Chapter 1

Risk Propagation

Risk propagation is a message-passing algorithm that estimates an individual's infection risk by considering their demographics, symptoms, diagnosis, and contact with others. Formally, a *risk score* s_t is a timestamped infection probability where $s \in [0, 1]$ and $t \in \mathbb{N}$ is the time of its computation. Thus, an individual with a high risk score is likely to test positive for the infection and poses a significant health risk to others. There are two types of risk scores: *symptom scores*, or prior infection probabilities, which account for an individual's demographics, symptoms, and diagnosis (Menni et al., 2020); and *exposure scores*, or posterior infection probabilities, which incorporate the risk of direct and indirect contact with others.

Given their recent risk scores and contacts, an individual's exposure score is derived by marginalizing over the joint infection probability distribution. Naively computing this marginalization scales exponentially with the number of variables (i.e., individuals). To circumvent this intractability, the joint distribution is modeled as a factor graph, and an efficient message-passing procedure is employed to compute the marginal probabilities with a time complexity that scales linearly in the number of factor nodes (i.e., contacts).

Let $G = (X, F, E)$ be a *factor graph* where X is the set of variable nodes, F is the set of factor nodes, and E is the set of edges incident between them (Kschischang et al., 2001).

A *variable node* $x : \Omega \to \{0, 1\}$ is a random variable that represents the infection status of an individual, where the sample space is $\Omega = \{\textit{healthy}, \textit{infected}\}$ and

$$x(\omega) = \begin{cases} 0 & \text{if } \omega = \textit{healthy} \\ 1 & \text{if } \omega = \textit{infected}. \end{cases}$$

Thus, $p_t(x_i) = s_t$ is a risk score of the i-th individual.

A *factor node* $f : X \times X \to [0, 1]$ defines the transmission of infection risk between two contacts. Specifically, contact between the i-th and j-th individual is represented by the factor node $f(x_i, x_j) = f_{ij}$, which is adjacent to the variable nodes x_i, x_j. This work and Ayday et al. (2021) assume risk transmission is a symmetric function, $f_{ij} = f_{ji}$. However, it may be extended to account for an individual's susceptibility and transmissibility such that $f_{ij} \neq f_{ji}$. Figure 1.1 depicts a factor graph that reflects the domain constraints.

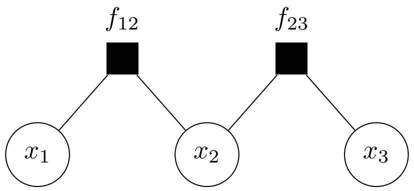

Figure 1.1: A factor graph of 3 variable nodes and 2 factor nodes.

1.1 Synchronous Risk Propagation

Ayday et al. (2021) first proposed risk propagation as a synchronous, iterative message-passing algorithm that uses the factor graph to compute exposure scores. The first input to Risk-Propagation is the set family S, where

$$S_i = \{\, s_t \mid \tau - t < T_s \,\} \in S \tag{1.1}$$

is the set of recent risk scores of the i-th individual. The second input to Risk-Propagation is the contact set

$$C = \{\, (i, j, t) \mid i \neq j, \tau - t < T_c \,\} \tag{1.2}$$

such that (i, j, t) is the *most recent* contact between the i-th and j-th individual that occurred from time t until at least time $t+\delta$, where $\delta \in \mathbb{N}$ is the *minimum contact duration*[1]. Naturally, risk scores and contacts have finite relevance, so (1.1) and (1.2) are constrained by the *risk score expiry* $T_s \in \mathbb{N}$ and the *contact expiry* $T_c \in \mathbb{N}$, respectively. The *reference time* $\tau \in \mathbb{N}$ defines the relevance of the inputs and is assumed to be the time at which Risk-Propagation is invoked. For notational simplicity in Risk-Propagation, let X be a set. Then $\max X = 0$ if $X = \emptyset$.

[1] While Ayday et al. (2021) require contact over a δ-contiguous period of time, the Centers for Disease Control and Prevention (2021) account for contact over a 24-hour period.

1.1.1 Variable Messages

The current exposure score of the i-th individual is defined as $\max S_i$. Hence, a *variable message* $\mu_{ij}^{(n)}$ from the variable node x_i to the factor node f_{ij} during the n-th iteration is the set of maximal risk scores $R_i^{(n-1)}$ from the previous $n-1$ iterations that were not derived by f_{ij}. In this way, risk propagation is reminiscent of the max-sum algorithm; however, risk propagation aims to maximize *individual* marginal probabilities rather than the joint distribution (Bishop, 2006, pp. 411–415).

1.1.2 Factor Messages

A *factor message* $\lambda_{ij}^{(n)}$ from the factor node f_{ij} to the variable node x_j during the n-th iteration is an exposure score of the j-th individual that is based on interacting with those at most $n-1$ degrees separated from the i-th individual. This population is defined by the subgraph induced in G by

$$\{\, v \in X \cap F \setminus \{x_j, f_{ij}\} \mid d(x_i, v) \leq 2(n-1) \,\},$$

where $d(u,v)$ is the distance between the nodes u, v. The computation of a factor message assumes the following.

