Then, we took the quotes, and distilled a comprehensive list of goals, requirements, and risks. The list is presented in Section 3. In Section 4, we make the first step towards a formalization of the properties in multi-agent logic. We conclude in Section 5.

Besides the potential input to the design of anti-COVID-19 strategies, the main contribution of this paper is methodological: we demonstrate how to obtain a comprehensive specification of properties for complex Multi-Agent Systems (MAS) by searching for hints in the public space.

2. EXTRACTING REQUIREMENTS FROM NEWS CLIPS

Specification of properties is probably the most neglected part of formal verification for MAS. The tools usually come with examples of how to model the system [11–14]. For a complex multi-agent scenario, however, it is not clear *where the specifications of relevant properties should come from*.

Mitigating COVID-19 illustrates the point well. Research on mitigation measures is typically characterized by: (a) strong focus on the native domain of the authors, and (b) focus on the details, rather than the general picture. In order to avoid "overlooking the forest for the trees," we came up with a different methodology.

2.1. Methodology

We have looked for relevant phrases that appeared in the media, with no particular method of source selection. Then,

*e-mail: wojciech.jamroga@uni.lu

Manuscript submitted 2021-03-01, revised 2021-05-06, initially accepted for publication 2021-06-06, published in August 2021

we extracted the properties, and whenever possible generalized statements on specific measures to the mitigation strategy in general. Finally, we sorted them thematically, and divided into 3 categories: *goals*, additional *requirements*, and potential *risks and threats*. While most of the collected snippets focus on digital contact tracing, the relevance of the requirements goes well beyond that, and applies to all the aspects of the epidemic.

We emphasize that *we do not endorse the opinions being presented in the quotes*. We also *do not comment on their content*. We merely use the quotes to collect relevant keywords and conceptual categories. The reasons are twofold. First, we are not competent enough to assess the merits of most of the statements, in particular the ones concerning the medical, epidemiological, economic, ethical, legal, and social aspects. Secondly, the aim of this paper is to collect *plausible* requirements, i.e., ones that are considered relevant by (at least some) experts. Clearly, no mitigation strategy can satisfy them all. A systematic analysis of which subset can be feasibly obtained, and how to weigh their relative importance, should follow as the next step through a consensus of multidisciplinary experts.

We present a sample of the quotes in the remainder of this section, namely the ones related to basic epidemiological goals, societal requirements, and data protection. A more comprehensive collection of "news clips" can be found in the technical report [10]. The resulting list of goals, requirements and threats will be presented in Section 3.

2.2. News clips: epidemiological goals

Containment measures should slow the spread of the virus, decrease the transmission rate, and save lives:

> Since the outbreak of COVID-19, governments around the world have implemented a range of digital tracking, physical surveillance and censorship measures in a bid to *slow the spread of the virus* [15].

> Lockdowns *prevented* around 3.1 million *deaths* in 11 European countries [16].

> Researchers also calculated that the interventions had *caused the reproduction number* – how many people someone with the virus infects – *to drop* by an average of 82 percent, to below 1.0 [16].

> Contact tracing can be an important component of an *epidemic response* especially when the prevalence of infection is low. Such efforts are most *effective* where testing is rapid and widely available and when infections are relatively rare [1].

> To *best meet public health needs*, digital technology should be able to *trace the spread of the virus*, *identify dangerous Covid-19 clusters* and *limit further transmission*. The essential goal is to *register contacts between potential carriers and those who might be infected* [17].

> designed and built by the NHS to help *slow the spread of the coronavirus* [18].

> even finding a fraction of cases through contact tracing will help *slow the virus's spread* [19].

> Contact tracing via smartphone is a powerful way to *tackle the spread of coronavirus*, but it mustn't be done at the expense of individual civil rights [20].

> Smittestopp is an app that will *help the health authorities to limit the transmission of coronavirus* and alert users with text messages about close contact with infected persons [21].

2.3. News clips: impact on society

Regarding the available measures in general, and contact tracing apps in particular:

> we know very little about them or how they could *affect society* [21].

> As the global fight against the COVID-19 pandemic continues, much of the world is pinning its hopes of *easing lockdowns* on being able to quickly identify people who might have been exposed to the virus [23].

> [The Covidsafe app] was sold as the key to *unlocking restrictions* (…) but as the country begins to open up, the role of the Covidsafe app in the recovery seems to have dropped to marginal at best [24].

> The health minister, Greg Hunt, tweeted that [the Covidsafe app] was the key to *being allowed to go back to watching football* [24].

2.3.1. Disinformation and information abuse

> We worry that contact-tracing apps will serve as vehicles for *abuse and disinformation*, while providing a *false sense of security* to justify reopening local and national economies well before it is safe to do so [1].

> Since the outbreak of COVID-19 there has been a rapid acceleration in the *spread of mis- and disinformation*. To *control this*, governments and social media platforms have sought to stringently *regulate online content* and *promote official facts and figures from international health organisations* [15].

2.3.2. Potential for discrimination and social divides

> There is also a very real danger that these voluntary surveillance technologies will effectively become *compulsory for any public and social engagement* [1].

there is a real risk that these mobile-based apps can *turn unaffected individuals into social pariahs*, *restricted from accessing public and private spaces or participating in social and economic activities* [1].

protecting those *communities who can be (...) harmed by the collection and exploitation of personal data* [1].

Protections need to be put in place to expressly *prohibit economic and social discrimination on the basis of information and technology designed to address the pandemic* [1].

2.3.3. Political Impact

The pandemic creates new space for political manipulation and changes the distribution of power:

the issue of malicious use is paramount—particularly given this current climate of disinformation, astroturfing, and *political manipulation*. Imagine an unscrupulous political operative who wanted to dampen voting participation in a given district, or a desperate business owner who wanted to stifle competition. Either could falsely report incidences of coronavirus without much fear of repercussion. Trolls could sow chaos for the malicious pleasure of it. Protesters could trigger panic as a form of civil disobedience. A foreign intelligence operation could shut down an entire city by falsely reporting COVID-19 infections in every neighborhood [1].