1. Contacts have a nondecreasing effect on an individual's exposure score.
2. A risk score s_t is *relevant* to the contact (i, j, t_{ij}) if $t < t_{ij} + \beta$, where $\beta \in \mathbb{N}$ is a *time buffer* that accounts for the incubation period, along with the delayed reporting of symptom scores and contacts. The expression

$t_{ij} + \beta$ is called the *buffered contact time*.

3. Risk transmission between contacts is incomplete. Thus, a risk score decays exponentially along its transmission path in G at a rate of $\log \alpha$, where $\alpha \in (0, 1)$ is the *transmission rate*.

To summarize, a factor message $\lambda_{ij}^{(n)}$ is the maximum relevant risk score in the variable message $\mu_{ij}^{(n)}$ (or 0) that is scaled by the transmission rate α.

Ayday et al. (2021) assume that the contact set C may contain (1) multiple contacts between the same two individuals and (2) *invalid* contacts, or those lasting less than δ time. However, these assumptions introduce unnecessary complexity. Regarding assumption 1, suppose the i-th and j-th individual come into contact m times such that $t_k < t_\ell$ for $1 \leq k < \ell \leq m$. Let $\mathit{\Lambda}_k$ be the set of relevant risk scores, according to the contact time t_k, where

$$\mathit{\Lambda}_k = \{\, \alpha s_t \mid s_t \in \mu_{ij}^{(n)}, t < t_k + \beta \,\} .$$

Then $\mathit{\Lambda}_k \subseteq \mathit{\Lambda}_\ell$ if and only if $\max \mathit{\Lambda}_k \leq \max \mathit{\Lambda}_\ell$. Therefore, only the most recent contact time t_m is required to compute the factor message $\lambda_{ij}^{(n)}$. With respect to assumption 2, there are two possibilities.

1. If an individual has at least one valid contact, then their exposure score is computed over the subgraph induced in G by their contacts that define the neighborhood N_i of the variable node x_i.

2. If an individual has no valid contacts, then their exposure score is $\max S_i$ or 0, if all of their previously computed risk scores have expired.

In either case, a set C containing only valid contacts implies fewer factor nodes and edges in the factor graph G. Consequently, the complexity of Risk-Propagation is reduced by a constant factor since fewer messages must be computed.

1.1.3 Termination

To detect convergence, the normed difference between the current and previous exposure scores is compared to the threshold $\epsilon \in \mathbb{R}$. Note that $\mathbf{r}^{(n)}$ is the vector of exposure scores in the the n-th iteration such that $r_i^{(n)}$ is the i-th component of $\mathbf{r}^{(n)}$. The ℓ^1 and ℓ^∞ norms are sensible choices for detecting convergence. Ayday et al. (2021) use the ℓ^1 norm, which ensures that an individual's exposure score changed by at most ϵ after the penultimate iteration.

```
Risk-Propagation$(S, C)$
$(X, F, E) \leftarrow$ Create-Factor-Graph$(C)$
$n \leftarrow 1$
for each $x_i \in X$
    $R_i^{(n-1)} \leftarrow$ top $K$ of $S_i$
    $r_i^{(n-1)} \leftarrow \max R_i^{(n-1)}$
    $r_i^{(n)} \leftarrow \infty$
while $\|\mathbf{r}^{(n)} - \mathbf{r}^{(n-1)}\| > \epsilon$
    for each $\{x_i, f_{ij}\} \in E$
        $\mu_{ij}^{(n)} \leftarrow R_i^{(n-1)} \setminus \{\, \lambda_{ji}^{(k)} \mid k \in [1 \mathinner{..} n-1] \,\}$
    for each $\{x_i, f_{ij}\} \in E$
        $\lambda_{ij}^{(n)} \leftarrow \max \{\, \alpha s_t \mid s_t \in \mu_{ij}^{(n)}, t < t_{ij} + \beta \,\}$
    for each $x_i \in X$
        $R_i^{(n)} \leftarrow$ top $K$ of $\{\, \lambda_{ji}^{(n)} \mid f_{ij} \in N_i \,\}$
    for each $x_i \in X$
        $r_i^{(n-1)} \leftarrow r_i^{(n)}$
        $r_i^{(n)} \leftarrow \max R_i^{(n)}$
    $n \leftarrow n + 1$
return $\mathbf{r}^{(n)}$
```

1.2 Asynchronous Risk Propagation

While straightforward to specify, Risk-Propagation, is not a viable implementation for real-world application, because it is an *offline algorithm* that requires all individuals' recent contacts and risk scores to run. As Ayday et al.

(2021) note, the centralization of health and contact data is not privacy preserving. An offline design is also computational inefficient and risks human safety. Specifically, most exposure scores may not change across invocations of Risk-Propagation, which implies communication overhead and computational redundancy. As a mitigation, Ayday et al. (2020) suggest running Risk-Propagation only once or twice daily. However, this causes substantial delay in reporting to individuals their exposure scores; and in the face of a pandemic, timely information is essential for individual and collective health.

To address the privacy limitations of Risk-Propagation, Ayday et al. (2021) propose decentralizing the factor graph such that the processing entity (e.g., mobile device or "personal cloud") associated with the i-th individual maintains the state of the i-th variable node and its neighboring factor nodes. But for real-world application, the proposal leaves key questions unanswered:

1. Is message passing synchronous or asynchronous?
2. How does message passing terminate?
3. Are any optimizations utilized to reduce communication cost?
4. How do processing entities exchange messages over the network?
5. How private is decentralized risk propagation?

The only purpose of a factor node is to compute and relay messages between variable vertices. Thus, one-mode projection onto the variable vertices can be applied such that variable vertices $x_i, x_j \in X$ are adjacent if the factor node $f_{ij} \in F$ exists (Zhou et al., 2007). Figure 1.2 shows the modified topology.

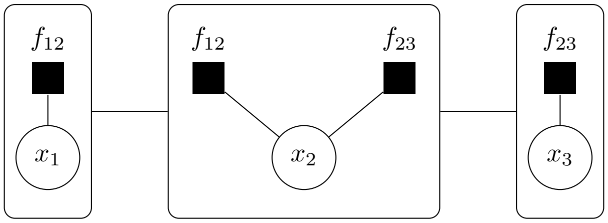

Figure 1.2: One-mode projection onto the variable nodes in Figure 1.1.

To send a message to variable node x_i, variable node x_j applies the computation associated with the factor node f_{ij}. This modification differs from the distributed extension of risk propagation (Ayday et al., 2021) in that we do not create duplicate factor vertices and messages in each user's PDS. By storing the contact time between users on the edge incident to their variable vertices, this modified topology is identical to the *contact-sequence* representation of a *contact network*, a kind of *temporal network* in which a node represents a person and an edge indicates that two persons came in contact:

$$\{ (u, v, t) \mid u, v \in V; u \neq v; t \in \mathbb{N} \}, \tag{1.3}$$

where a triple (u, v, t) is called a *contact* (Holme and Saramäki, 2012). Specific to risk propagation, t is the time at which users u and v *most recently* came in contact (see Section 1.2).

The usage of a temporal network in this work differs from its typical usage in epidemiology which focuses on modeling and analyzing the spreading dynamics of disease (Craft, 2015; Danon et al., 2011; Koher et al., 2019; Lokhov et al., 2014; Riolo et al., 2001; Zino and Cao, 2021; **?**). In contrast, this work uses a temporal network to infer a user's MPPI. As a result, Section 1.2.3

extends temporal reachability to account for both the message-passing semantics and temporal dynamics of the network. As noted by Holme and Saramäki (2012), the transmission graph provided by Riolo et al. (2001) "cannot handle edges where one node manages to not catch the disease." Notably, the usage of a temporal network in this work allows for such cases by modeling the possibility of infection as a continuous outcome. Factor graphs are useful for decomposing complex probability distributions and allowing for efficient inference algorithms.

However, as with risk propagation, and generally any application of a factor graph in which the variable vertices represent entities of interest (i.e., of which the marginal probability of a variable is desired), applying one-mode projection is a .

1.2.1 Actor System

As a distributed algorithm, risk propagation is specified from the perspective of an *actor*. Some variation exists on exactly how actor behavior is defined (Agha, 1985; **?**). Perhaps the simplest definition is that the *behavior of an actor* is both its *interface* (i.e., the types of messages it can receive) and *state* (i.e., the internal data it uses to process messages) (**?**). An *actor system*[2] is defined as the set of actors it contains and the set of unprocessed messages[3] in the actor mailboxes. An expanded definition of an actor system also includes a *local states function* that maps mail addresses to behaviors, the set of *receptionist*

[2] This is technically referred to as an *actor system configuration*.

[3] Formally, a *message* is called a *task* and is defined by a *tag*, a unique identifier; a *target*, the mail address to which the message is delivered; and a *communication*, the message content (Agha, 1985).

actors that can receive communication that is external to the actor system, and the set of *external actors* that exist outside of the actor system (Agha, 1985). Practically, a local states function is unnecessary to specify, so the narrower definition of an actor system is used. The remainder of this section describes the components of the ShareTrace actor system.

1.2.2 Actor Behavior

Each individual corresponds to an actor that participates in the message-passing protocol of risk propagation. Herein, the user of an actor will only be referred to as an *actor*. The following variant of the concurrent, object-oriented actor model is assumed to define actor behavior (Agha, 1985).

- An actor follows the *active object pattern* (Lavender and Schmidt, 1996; **?**) and the *Isolated Turn Principle* (**?**). Specifically, the state change of an actor is carried out by instance- variable assignment, instead of the canonical BECOME primitive that provides a functional construct for pipelining actor behavior replacement (Agha, 1985). The interface of an actor is fixed in risk propagation, so the more general semantics of BECOME is unnecessary.

- The term "name" (Agha, 1985; **?**) is preferred over "mail address" (Agha, 1985) to refer to the sender of a message. Generally, the mail address that is included in a message need not correspond to the actor that sent it. Risk propagation, however, requires this actor is identified in a risk score message. Therefore, to emphasize this requirement, "name" is used to refer to both the identity of an actor and its mail address.

- An actor is allowed to include a loop with finite iteration in its behavior definition; this is traditionally prohibited in the actor model (Agha, 1985).
- The behavior definition is implied by all procedures that take as input an actor.

The CREATE-ACTOR operation initializes an actor (Agha, 1985). An actor a has the following attributes.