In the long run, however, this poses a far more fundamental question: *how much can the decisions of sovereign democratic countries be overruled by technology companies* [i.e., Google and Apple]? [17].

2.4. News clips: data protection and misuse of data

Here, the key questions are:

What data will they collect, and *who is it shared with* [22].

as well as

how data is *collected*, *stored and deleted* [25].

In particular, it is often postulated to have

less *state access* and *control over user data* [25].

the *limits on the type of data collection* are the core concern for states [26].

In Singapore, for example, the TraceTogether app can be used *only by its health ministry* to access data. It assures citizens that the data is to be *used strictly for disease control* and will not be *shared with law enforcement agencies* for enforcing lockdowns and quarantine [27].

[Australia:] *Only health officials* in the states *can access the data*, and you can't be forced to download it [24].

The app does not *collect any of your personal data* [18].

2.4.1. Risks and threats

collection of data on centralised servers: Aside from the risk to privacy, *collecting millions of datasets of personal information in a single place could be viewed as somewhat of a treasure trove* [28].

if the [central] database is hacked, the *anonymity* provided by rotating pseudonyms is nullified, and *individuals can be more easily tracked*. Plus, says Kreps, "there's a risk of *function creep* and *state surveillance*". "I have little faith in government's ability to keep data like this secure," says Green [23].

data breaches can also come through *cyberattacks* or *independent actors within an agency* [29].

In particular, the collected information should not be exploited for commercial purposes:

existing regulations don't address whether *data can be shared across agencies* or if it can be *sold by a third party* for non-Covid-19 tracking [29].

We found code relating to *Google's advertising and tracking platforms* in 17 contact tracing apps. (...) We also found code that enabled *varying levels of integration with Facebook* in seven apps [15].

The full list of collected quotes can be found in [10].

3. GOALS AND REQUIREMENTS FOR COVID-19

Based on the quotes, we identified the following goals, requirements and potential vulnerabilities of a containment strategy.

3.1. Epidemiological and health-related concerns

COVID-19 is first and foremost a threat to people's health. Accordingly, we begin with requirements related to this aspect.

3.1.1. Epidemiological goals

The goal of the mitigation strategy in general, and digital measures in particular, is to:

i *provide an epidemic response* [1],
ii *bring the pandemic under control* [2],
iii *slow the spread of the virus* [1, 15, 17, 18, 20, 21],
iv *prevent deaths* [16],
v *reduce the reproduction rate of the virus* [16].

The specific goals of digital measures are to:
i *trace spread of the virus* and *identify COVID-19 clusters* [17],
ii *find potential new infections* [30],
iii *register contacts between potential carriers* [17],
iv *deter people from breaking quarantine* [27].
Note that the above goals are *different* (though clearly related). For example, reducing the reproduction rate and preventing deaths are not equivalent, and may require different concrete countermeasures.

Requirements:
1. The efforts must meet *public health needs* best [1, 17].
2. Digital measures should *complement* traditional ones [1, 30].
3. They should be designed to *help the health authorities* [21].

3.1.2. Effectiveness of epidemic response
1. The strategy should be *effective* [1, 3].
2. It should *make a difference* [31].

Risks and threats:
a) *Inaccurate detection* of carriers and infected people due to the limitations of the technology and the underlying model of human interaction [1].
b) *Adverse impact on relaxation of lockdowns* [15].
c) Misguided *assurance* that going out is safe [1].

3.1.3. Information flow requirements
The strategy should:
1. allow *identifying people who might have been exposed* [23].
2. allow *alerting those people* [2, 21, 30, 32].
3. The identification and notification must be *rapid* [2, 23].

3.1.4. Monitoring
The containment strategy should facilitate:
1. *monitoring the state of the pandemic*, e.g., the outbreaks and the spread of the virus [32, 33].
2. *monitoring the behavior of people*, in particular if they are following the rules [34].
3. *monitoring the effectiveness of the strategy* [28].

3.1.5. Tradeoffs
There are *tradeoffs* between effective containment of the epidemic and other concerns, such as *privacy* and protection of *fundamental freedoms* [17, 27, 28, 32, 35]. Thus, the strategy should:
1. *strike the right balance* between different concerns [17].
We will see more detailed tradeoff-related requirements in the subsequent sections.

3.2. Economic and social impact
Most measures to contain the epidemic have a strong social and economic impact (cf. lockdown).

3.2.1. Economic stability
The containment strategy should:
1. minimize the *cost to local economies* and the negative impact on *economic growth* [1, 16].
2. allow for *return to normal economy and society* and make resumption of economic and social activities *safer* [24, 30].

3.2.2. Social and political impact
The containment strategy (and digital measures in particular) should:
1. *ease lockdowns* and *home confinement* [1, 3, 23, 24].
2. minimize adverse impact on *social relationships* and *personal well-being* [1].
3. *prohibit economic and social discrimination* on the basis of information and technology being part of the strategy [1].
4. *protect the communities* that can be harmed by the collection and exploitation of personal data [1]

Risks and threats:
a) *Little knowledge* about social impact of the measures [22].
b) *Discrimination* and creation of *social divides* [1, 36].
c) *Disinformation* and *information abuse* [1, 15].
d) Providing a *false sense of security* [1].
e) *Political manipulation*, creating *social unrest*, and *dishonest competition* by false reports on coronavirus [1].
f) Too much political influence of IT companies on *the decisions of sovereign democratic countries* [17].

3.2.3. Costs, human resources, logistics
Requirements:
1. The *financial cost* of the measures should be minimized [37].
2. Minimization of the involved *human resources* [1, 34].
3. *Timeliness* [37].
4. *Coordination* between different institutions and authorities [26, 38] and establishment of *common standards* [26].