- $a.exposure$: the current exposure score of the individual that this actor represents. This attribute is either a symptom score, a risk score sent by another actor, or the null risk score (see NULL-RISK-SCORE).
- $a.contacts$: a *dictionary* (Appendix B) of contacts. In the context of an actor, a contact is a *proxy* (Gamma et al., 1995) of the actor that represents an individual with which the individual represented by this actor was physically proximal. That is, if the i-th individual interacted with the j-th individual, then $a_i.contacts$ contains a contact c such that $c.key = c.name$ is a name of the j-th actor and $c.t$ is the most recent time of contact. This attribute extends the concept of *actor acquaintances* (Agha, 1985; Hewitt, 1977; Hewitt and Baker, 1977) to be time-varying.
- $a.scores$: a dictionary of exposure scores, such that $s.key$ for an exposure score s is the time interval during which $a.exposure = s$. The null risk score is returned for queries in which the dictionary does not contain

a risk score with a key that intersects with the given query interval. Figure 1.3 depicts a hypothetical step function that *a.scores* represents.

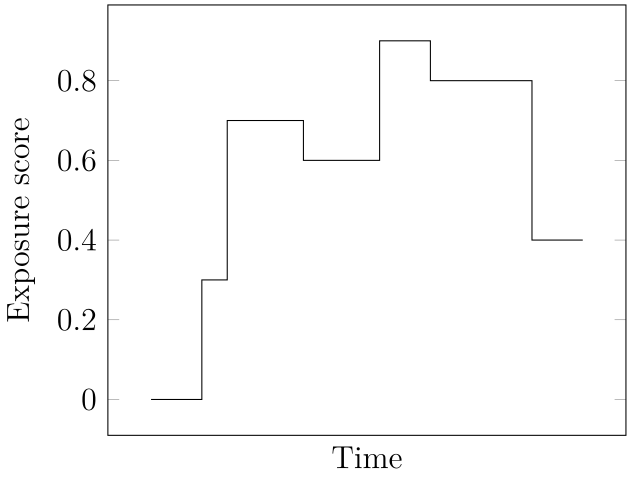

Figure 1.3: Historical exposure scores of an actor.

```
Null-Risk-Score
    $s.value \leftarrow 0$
    $s.t \leftarrow 0$
    $s.sender \leftarrow$ NIL
    return $s$
```

```
Create-Actor
    $a.contacts \leftarrow \emptyset$
    $a.scores \leftarrow \emptyset$
    $a.exposure \leftarrow$ Null-Risk-Score
    return $a$
```

Note that Create-Actor does not specify a name for the actor. This allows the actor to have multiple names and for them to be specified "out-of-band."

The interface of an actor is primarily defined by two types of messages: contacts and risk scores. As with Section 1.1, contacts and risk scores have finite relevance. Let the *time-to-live* (TTL) of a message be the remaining time of its relevance. The reference time τ is assumed to be the current time.

```
Risk-Score-Ttl($s$)
    return $T_s - (\tau - s.t)$
```

```
Contact-Ttl($c$)
    return $T_c - (\tau - c.t)$
```

The Handle-Risk-Score operation defines the actions an actor performs upon receiving a risk score. The key initially associated with the risk score is the time interval for which it is relevant. For the dictionary $a.scores$, Merge preserves the mapping invariant defined above such that risk scores are ordered first by value and then by time. Thus, $s.key \subseteq [s.t, s.t + T_s)$ for all exposure scores in $a.scores$. The Update-Exposure-Score operation describes how $a.exposure$ is updated. The dictionary $a.contacts$ is assumed to only contain unexpired contacts. Additional context is needed before specifying Apply-Risk-Score in detail. For now, it is sufficient to know that the operation uses the risk score to update the state of a contact.

```
Handle-Risk-Score($a, s$)
1: if Risk-Score-Ttl($s$) $> 0$
2:     $s.key \leftarrow [s.t, s.t + T_s)$
3:     Merge($a.scores, s$)
4:     Update-Exposure-Score($a, s$)
5:     for each $c \in a.contacts$
6:         Apply-Risk-Score($a, c, s$)
```

```
Update-Exposure-Score($a, s$)
1: if $a.exposure.value < s.value$
2:     $a.exposure \leftarrow s$
3: else if Risk-Score-Ttl($a.exposure$) $\leq 0$
4:     $a.exposure \leftarrow$ Maximum($a.scores$)
```

For the moment, assume that Apply-Risk-Score is equivalent to computing a factor message (see Section 1.1). Line 2 indicates that the risk score s is copied and updated.

```
Apply-Risk-Score($a, c, s$)
1: if $c.t + \beta > s.t$
2:     $s'.value \leftarrow \alpha \cdot s.value$
3:     Send($c.name, s'$)
```

The problem with Apply-Risk-Score is that it causes risk scores to propagate *ad infinitum*. For asynchronous risk propagation to be scalable and cost-efficient, actors should only send risk scores that offer new information to other actors. Unlike Risk-Propagation, a global convergence test is not available to terminate message passing, so it is necessary to define a local condition that determines if a risk score should be sent to another actor.

The objective of sending a risk score to another actor is to update its exposure score. Based on Handle-Risk-Score, it is only necessary to send an actor risk scores with values greater than its current exposure score. However, an actor is only privy to the risk scores that it sends. Thus, an actor can associate a *send threshold* for a contact that must be exceeded for a risk score to be sent to the target actor. To permit a trade-off between accuracy and efficiency of asynchronous risk propagation, let the *send coefficient* $\gamma \in \mathbb{R}$ be a scaling factor that is applied to a risk score upon setting the send threshold.

```
Set-Send-Threshold($c, s$)
  $s'.value \leftarrow \gamma \cdot s.value$
  $c.threshold \leftarrow s'$
```

Below is the definition of Apply-Risk-Score that incorporates this new aspect of message passing. Assuming a finite number of actors, a positive send coefficient guarantees that a risk score has finite propagation.

```
Apply-Risk-Score($a, c, s$)
  if $c.threshold.value < s.value$ and $c.t + \beta > s.t$
      $s'.value \leftarrow \alpha \cdot s.value$
      Set-Send-Threshold($c, s'$)
      Send($c.name, s'$)
```

The Set-Send-Threshold operation defines *how* the send threshold is updated, but not *when* it should be updated. The Update-Send-Threshold operation encapsulates this update behavior. The latter predicate of Line 1 stems from the fact that the send threshold is a risk score and thus subject to expiry. The former predicate is more subtle and will be revisited shortly. The Maximum-Older-Than is the same as Maximum with the additional restriction that the interval key intersects with the query interval $(-\infty, c.t + \beta)$. In this way, the returned risk score is always relevant to the contact. As with Apply-Risk-Score, the risk score retrieved from *a.scores* is also scaled by the transmission rate and set as the new send threshold.

```
Update-Send-Threshold($a, c$)
1: if $c.threshold.value > 0$ and Risk-Score-Ttl($c.threshold$) $\leq 0$
2:     $s \leftarrow$ Maximum-Older-Than($a.scores, c.t + \beta$)
3:     $s'.value \leftarrow \alpha \cdot s.value$
4:     Set-Send-Threshold($c, s'$)
```

The Update-Send-Threshold is invoked during Apply-Risk-Score, so another modification to the operation is defined below.

```
Apply-Risk-Score($a, c, s$)
1: Update-Send-Threshold($a, c$)
2: if $c.threshold.value < s.value$ and $c.t + \beta > s.t$
3:     $s'.value \leftarrow \alpha \cdot s.value$
4:     Set-Send-Threshold($c, s'$)
5:     Send($c.name, s'$)
```

Returning to the first predicate on Line 1 of Update-Send-Threshold, there are two cases in which the send threshold has a value of 0:

1. when initially assigning the send threshold to be the null risk score; and

2. when no key interval in *a.scores* intersects the query interval, and thus the null risk score again is assigned the send threshold.

Suppose the first predicate is omitted from Line 1. Given that Update-Send-Threshold is the first statement in Apply-Risk-Score, it is possible that the send threshold is set prior to sending the contact a relevant risk score. In the worst case, this prevents *any* risk score from being sent to the target actor, thus providing the individual associated with target actor a false sense of security that they are not at risk of being infected. From a broader message-passing perspective, updating the send threshold to a non-null risk score *before* applying the risk score received by the actor may introduce a non-trivial amount of inaccuracy. To summarize, updating the send threshold only when its value is nonzero ensures correct message-passing behavior between actors.

Up until this point, the refinements to Apply-Risk-Score have focused on ensuring that message passing terminates and correctly adjusts over time, as risk scores expire. Prior to concluding this section, a message-passing optimization is introduced. Over a given period of time, an actor may receive several risk scores that are then propagated to multiple contacts. Intuitively, rather than sending multiple risk scores, it would be more efficient to send just the final risk score. To increase the likelihood of that this occurs, Apply-Risk-Score can be modified so that a contact "buffers" a single risk score that is intended to be sent to the target actor. Upon receiving a *flush timeout* message, the actor then "flushes" all contacts by sending the buffered message of each contact to the respective target actor. This is also known as *sender-side aggregation* in which the contact is an *aggregator* of risk scores.

The final iteration Apply-Risk-Score integrates sender-side aggregation. Moreover, Handle-Flush-Timeout clarifies the concept of "flushing" a contact. A flush timeout is assumed to be a periodically occurring "self" message.

```
Apply-Risk-Score($a, c, s$)
Update-Send-Threshold($a, c$)
if $c.threshold.value < s.value$ and $c.t + \beta > s.t$
    $s'.value \leftarrow \alpha \cdot s.value$
    Set-Send-Threshold($c, s'$)
    if $c.name \neq s.sender$
        $c.buffered \leftarrow s'$
```

```
Handle-Flush-Timeout($a$)
for each $c \in a.contacts$
    if $c.buffered \neq$ NIL
        Send($c.name, c.buffered$)
        $c.buffered \leftarrow$ NIL
```

To conclude the specification of actor behavior, the Handle-Contact operation indicates how an actor responds when a new contact or contact with a newer contact time is received. Similar to Handle-Risk-Score, expired contacts are not processed. The Merge operation for *a.contacts* differs from how its used for *a.scores*. Specifically, if a contact with the same key already exists, its contact time is updated to that of the new contact; all other state of the previous contact is maintained.

```
Handle-Contact($a, c$)
if Contact-Ttl($c$) $> 0$
    $c.threshold \leftarrow$ Null-Risk-Score
    $c.buffered \leftarrow$ nil
    $c.key \leftarrow c.name$
    Merge($a.contacts, c$)
    $s \leftarrow$ Maximum-Older-Than($a.scores, c.t + \beta$)
    Apply-Risk-Score($a, c, s$)
```

1.2.3 Message Reachability

A fundamental concept of reachability in temporal networks is the *time-respecting path*: a contiguous sequence of contacts with nondecreasing time. Thus, node v is *temporally reachable* from node u if there exists a time-respecting path from u to v (Moody, 2002). The following quantities are derived from the notion of a time-respecting path and help quantify reachability in a time-varying network (Holme and Saramäki, 2012).