3.3. Ethical and legal aspects
In this section, we look at requirements that aim at the long-term robustness and resilience of the social structure.

3.3.1. Ethical and Legal Requirements}
1. The mitigation strategy must be *ethically justifiable* [2].
2. Measures should be *necessary*, *proportionate*, *legitimate*, *just*, *scientifically valid*, and *time-bound* [2, 15, 34, 36, 39].
3. They should not be *invasive* [27] and must not be done at the expense of *individual civil rights* [20, 22, 36].
4. Means of protection should be *available to anyone* [2].
5. They should be *voluntary* [18, 22].
6. Measures must *comply with legal regulations* [35, 36, 40].
7. *Implementation* and *impact* must also be considered [2, 15].
8. *Impact assessment* is to be *conducted* and *made public* [36].

3.3.2. Risks and threats
a) Serious and long-lasting *harm to fundamental rights and freedoms* [2].
b) Costs of *not devoting resources to something else* [2].
c) Measures that support *extensive physical surveillance* [15].

d) Social costs of *mandatory* use of digital measures, *collecting sensitive information*, and *sharing the data* with the government [23, 27].
e) *Censorship practices* [15].

3.4. Privacy and data protection

Privacy-related issues for COVID-19 mitigation strategies have triggered heated discussion and substantial media coverage.

3.4.1. General privacy requirements

1. The strategy should be designed with *privacy* and *information security* in mind [1, 22, 30].
2. It should be *anonymous* under data protection laws, i.e., it cannot *lead to the identification of an individual* [31].
3. *Information* about users must be *protected at all times* [18].
4. The design should include recommendations for *how back-end systems should be secured*, and identify *vulnerabilities* as well as *unintended consequences* [1].

Risks and threats:
a) Lack of *clear privacy policies* [15, 22, 29].
b) *Exploitation of personal information* by authorities or third parties [15, 29, 41], in particular *live or near-live tracking of users' locations* and *linking sensitive personal information to an individual* [41].
c) *Linking different datasets* at some point in the future [40].
d) Alerts can be *too revealing* [42].
e) Possibility to work out *who is associating with whom* [35].

3.4.2. Data protection and potential misuse of data

Here, the key question is: *What data is collected* and *who is it shared with*? [1, 22] This leads to the following requirements:

1. Clear and reasonable *limits on the data collection types* [1, 18, 26, 27, 30].
2. Limitations on *how the data is used* [22].
3. In particular, the data is to be *used strictly for disease control* and not *shared with law enforcement agencies* [24, 27].
4. Less *state access* and *control* over *user data* [20].
5. Data collection should be *minimized* [22] and based on *informed consent* of the participants [17].
6. Giving access to one's data should be *voluntary* [22].
7. One should have the *right to access their own data* [21, 35].
8. ...and ability to *delete their personal information* [21, 35].
9. For digital measures, the user should be able to *remove the software* and *disable more invasive features* [21].

Risks and threats:
a) Data storage that can be *hacked* and *exploited* [15, 23, 28].
b) *Data breaches* due to insider threats [29].
c) *Function creep* and *state surveillance* [23].
d) *Sharing data* across agencies or *selling* [15, 29].
e) Integration with *commercial services* [15].

3.4.3. Sunsetting and safeguards

Requirements:

1. Measures must be *terminated* as soon as possible [1, 21, 34].
2. Data should be *eventually* or even *periodically destroyed* [1, 21, 22, 30, 34, 35], in particular *when it is no longer needed to help manage the spread of coronavirus* [18].
3. *Transparency* of data collection [22].
4. There should be clear *policies to prevent abuse* [22].
5. Privacy must be backed up with clear lines of *accountability* and processes for *evaluation* and *monitoring* [40].
6. *Judicial oversight* must be provided [1].
7. Safeguards should be backed by *an independent figure* [34].

Risks and threats:
a) Surveillance might *continue* after the pandemic [41].
b) Data can *stay with the government* longer than necessary [34].

3.4.4. Impact of privacy on epidemiological and social concerns

Requirements:

1. People must *get the information they need* to protect themselves and others [42].
2. There must be protections against *economic and social discrimination* based on *information* and *technology* designed to fight the pandemic, in particular w.r.t. communities vulnerable to *collection and exploitation of personal data* [1].
3. Information should be used in such a way that people who fear being judged will not *put other people in danger* [42].

Risks and threats:
a) *Fear of social stigma* [42].
b) Online *judgement* and *ridicule* [42].

3.4.5. Privacy vs. epidemiological efficiency

There is a tradeoff between protecting privacy vs. collecting all the information that can be useful in fighting the epidemic:

- Privacy hinders *making the best possible use of the data*, including *analysis of the population*, *contact matching*, *modeling the network of contacts*, enabling *epidemiological insights* such as *revealing clusters* and *superspreaders*, and providing *advice to people* [23, 24, 35].
- On the other hand, privacy-preserving solutions put users in *more control of their information* and require *no intervention from a third party* [35].

The relationship is not simply antagonistic, though:

- Privacy is instrumental in building *trust*. Conversely, lack of privacy undermines trust, and *hinders the epidemiological*, *economic*, *and social effects of the mitigation activities* [29].

Thus, while it might be necessary to waive users' privacy in the short term to contain the epidemic, one must look for

1. mechanisms such that *exploiting the risks would require significant effort by the attackers for minimal reward* [23].

3.5. User-related aspects

The measures must be adopted in order to make them effective.

3.5.1. User incentives

Goals:

i *High acceptance rate* for the mitigation measures [30].
ii *Creating incentives* and overcoming *incentive problems* for individual people to adopt the strategy [1].