- The *influence set* I_v of node v is the set of nodes that v can reach by a time-respecting path.
- The *source set* S_v of node v is the set of nodes that can reach v by a time-respecting path.
- The *reachability ratio* $f(G)$ of a temporal network G is the average influence-set cardinality of a node v.

Generally, a message-passing algorithm defines a set of constraints that determine when and what messages are sent from one node to another. Even if operating on a temporal network, those constraints may be more or less strict than requiring temporal reachability. As a dynamic process, message passing on a time-varying network requires a more general definition of reachability that can account for network topology *and* message-passing semantics (Barrat and Cattuto, 2013).

Formally, the *message reachability from node u to node v* is the number of edges along the *shortest path P* that satisfy the message passing constraints,

$$m(u,v) = \sum_{(i,j)\in P} f(u,i,j,v),$$

where

$$f(u,i,j,v) = \begin{cases} 1 & \text{if all constraints are satisfied} \\ 0 & \text{otherwise.} \end{cases}$$

Node v is *message reachable* from node u if there exists a shortest path such that $m(u,v) > 0$. The *message reachability* of node u is the maximum message reachability from node u:

$$m(u) = \max_{v\in V} m(u,v). \tag{1.4}$$

The temporal reachability metrics previously defined can be extended to message reachability by only considering the message-reachable vertices:

$$\begin{aligned} I_u &= \{\, v \in V \mid m(u,v) = |P| \,\} \\ S_v &= \{\, u \in V \mid m(u,v) = |P| \,\} \\ f(G) &= \sum_{v \in V} |I_v| \cdot |V|^{-1} . \end{aligned}$$

Let $\mathbf{M}$ be the *message reachability matrix* of the temporal network G such that nodes are enumerated $1, 2, \ldots, |V|$ and for each $m_{ij} \in \mathbf{M}$,

$$m_{ij} = \begin{cases} 1 & \text{if } m(i,j) = |P| \\ 0 & \text{otherwise.} \end{cases}$$

Then the cardinality of the influence set for node i is the number of nonzero elements in the i-th row of $\mathbf{M}$:

$$|I_i| = \sum_{j=1}^{|V|} m_{ij}. \tag{1.5}$$

Similarly, the cardinality of the source set for node j is the number of nonzero elements in the j-th column of $\mathbf{M}$:

$$|S_j| = \sum_{i=1}^{|V|} m_{ij}. \tag{1.6}$$

For risk propagation, let P is the set of edges along the shortest path from u to v such that the actors are enumerated $1, \ldots, |P|$. Then message reachability is defined as

$$m(u,v) = \sum_{(i,j)\in P} [\alpha^i s_u > \gamma \alpha s_{ij}] \cdot [t_u < t_{ij} + \beta] \tag{1.7}$$

The value of (1.7) can be found by associating with each symptom score a unique identifier. If each actor maintains a log of the risk scores it receives, then the set of actors that receive the symptom score or a propagated risk score thereof can be identified. This set of actors defines the induced subgraph on which to compute (1.7) using a shortest-path algorithm (Johnson, 1977).

Regarding efficiency, (1.4) to (1.6) provide the means to quantify the communication overhead of a given message-passing algorithm on a temporal network. Moreover, because such metrics capture the temporality of message passing, they can better quantify complexity than traditional graph metrics.

By relaxing the constraint (**??**), it is possible to estimate (1.7) with (**??**). The *estimated message reachability* of node u to node v, denoted $\hat{m}(u,v)$, is defined as follows. Based on (**??**),

$$\alpha^{\hat{m}(u,v)} \cdot s_u \leq \gamma \cdot s_v,$$

where the left-hand side is the value of the propagated symptom score for actor u when $\hat{m}(u,v) = 1$, and the right-hand side is the value required by some message-reachable actor v to propagate the message received by actor u or some intermediate actor. Solving for $\hat{m}(u,v)$,

$$\hat{m}(u,v) \leq f(u,v), \tag{1.8}$$

where

$$f(u,v) = \begin{cases} 0 & \text{if } s_u = 0 \\ |P| & \text{if } s_v = 0 \\ \log_\alpha \gamma + \log_\alpha s_v - \log_\alpha s_u & \text{otherwise.} \end{cases}$$

Equation (1.8) indicates that a lower send coefficient γ will generally result in higher message reachability, at the cost of sending possibly ineffective messages (i.e., risk scores that do not update the exposure score of another actor). Equation (1.8) also quantifies the effect of the transmission rate α. Unlike the send coefficient, however, the transmission rate is intended to be derived from epidemiology to quantify disease infectivity and should not be optimized to improve performance.

Given the multivariate nature of message reachability, it is helpful to visualize how it with various combinations of parameter values. Figure 1.4 includes several line plots of estimated message reachability $\hat{m}(u,v)$ with respect to the initial risk score magnitude of actor u.

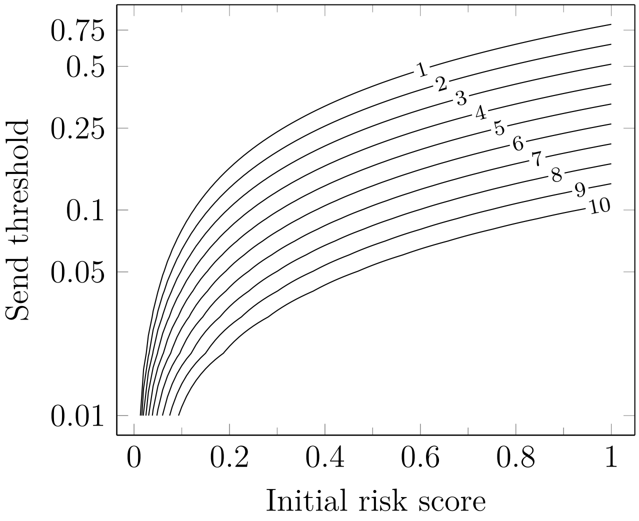

Figure 1.4: Estimated message reachability. Contour lines are shown for integral reachability values. Given an initial risk score and message reachability, a contour line indicates an upper bound on the permissible send threshold.

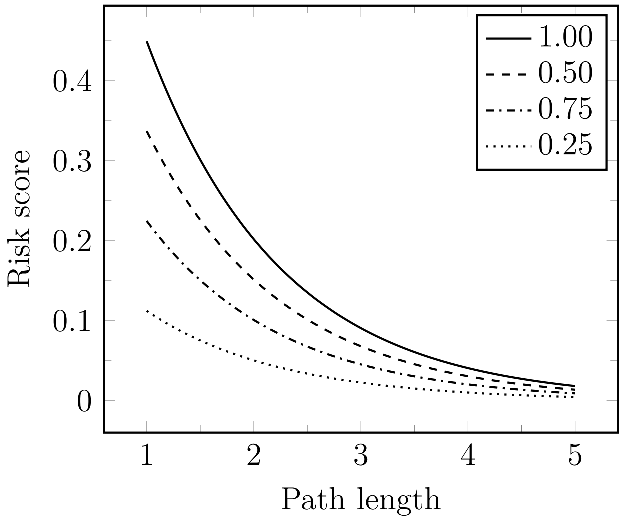

Figure 1.5: Exponential decay of risk scores.

Appendix A

Pseudocode Conventions

Pseudocode conventions are mostly consistent with Cormen et al. (2022).

- Indentation indicates block structure.

- Looping and conditional constructs have similar interpretations to those in standard programming languages.

- Composite data types are represented as *objects*. Accessing an *atttribute* a of an object o is denoted $o.a$. A variable representing an object is a *pointer* or *reference* to the data representing the object. The special value NIL refers to the absence of an object.

- Parameters are passed to a procedure *by value*: the "procedure receives its own copy of the parameters, and if it assigns a value to a parameters, the change is *not* seen by the calling procedure. When objects are passed, the pointer to the data representing the object is copied, but the attributes of the object are not." Thus, attribute assignment "is visible if the calling procedure has a pointer to the same object."

- A **return** statement "immediately transfers control back to the point of call in the calling procedure."
- Boolean operators **and** and **or** are *short circuiting*.

The following conventions are specific to this work.

- Object attributes may be defined *dynamically* in a procedure.
- Variables are local to the given procedure, but parameters are global.
- The "$\leftarrow$" symbol is used to denote assignment, instead of "$=$".
- The "$=$" symbol is used to denote equality, instead of "$==$", which is consistent with the use of "$\neq$" to denote inequality.
- The "$\in$" symbol is used in **for** loops when iterating over a collection.
- Set-builder notation $\{\, x \in X \mid \textsc{Predicate}(x) \,\}$ is used to create a subset of a collection X in place of constructing an explicit data structure.

Appendix B

Data Structures

Let a *dynamic set* X be a mutable collection of distinct elements. Let x be a pointer to an element in X such that $x.key$ uniquely identifies the element in X. Let a *dictionary* be a dynamic set that supports insertion, deletion, and membership querying (Cormen et al., 2022).

- INSERT(X, x) adds the element pointed to by x to X.
- DELETE(X, x) removes the element pointed to by x from X.
- SEARCH(X, k) returns a pointer x to an element in the set X such that $x.key = k$; or NIL, if no such element exists in X.
- MERGE(X, x) adds the element pointed to by x, if no such element exists in X; otherwise, the result of applying a function to x and the existing element is added to X.
- MAXIMUM(X) returns a pointer x to the maximum element of the totally ordered set X; or NIL if X is empty.

Bibliography

Gul Agha. *Actors: A model of concurrent computation in distributed systems*. PhD thesis, MIT, 1985. URL `http://hdl.handle.net/1721.1/6952`.