Risks and threats:

a) Lack of *immediate benefits* for the participants [1].
b) Perceived *privacy* and *security risks* [30].
c) Some measures can *divert attention from more important measures*, and *make people less alert* [43].
d) Creating *false sense of security* from the pandemic [33].

3.5.2. Adoption and its impact

Requirements:

1. *Enough people* should *download* and *use* the app to make it *effective* [22, 23, 30, 44]. Note: this requirement is *graded* rather than binary [29, 46].

Risks and threats:

a) Lack of users' *trust* [29, 31], see also the connection between privacy and trust in Section 3.4.5.
b) Authorities' lack of *social knowledge* and *empathy* [32].

3.6. Technological aspects

General requirements:

1. The measures and tools must be *operational* [34, 35].
2. In particular, they should be *compatible* with their environment of implementation [40].
3. Design and implementation should be *transparent* [22, 47].

Specific requirements for digital measures:

1. They should be *compatible with most available devices* [40].
2. Reasonable *use of battery* [40].
3. *Usable interface* [40].
4. *Accurate measurements* of how close two devices are [23].
5. *Cross-border interoperability* [48].
6. Possibility to *verify the code* by the public and experts [47].

3.7. Evaluation and learning for the future

COVID-19 mitigation activities should be rigorously assessed. Their outcomes should be used to extend our knowledge, and better defend ourselves in the future. The main goal here is:

i to use the collected data in order to *develop efficient infection control measures* and *gain insight into the effect of changes to the measures for fighting the virus* [21, 35].

Requirements:

1. A *review* and *exit strategy* should be defined [2].
2. Before implementing the measures, an *institutional assessment*} is needed of their *usefulness*, *effectiveness*, *technological readiness*, *cybersecurity risks and threats to fundamental freedoms and human rights* [3].
3. After the pandemic, there must be *the society's assessment* whether the strategy has been effective and appropriate [42].
4. The *assessments* should be conducted *by an independent body* at *regular intervals* [2].

4. TOWARDS FORMAL SPECIFICATION

Here, we briefly show how the requirements presented in Section 3 can be rewritten in a more formal way. To this end, we use *modal logic for distributed and multi-agent systems* that have been in constant development for over 40 years [7, 49–53]. The reasons for this choice are as follows. First, the logic have been developed to address the dynamics of complex heterogeneous systems that involve interaction between autonomous processes – exactly what we are dealing with here. Secondly, they allow for a natural separation of concerns by using different modalities for different aspects of the system and its participants (knowledge, beliefs, intentions, temporal evolution, strategic planning, social norms, available resources, etc.). To this day, they have been applied in numerous case studies to formalize multi-agent scenarios.

Thirdly, the logic is based on intuitive Kripke-style semantics that interprets the different modalities in a reasonably uniform way. Moreover, models can be visualized as graphs that are easy to explain, and can be scrutinized by non-experts. Fourthly, many relevant requirements can be specified in the propositional variants of MAS logic, i.e., by formulas without quantifiers. This makes reading the formulas somewhat easier. Even more importantly, propositional formulas often allow for decidable model checking with manageable complexity, which gives hope for automated verification. Last but not least, in parallel with the formal framework, the MAS community have been developing model checking tools that can be used to verify some of the requirements against models of the pandemic. We mention some of the tools, and speculate on the possibilities for actual verification at the end of this section.

Note that the following specifications are only *semi*-formal, as we do not fix the models nor give the precise semantics of the logical operators and atomic predicates. We leave that step for the future work.

4.1. Temporal properties

The simplest kind of requirements are those that refer to achievement or maintenance of a particular state of affairs. They can be expressed by formulas of the branching-time logic **CTL*** [49], with path quantifiers E (*there is a path*), A (*for all paths*), and temporal operators $\bigcirc$ (*in the next moment*), $\Diamond$ (*sometime from now on*), $\Box$ (*always from now on*), and U (*until*). For example, the epidemiological goals in Section 3.1 can be tentatively rewritten as the following **CTL***:

(i) $\mathsf{A}\Box(\mathsf{outbreak} \rightarrow \Diamond\mathsf{response})$: for all possible execution paths, if outbreak holds at some point, then response must hold at a later point on the same path. That is, whenever an outbreak occurs, a response will be eventually provided;
(ii) $\mathsf{A}\Diamond\mathsf{controlPandemic}$: the pandemic will be eventually brought under control[1];
(iii) and (v) $\forall n.\,(\mathsf{R0} = \mathsf{n}) \rightarrow \mathsf{A}\Diamond(\mathsf{R0} < \mathsf{n})$: the reproduction rate of the virus will decrease below the current level;
(iv) $\mathsf{A}\Box\neg(\#\mathsf{deaths} > \mathsf{k})$: the number of fatalities will never exceed k, for a reasonably chosen k.

[1] In fact, a better specification is given by $\mathsf{A}\Diamond\mathsf{controlPandemic}$, saying that the pandemic is not only brought, but also kept under control.

The above formulas are supposed to serve as the first formal approximations of the requirements. In actual analysis, they should be iteratively refined, taking into account the desired level of granularity and the variables available in the model.

4.2. Combining temporal and epistemic aspects

Many important properties of multi-agent systems refer to agents' knowledge and its dynamics. In our case, this concerns for example the information flow and monitoring requirements in Sections 3.1.3 and 3.1.4. Such properties can be expressed by the combination of **CTL*** with epistemic operators $K_a\varphi$("*a knows that* φ"). For instance, the information flow requirement (pt 1) in Section 3.1.3 can be formalized as

$$\mathsf{exposed}_i \rightarrow \mathsf{A}\Diamond K_a \mathsf{exposed}_i,$$

where a is the authority supposed to identify vulnerable people. A more faithful transcription can be obtained using the past-time operator $\Diamond^{-1}$ (*sometime in the past*) [54] with

$$\left(\Diamond^{-1}\mathsf{exposed}_i\right) \rightarrow \mathsf{A}\Diamond K_a\left(\Diamond^{-1}\mathsf{exposed}_i\right),$$

saying that if exposed has held at some point in the past, then a will eventually know about it. Likewise, the information flow requirement (Section 3.1.3 pt 2) can be captured by

$$K_a\left(\Diamond^{-1}\mathsf{exposed}_i\right) \rightarrow \mathsf{A}\Diamond K_i\left(\Diamond^{-1}\mathsf{exposed}_i\right),$$

saying that, if a knows that i has been exposed, then i will eventually know about it, too.

Similar temporal-epistemic formulas may be used to express some privacy-related requirements, e.g.,

$$\forall j \neq i.\, \mathsf{A}\Box\left(\neg K_j(x = i) \wedge \neg K_j(x \neq i)\right)$$

tentatively captures the anonymity of person i wrt. the database entry represented by x, see requirement (pt 2) in Section 3.4.1.

4.3. Strategic requirements

Demanding that something must happen on all paths is often too strong. It often suffices that the responsible agent(s) can follow a recipe (formally, a strategy) that guarantees the desirable outcome. To this end, the temporal and epistemic patterns can be refined by replacing path quantifiers A, E with strategic operators $\langle\langle A\rangle\rangle$ of the logic **ATL*** [52, 53], where $\langle\langle A\rangle\rangle\varphi$ says that "*the agents in A have a strategy to bring about* φ". For example, the information flow requirements (Section 3.1.3 pt 1 and pt 2), discussed in the previous section, can be rewritten as

$$\left(\Diamond^{-1}\mathsf{exposed}_i\right) \rightarrow \langle\langle a\rangle\rangle\Diamond K_a\left(\Diamond^{-1}\mathsf{exposed}_i\right),$$
$$K_a\left(\Diamond^{-1}\mathsf{exposed}_i\right) \rightarrow \langle\langle a\rangle\rangle\Diamond\langle\langle i\rangle\rangle\Diamond K_i\left(\Diamond^{-1}\mathsf{exposed}_i\right).$$

The former says that if i has been exposed, then the health authority a has a strategy to eventually realize that. We leave the interpretation of the latter to the interested reader.

Strategic operators are also useful in formalizing the access control properties in Section 3.4.2. For instance, requirement (Section 3.4.2 pt 6) can be formalized by the formula

$$\langle\langle i\rangle\rangle\Diamond\mathsf{access}(\mathsf{a}, \mathsf{data}_\mathsf{i}) \wedge \langle\langle i\rangle\rangle\Box\neg\mathsf{access}(\mathsf{a}, \mathsf{data}_\mathsf{i})$$

expressing that i has a strategy which grants authority a with access to its data, and another strategy that never allows it.

4.4. Time bounds, mental effort, and bounded resources

For some requirements, the temporal and strategic operators should be combined with bounds imposed on the execution time [55, 56], mental complexity [57], and/or resources needed to accomplish the tasks [58, 59]. For example, the identification requirement (Section 3.1.3 pt 1), discussed above, can be refined as:

$$\left(\Diamond^{-1}\mathsf{exposed}_i\right) \rightarrow \langle\langle a\rangle\rangle\Diamond^{t\leq 48h} K_a\left(\Diamond^{-1}\mathsf{exposed}_i\right).$$

That is, the authority a should identify the exposed person in at most 48 hours from the exposure. Similarly, the notification requirement (Section 3.1.3 pt 2) becomes:

$$K_a\left(\Diamond^{-1}\mathsf{exposed}_i\right) \rightarrow \langle\langle a\rangle\rangle\Diamond^{t\leq 48h}\langle\langle i\rangle\rangle\Diamond^{compl\leq 5} K_i\left(\Diamond^{-1}\mathsf{exposed}_i\right),$$

based on the assumption that a should notify i within 1 hour of detecting i's exposure to the virus, and i should have a *simple* strategy (of complexity at most 5) to infer the relevant knowledge from the notification.

4.5. Probabilistic Extensions

Many events have probabilistic execution, e.g., actions may fail with some small probability. Scenarios with probabilistic events can be modeled by variants of Markov decision processes, and their properties can be specified by a probabilistic variant of **CTL*** [60] or **ATL*** [61]. For instance, formula

$$\langle\langle a\rangle\rangle^{P\geq 0.99}\Diamond^{t\leq 1h}\langle\langle i\rangle\rangle^{compl\leq 5}\Diamond K_i\left(\Diamond^{-1}\mathsf{exposed}_i\right),$$

refines the previous specification by demanding that the authority can successfully notify i with probability at least 99%.

4.6. Towards formal verification of mitigation strategies

Ideally, one would like to automatically evaluate COVID-19 strategies with respect to the requirements, and choose the best mitigation policy. A number of model checking tools have been developed over the past 30 years, including Uppaal [12] for temporal and time-bounded properties, MCMAS [11] for temporal-epistemic and strategic specifications, STV [14] for strategic agents with imperfect information, and PRISM [62] for stochastic multi-agent systems. In the future, we plan to use a selection of those tools to formally verify our formulas over micro-level models created to simulate and predict the progress of the pandemic [63–66].

As we already pointed out, different requirements may be in partial conflict. Thus, selecting an optimal mitigation strategy may require solving a multicriterial optimization problem [67–69], e.g., by identifying the Pareto frontier and choosing a criterion to select a point on the frontier.