Erman Ayday, Fred Collopy, Taehyun Hwang, Glenn Parry, Justo Karell, James Kingston, Irene Ng, Aiden Owens, Brian Ray, Shirley Reynolds, Jenny Tran, Shawn Yeager, Youngjin Yoo, and Gretchen Young. Sharetrace: A smart privacy-preserving contact tracing solution by architectural design during an epidemic. Technical report, Case Western Reserve University, 2020. URL `https://github.com/cwru-xlab/sharetrace-papers/blob/main/sharetace-whitepaper.pdf`.

Erman Ayday, Youngjin Yoo, and Anisa Halimi. ShareTrace: An iterative message passing algorithm for efficient and effective disease risk assessment on an interaction graph. In *Proc. 12th ACM Con. Bioinformatics, Comput. Biology, Health Inform.*, BCB 2021, 2021.

Alain Barrat and Ciro Cattuto. Temporal networks of face-to-face human interactions. In Petter Holme and Jari Saramäki, editors, *Temporal Netw.*, Underst. Complex Syst. Springer, 2013. doi:10.1007/978-3-642-36461-7_10.

Christopher M. Bishop. Pattern recognition and machine learning. In M. I. Jordan, Robert Nowak, and Bernhard Schoelkopf, editors, *Inf. Sci. Stat.* Springer, 2006.

Thomas H. Cormen, Charles E. Leiserson, Ronald L. Rivest, and Clifford Stein. *Introduction to Algorithms.* The MIT Press, fourth edition, 2022.

Meggan E. Craft. Infectious disease transmission and contact networks in wildlife and livestock. *Phil. Trans. R. Soc. B*, 370, 2015. doi:10.1098/rstb.2014.0107.

Leon Danon, Ashley P. Ford, Thomas House, Chris P. Jewell, Gareth O. Roberts, Joshua V. Ross, and Matthew C. Vernon. Networks and the epidemiology of infectious disease. *Interdiscip. Perspect. Infect. Dis.*, 2011, 2011. doi:10.1155/2011/284909.

Centers for Disease Control and Prevention. Quarantine and isolation, 2021. `https://www.cdc.gov/coronavirus/2019-ncov/your-health/quarantine-isolation.html`.

Erich Gamma, Richard Helm, Ralph Johnson, and John Vlissides. *Design patterns: Elements of reusable object-oriented software.* Addison-Wesley, 1995.

Carl Hewitt. Viewing control structures as patterns of passing messages. *Artificial Intelligence*, 8(3):323–364, 1977. doi:10.1016/0004-3702(77)90033-9.

Carl Hewitt and Henry Baker. Laws for communicating parallel processes.

Working paper, MIT Artificial Intelligence Laboratory, 1977. URL http://hdl.handle.net/1721.1/41962.

Petter Holme and Jari Saramäki. Temporal networks. *Phys. Rep.*, 519, 2012. doi:10.1016/j.physrep.2012.03.001.

Donald B. Johnson. Efficient algorithms for shortest paths in sparse networks. *J. ACM*, 24, 1977. doi:10.1145/321992.321993.

Andreas Koher, Hartmut H. K. Lentz, James P. Gleeson, and Philipp Hövel. Contact-based model for epidemic spreading on temporal networks. *Phys. Rev. X*, 9, 2019. doi:10.1103/PhysRevX.9.031017.

Frank R. Kschischang, Brendan J. Frey, and Hans A. Loeliger. Factor graphs and the sum-product algorithm. *IEEE Trans. Inf. Theory*, 47, 2001. doi:10.1109/18.910572.

R. Greg Lavender and Douglas C. Schmidt. Active object – an object behavioral pattern for concurrent programming, 1996. https://csis.pace.edu/~marchese/CS865/Papers/Act-Obj.pdf.

Andrey Y. Lokhov, Marc Mézard, Hiroki Ohta, and Lenka Zdeborová. Inferring the origin of an epidemic with a dynamic message-passing algorithm. *Phys. Rev. E*, 90, 2014. doi:10.1103/PhysRevE.90.012801.

Cristina Menni, Ana M Valdes, Maxim B Freidin, Carole H Sudre, Long H Nguyen, David A Drew, Sajaysurya Ganesh, Thomas Varsavsky, M Jorge Cardoso, Julia S El-Sayed Moustafa, Alessia Visconti, Pirro Hysi, Ruth

C E Bowyer, Massimo Mangino, Mario Falchi, Jonathan Wolf, Sebastien Ourselin, Andrew T Chan, Claire J Steves, and Tim D Spector. Real-time tracking of self-reported symptoms to predict potential COVID-19. *Nat. Med.*, 26, 2020. doi:10.1038/s41591-020-0916-2.

James Moody. The importance of relationship timing for diffusion. *Soc. Forces.*, 81, 2002.

Christopher S. Riolo, James S. Koopman, and Stephen E. Chick. Methods and measures for the description of epidemiologic contact networks. *J. Urban Health*, 78, 2001. doi:10.1093/jurban/78.3.446.

Tao Zhou, Jie Ren, Matú š Medo, and Yi-Cheng Zhang. Bipartite network projection and personal recommendation. *Phys. Rev. E*, 76, 2007.

Lorenzo Zino and Ming Cao. Analysis, prediction, and control of epidemics: A survey from scalar to dynamic network models. *IEEE Circuits Syst. Mag.*, 21, 2021. doi:10.1109/mcas.2021.3118100.