5. CONCLUSIONS

In this paper, we make the first step towards a systematic analysis of strategies for effective and trustworthy mitigation of the current pandemic. The strategies may incorporate medical, social, economic, as well as technological measures. Consequently, there is a large number of medical, social, economic, and technological requirements that must be taken into account when deciding which strategy to adopt. For computer scientists,

the latter kind of requirements is most natural, which is exactly the pitfall that a computer scientist must avoid. The goals (and acceptability criteria) are much more diverse, and we must consciously choose a solution that satisfies the multiple criteria to a reasonable degree. We suggest that formal methods for MAS provide an excellent framework for that. We also propose a methodology to collect general requirements by mining the public information space (rather than scientific papers which are usually more technical and narrowly focused).

In the future, we would like to study how the technical requirements proposed in research articles refine the general requirements presented here. We also plan to use model checking in multi-agent logic to verify some of the requirements against the existing models of the pandemic.

ACKNOWLEDGEMENTS

The authors acknowledge the support of the Luxembourg National Research Fund (FNR) under the COVID-19 project SmartExit, and the support of the National Centre for Research and Development Poland (NCBR) and the Luxembourg National Research Fund (FNR), under the PolLux/CORE project STV (POLLUX-VII/1/2019).

REFERENCES

[1] A. Soltani, R. Calo, and C. Bergstrom, "Contacttracing apps are not a solution to the COVID-19 crisis," *Brookings Tech Stream*, 27 April 2020. [Online]. Available: https://www.brookings.edu/techstream/inaccurate-and-insecure-why-contact-tracing-apps-could-be-a-disaster/.

[2] J. Morley, J. Cowls, M. Taddeo, and L. Floridi, "Ethical guidelines for COVID-19 tracing apps," *Nat. Comment*, pp. 29–31, 4 June 2020. [Online]. Available: https://www.nature.com/articles/d41586-020-01578-0.

[3] A. Stollmeyer, M. Schaake, and F. Dignum, "The Dutch tracing app 'soap opera' – lessons for Europe," euobserver, 7 May 2020. [Online]. Available: https://euobserver.com/opinion/148265.

[4] G. Weiss, Ed., *Multiagent Systems. A Modern Approach to Distributed Artificial Intelligence*. MIT Press: Cambridge, Mass, 1999.

[5] Y. Shoham and K. Leyton-Brown, *Multiagent Systems – Algorithmic, Game-Theoretic, and Logical Foundations*. Cambridge University Press, 2009.

[6] A. Rao and M. Georgeff, "Modeling rational agents within a BDI-architecture," in *Proceedings of KR*, 1991, pp. 473–484.

[7] M.Wooldridge, *Reasoning about Rational Agents*. MIT Press : Cambridge, Mass, 2000.

[8] M. Dastani, K. Hindriks, and J. Meyer, Eds., *Specification and Verification of Multi-Agent Systems*. Springer, 2010.

[9] W. Jamroga, *Logical Methods for Specification and Verification of Multi-Agent Systems*. ICS PAS, 2015.

[10] W. Jamroga, D. Mestel, P.B. Rønne, P.Y.A. Ryan, and M. Skrobot, "A survey of requirements for COVID-19 mitigation strategies. Part I: newspaper clips," *CoRR*, vol. abs/2011.07887, 2020.

[11] A. Lomuscio, H. Qu, and F. Raimondi, "MCMAS: An open-source model checker for the verification of multiagent systems," *Int. J. Software Tools Technol. Trans.*, vol. 19, no. 1, pp. 9–30, 2017.

[12] G. Behrmann, A. David, and K. Larsen, "A tutorial on UPPAAL," in *Formal Methods for the Design of Real-Time Systems: SFM-RT*, ser. LNCS, no. 3185. Springer, 2004, pp. 200–236.

[13] G. Kant, A. Laarman, J. Meijer, J. van de Pol, S. Blom, and T. van Dijk, "LTSmin: High-performance languageindependent model checking," in *Proceedings of TACAS*, ser. Lecture Notes in Computer Science, vol. 9035. Springer, 2015, pp. 692–707.

[14] D. Kurpiewski, W. Jamroga, and M. Knapik, "STV: Model checking for strategies under imperfect information," in *Proceedings of AAMAS*. IFAAMAS, 2019, pp. 2372–2374.

[15] S. Woodhams, "COVID-19 digital rights tracker," Top10VPN, 10 June 2020. [Online]. Available: https://www.top10vpn.com/research/covid-19-digital-rights-tracker/.

[16] AFP, "Major finding: Lockdowns averted 3 million deaths in 11 European nations: study," *RTL Today*, 9 June 2020. [Online]. Available: https://today.rtl.lu/news/science-and-environment/a/1530963.html.

[17] I. Ilves, "Why are Google and Apple dictating how European democracies fight coronavirus?" *The Guardian*, 16 June 2020. [Online]. Available: https://www.theguardian.com/commentisfree/2020/jun/16/google-apple-dictating-european-democracies-coronavirus.

[18] "NHS COVID-19: the new contact-tracing app from the NHS," *NCSC*, 14 May 2020. [Online]. Available: https://www.ncsc.gov.uk/information/nhs-covid-19-app-explainer.

[19] J. Steinhauer and A. Goodnough, "Contact tracing is failing in many states. Here's why." *New York Times*, 5 October 2020. [Online]. Available: https://www.nytimes.com/2020/07/31/health/covid-contact-tracing-tests.html.

[20] S. Bicheno, "Unlike France, Germany decides to do smartphone contact tracing the Apple/Google way," *telecoms.com*, 27 April 2020. [Online]. Available: https://telecoms.com/503931/unlike-france-germany-de cides-to-do-smartphone-contact-tracing-the-apple-goo gle-way/.

[21] "Together we can fight coronavirus — Smittestopp," helsenorge, 28 April 2020. [Online]. Available: https://helsenorge.no/coronavirus/smittestopp?redirect=false.

[22] P.H. O'Neill, T. Ryan-Mosley, and B. Johnson, "A flood of coronavirus apps are tracking us. now it's time to keep track of them," *MIT Technol. Rev.*, 7 May 2020. [Online]. Available: https://www.technologyreview.com/2020/05/07/1000961/launching-mittr-covid-tracing-tracker/.

[23] M. Zastrow, "Coronavirus contact-tracing apps: can they slow the spread of COVID-19?" *Nature (Technol. Feature)*, 19 May 2020. [Online]. Available: https://www.nature.com/articles/d41586-020-01514-2.

[24] J. Taylor, "How did the Covidsafe app go from being vital to almost irrelevant?" *The Guardian*, 23 May 2020. [Online]. Available: https://www.theguardian.com/world/2020/may/24/how-did-the-covidsafe-app-go-from-being-vital-to-almost-irrelevant.

[25] D. Robertson, "Transparency key to uptake of coronavirus tracing app," *RMIT news*, 27-April 2020. [Online]. Available: https://www.rmit.edu.au/news/all-news/2020/april/transparency-key-to-uptake-of-coronavirus-traci ng-app.

[26] D. Tahir and C. Lima, "Google and Apple's rules for virus tracking apps sow division among states," *Politico*, 10 June 2020. [Online]. Available: https://www.politico.com/news/2020/06/10/google-and-apples-rules-for-virus-tracking-apps-sow-division-among-states-312199.

[27] A. Clarance, "Aarogya Setu: Why India's Covid-19 contact tracing app is controversial," *BBC News*, 15 May 2020. [Online]. Available: https://www.bbc.com/news/world-asia-india-52659520.

[28] J. Davies, "UK snubs Google and Apple privacy warning for contact tracing app," *telecoms.com*, 28 April 2020. [Online]. Available: https://telecoms.com/503967/uk-s nubs-google-and-apple-privacy-warning-for-contact-tr acing-app/.

[29] A. Eisenberg, "Privacy fears threaten New York City's coronavirus tracing efforts," *Politico*, 4 June 2020. [Online]. Available: https://www.politico.com/states/new-york/albany/story/2020/06/04/privacy-fears-threaten-new-york-citys-coronavirus-tracing-efforts-1290657.

[30] C. Timberg, "Most Americans are not willing or able to use an app tracking coronavirus infections. that's a problem for Big Tech's plan to slow the pandemic," *Washington Post*, 29 April 2020. [Online]. Available: https://www.washingtonpost.com/technology/2020/04/ 29/most-americans-are-not-willing-or-able-use-an-app-tracking-coronavirus-infections-thats-problem-big-tec hs-plan-slow-pandemic/.

[31] M. Burgess, "Just how anonymous is the NHS Covid-19 contact tracing app?" Wired, 12 May 2020. [Online]. Available: https://www.wired.co.uk/article/nhs-covid-app-data-anonymous.

[32] "Getting it right: States struggle with contact tracing push," *Politico*, 17 May 2020. [Online]. Available: https://www.politico.com/news/2020/05/17/privacy-coronavirus-tracing-261369.

[33] S.L. Frasier, "Coronavirus antibody tests have a mathematical pitfall," *Sci. Am.*, 1 July 2020. [Online]. Available: https://www.scientificamerican.com/article/coronavirus-antibody-tests-have-a-mathematical-pitfall/.

[34] M. Scott and Z. Wanat, "Poland's coronavirus app offers playbook for other governments," Politico, 2 April 2020. [Online]. Available: https://www.politico.eu/article/poland-coronavirus-app-offers-playbook-for-other-governments/.

[35] K. McCarthy, "UK finds itself almost alone with centralized virus contact-tracing app that probably won't work well, asks for your location, may be illegal," *The Register*, 5 May 2020. [Online]. Available: https://www.theregister.com/2020/05/05/uk_coronavirus_app/.

[36] "Legal advice on smartphone contact tracing published," matrix chambers, 3 May 2020. [Online]. Available: https://www.matrixlaw.co.uk/news/legal-advice-on-smartphone-contact-tracing-published/.

[37] A. Hern, "UK abandons contact-tracing app for Apple and Google model," *The Guardian*, 18 June 2020. [Online]. Available: https://www.theguardian.com/world/2020/jun/18/uk-poised-to-abandon-coronavirus-app-in-favour-of-apple-and-google-models.

[38] "Coronavirus: Member States agree on an interoperability solution for mobile tracing and warning apps," European Commission – *Press release*, 16 June 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/news/coronavirus-member-states-agree-interoperability-solution-mobile-tracing-and-warning-apps.

[39] A. Oslo, "Norway suspends virus-tracing app due to privacy concerns," *The Guardian*, 15 June 2020. [Online]. Available: https://www.theguardian.com/world/2020/jun/15/norway-suspends-virus-tracing-app-due-to-privacy-concerns.

[40] S. Wodinsky, "The UK's contact-tracing app breaks the UK's own privacy laws (and is just plain broken)," *Gizmodo*, 13 May 2020. [Online]. Available: https://gizmodo.com/the-uk-s-contact-tracing-app-breaks-the-uk-s-own-privac-1843439962.

[41] R. Garthwaite and I. Anderson, "Coronavirus: Alarm over 'invasive' Kuwait and Bahrain contact-tracing apps," *BBC News*, 16 June 2020. [Online]. Available: https://www.bbc.com/news/world-middle-east-53052395.

[42] "Coronavirus privacy: Are South Korea's alerts too revealing?" *BBC News*, 5 March 2020. [Online]. Available: https://www.bbc.com/news/amp/world-asia-51733145.

[43] K. Szymielewicz, A. Obem, and T. Zieliński, "Jak Polska walczy z koronawirusem i dlaczego aplikacja nas przed nim nie ochroni [How Poland fights the corona, and why the app won't protect us]?" *Panoptykon*, 5 May 2020. [Online]. Available: https://panoptykon.org/protego-safe-ryzyka.

[44] J.-M. Bezat, "L'application StopCovid, activée seulement par 2% de la population, connaît des débuts décevants," *Le Monde*, 10 June 2020. [Online]. Available: https://www.lemonde.fr/pixels/article/2020/06/10/l-application-stopcovid-connait-des-debuts-decevants_6042404_4408996.html.

[45] P.H. O'Neill, "No, coronavirus apps don't need 60% adoption to be effective," *MIT Technol. Rev.*, 5 June 2020. [Online]. Available: https://www.technologyreview.com/2020/06/05/1002775/covid-apps-effective-at-less-than-60-percent-download/.

[46] R. Hinch *et al.*, "Effective configurations of a digital contact tracing app: A report to NHSX," Oxford University, Tech. Rep., 2020. [Online]. Available: https://github.com/BDI-pathogens/covid-19_instant_tracing/blob/master/Report-EffectiveConfigurationsofaDigitalContactTracingApp.pdf.

[47] "Corona-app soll open source werden," *Süddeutsche Zeitung*, 6 May 2020. [Online]. Available: https://www.sueddeutsche.de/digital/corona-app-tracing-open-source-1.4899711.

[48] "Cybernetica proposes privacy-preserving decentralised architecture for COVID-19 mobile application for Estonia," *Cybernetica*, 6 May 2020. [Online]. Available: https://cyber.ee/news/2020/05-06/.

[49] E. Emerson, "Temporal and modal logic," in *Handbook of Theoretical Computer Science*, J. van Leeuwen, Ed. Elsevier, 1990, vol. B, pp. 995–1072.

[50] R. Fagin, J.Y. Halpern, Y. Moses, and M.Y. Vardi, *Reasoning about Knowledge*. MIT Press, 1995.

[51] J. Broersen, M. Dastani, Z. Huang, and L. van der Torre, "The BOID architecture: conflicts between beliefs, obligations, intentions and desires," in *Proceedings of the Fifth International Conference on Autonomous Agents*. ACM Press, 2001, pp. 9–16.

[52] R. Alur, T.A. Henzinger, and O. Kupferman, "Alternating-time Temporal Logic," *J. ACM*, vol. 49, pp. 672–713, 2002.

[53] N. Bulling, V. Goranko, andW. Jamroga, "Logics for reasoning about strategic abilities in multi-player games," in *Models of Strategic Reasoning. Logics, Games, and Communities*, ser. Lecture Notes in Computer Science. Springer, 2015, vol. 8972, pp. 93–136.

[54] F. Laroussinie and P. Schnoebelen, "A hierarchy of temporal logics with past," *Theoretical Computer Science*, vol. 148, no. 2, pp. 303–324, 1995.

[55] W. Penczek and A. Polrola, *Advances in Verification of Time Petri Nets and Timed Automata: A Temporal Logic Approach*, ser. Studies in Computational Intelligence. Springer, 2006, vol. 20.

[56] M. Knapik, É. André, L. Petrucci, W. Jamroga, and W. Penczek, "Timed ATL: forget memory, just count," *J. Artif. Intell.*, vol. 66, pp. 197–223, 2019.

[57] W. Jamroga, V. Malvone, and A. Murano, "Natural strategic ability," *Artif. Intell.*, vol. 277, 2019.

[58] N. Alechina, B. Logan, H. Nguyen, and A. Rakib, "Resource-bounded alternating-time temporal logic," in *Proceedings of International Joint Conference on Autonomous Agents and Multiagent Systems (AAMAS)*, 2010, pp. 481–488.

[59] N. Bulling and B. Farwer, "Expressing properties of resource-bounded systems: The logics RTL* and RTL," in *Proceedings of CLIMA*, ser. Lecture Notes in Computer Science, vol. 6214, 2010, pp. 22–45.

[60] C. Baier and M. Z. Kwiatkowska, "Model checking for a probabilistic branching time logic with fairness," *Distributed Comput.*, vol. 11, no. 3, pp. 125–155, 1998.

[61] T. Chen, V. Forejt, M. Kwiatkowska, D. Parker, and A. Simaitis, "PRISM-games: A model checker for stochastic multi-player games," in *Proceedings of TACAS*, ser. Lecture Notes in Computer Science, vol. 7795. Springer, 2013, pp. 185–191.

[62] M. Kwiatkowska, G. Norman, and D. Parker, "PRISM: probabilistic symbolic model checker," in *Proceedings of TOOLS*, ser. Lecture Notes in Computer Science, vol. 2324. Springer, 2002, pp. 200–204.

[63] N.M. Ferguson *et al.*, "Impact of non-pharmaceutical interventions (NPIs) to reduce COVID-19 mortality and healthcare demand," Imperial College London, Tech. Rep. 9 (16–03–2020), 2020.

[64] B. Adamik *et al.*, "Estimation of the severeness rate, death rate, household attack rate and the total number of COVID-19 cases based on 16 115 Polish surveillance records," *Prepr. Lancet*, 2020.

[65] W. Bock *et al.*, "Mitigation and herd immunity strategy for COVID-19 is likely to fail," *medRxiv*, 2020.

[66] R. McCabe *et al.*, "Modelling ICU capacity under different epidemiological scenarios of the COVID-19 pandemic in three western European countries," Imperial College London, Tech. Rep. 36 (16–11–2020), 2020.

[67] S. Zionts, "A multiple criteria method for choosing among discrete alternatives," *Eur. J. Oper. Res.*, vol. 7, no. 2, pp. 143–147, 1981, fourth EURO III Special Issue.

[68] Y. Collette and P. Siarry, *Multiobjective Optimization: Principles and Case Studies*. Springer, 2004.

[69] R. Radulescu, P. Mannion, D. M. Roijers, and A. Nowé, "Multi-objective multi-agent decision making: a utilitybased analysis and survey," *Auton. Agents Multi-Agent Syst.*, vol. 34, no. 1, p. 10, 2020.