Anomaly Characterization in Large Scale Networks

Emmanuelle Anceaume  
CNRS / IRISA, France  
emmanuelle.anceaume@irisa.fr

Yann Busnel  
LINA / Université de Nantes, France  
yann.busnel@univ-nantes.fr

Erwan Le Merrer  
Technicolor Rennes, France  
erwan.lemerrer@technicolor.com

Romaric Ludinard  
Inria, France  
romaric.ludinard@inria.fr

Jean-Louis Marchand  
Ecole Normale Supérieure de Rennes, France  
jean-louis.marchand@ens-rennes.fr

Bruno Sericola  
Inria, France  
bruno.sericola@inria.fr

Abstract—The context of this work is the online characterization of errors in large scale systems. In particular, we address the following question: Given two successive configurations of the system, can we distinguish massive errors from isolated ones, the former ones impacting a large number of nodes while the second ones affect solely a small number of them, or even a single one? The rationale of this question is twofold. First, from a theoretical point of view, we characterize errors with respect to their neighbourhood, and we show that there are error scenarios for which isolated and massive errors are indistinguishable from an omniscient observer point of view. We then relax the definition of this problem by introducing unresolved configurations, and exhibit necessary and sufficient conditions that allow any node to determine the type of errors it has been impacted by. These conditions only depend on the close neighbourhood of each node and thus are locally computable. We present algorithms that implement these conditions, and show through extensive simulations, their performances. Now from a practical point of view, distinguishing isolated errors from massive ones is of utmost importance for networks providers. For instance, for Internet service providers that operate millions of home gateways, it would be very interesting to have procedures that allow gateways to self distinguish whether their dysfunction is caused by network-level errors or by their own hardware or software, and to notify the service provider only in the latter case.

I. INTRODUCTION

In this paper we study the on-line monitoring problem in large scale distributed systems. This problem deals with the capability of collecting and analysing relevant information provided by monitored devices so as to make the monitoring application continuously aware of the state of the system. In presence of a large number of monitored devices (i.e., a typical scenario is the one encountered by Internet service providers operating millions of home gateways), an approach to solve this problem is to rely on customers care call centres. Such call centres are notified by customers that experience degradations of service quality. This approach while commonly adopted, shows several issues in terms of latency (i.e., the latent detection period between the occurrence of an incident and the instant at which the customer observes it is unpredictable), cost (i.e., it requires to mobilize agents for manually handling each customer notification), and inefficiency (e.g., when incidents lie in a part of the network that is not operated by the service provider or when notifications are due to customers negligences). These issues call for automated monitoring procedures that should be able to notify the service provider only for legitimate reasons. Actually, standardized procedures [4] exist at devices level to autonomously trigger investigations in presence of errors or networks events. However, these procedures are never used for practical reasons. Indeed if the cause of a QoS (Quality of Service) variation lies in the network itself – due to routing loops, router dysfunctions, or configuration errors – this may impact a very large number of devices (more precisely, impact services consumed by these devices), and thus letting thousands of impacted devices reporting the problem to the operator may quickly become a disaster. It is thus of utmost importance to minimize the overall pressure put on the service operator, by giving each device the capability to locally detect whether the local QoS degradation is also observed at many other devices or not, so that only isolated errors or events are reported on the fly by the devices experiencing them. Alternatively, there is a clear need for over-the-top operators – that rely on Internet Service Providers to transparently deliver content to their clients – to quickly detect network level events. Indeed, incidents at the network level may impact the quality at which data is received at thousands of clients that will naturally blame their over-the-top operators. Our solution provides each end-device the capability to self distinguish network-based events from local ones, so that only network-events are reported on the fly to the over-the-top operators.

In both cases, the key point is to provide each monitored device a way to estimate on other devices the impact of a locally perceived QoS degradation. The approach we propose boils down for a device to locally detect the presence of similarity features in the abnormal behaviour of other devices. This is achieved by modelling the QoS of the different services accessed by a device by a point in a QoS space $E$, and the temporal evolution of its QoS by a trajectory in $E$. A trajectory is abnormal if the predicted values of the QoS differ from the observed ones. The problem we tackle amounts for a device to locally identify all the abnormal trajectories that are close to its own one, to determine how dense they are, to finally decide whether its services have been impacted by an isolated event or a network one. The notion of closeness is...
modelled by the presence of points in a ball centred at a given point. Surprisingly, we show that it exists some trajectories that are indistinguishable (even from the point of view of an omniscient observer) in the sense that it is impossible to decide whether they are due to isolated events or a network one without knowing the event itself. We formally characterize these unresolved configurations, and derive necessary and sufficient conditions that allow each device to locally decide with certainty whether it belongs to an unresolved configuration or if it has been impacted by an isolated event, or by a network one. In our approach, the frequency at which QoS information is sampled is locally tuned, and only depends on the local occurrence of QoS degradations. Therefore, by avoiding any kind of global synchronization, devices can efficiently provide a fine grain event/errors detection without impacting the rest of the system. The influence of this local tuning has an enjoyable consequence on the number of unresolved configurations: by sampling sufficiently often one’s neighborhood, the number of unresolved configurations drastically shrinks. To summarize, our contributions are:

- A modelling of isolated and network based errors;
- The derivation of local conditions that allow each device to decide with certainty whether its observed QoS degradation is due to an isolated error or a network one;
- A fine granularity of error detection locally tunable and transparent to the remaining of the system;
- The design of local algorithms whose decisions are as accurate as the one provided by an omniscient observer.

The remaining of the paper is organized as follows. Section II provides an overview of existing monitoring approaches. Section III presents the model of the system, and how errors are modelled. Section IV formalizes the on-line anomaly detection problem and its relaxed version. Section V presents computable conditions that allow any device to locally solve the relaxed version of the anomaly detection problem. Section VI presents the local algorithms, and their performances are analysed through extensive simulations (see Section VII). Section VIII concludes and presents future works.

II. RELATED WORK

This section provides an overview of the existing techniques used in large scale systems to continuously and automatically monitor time-varying metrics. The authors in [15] exploit temporal and spatial correlations [3], [8], [11] among groups of monitored nodes to decrease monitoring communication costs, i.e., the cost incurred by the periodic reporting of the updated metrics values from the monitored nodes to the management node. The idea is to prevent any reporting message from occurring when such a reporting would contain metrics values that could be directly inferred by the management node. This is achieved by giving each monitored node the capability to locally detect whether the current values of its monitored metrics are in accordance with predicted ones (through Kalman filters tools [7] installed at both monitored nodes and the management node), and by gathering nodes into clusters (such that, for each monitored metric, a set of clusters groups together nodes that share correlated values of the considered metric according to the Pearson correlation coefficient). At clusters level, an elected leader is in charge of communicating with the management system when the current metric values of its group members differ from each others. Although close to our objectives, the main drawback of this solution lies on the centralized clustering process. All the nodes of the system are continuously organized into clusters computed through the k-means algorithm exclusively run by the management node, which is a clear impediment to the scalability of their approach. Other works aim at minimizing the processing cost for continuous monitoring [13], [9], [14] in the light of the theoretical results of [5], however similarly to [15], all these approaches suffer from a centralized handling of the clustering process. Recently, Choffnes et al. [2] have proposed to leverage structured peer-to-peer architectures (i.e., Distributed Hashing Tables) to guarantee scalable monitoring management. In contrast to the previous described works that focus on monitoring fine-grained changes on individual nodes, [2] pushes monitoring on end users. Their approach consists in having a set of cooperating edge system monitors (ESM), such that each one has access to a distributed storage system based on a DHT in which they publish aggregated informations about events detected in their own sub-network. This allows network operators to regularly access the storage architecture to analyse system wide detected events, and thus to detect global, or at least massive, network outages. The authors in [1] propose an on-line error detection mechanism that in contrast to [2] is proactive. Their mechanism fully depends on the tessellation of the overlay. However, tessellating the space with large bucket sizes tends to identify each possible error as a massive one, while considering small bucket sizes reduces drastically the probability of having a large number of devices into a single bucket, giving rise to the triggering of false alarms. In our approach, we go a step further by providing to close end devices the capability to locally exploit correlation between their state to detect on the fly the type of error they have been impacted by.

III. SYSTEM MODEL

This section presents the terminology and concepts we need to model the impact of outages on the monitored devices. Note that we adopt the following conventional notations. Variables are represented by lower-case letters as $j, \ell, p$ and $q$, sets are denoted by capital letters as $S$ and $E$, and families of sets are denoted by capital calligraphic letters as $\mathcal{P}$. The set of integers $\{1, \ldots, n\}$ is denoted by $[1, n]$.

A. Preliminaries

We consider a set of $n$ monitored devices, such that each one consumes a subset of $d$ services $s_1, \ldots, s_d$. At any discrete time $k$, the QoS of each consumed service $s_j$ at device $j$ is locally measured with an end-to-end performance measurement function $q_{i,k}(j)$, whose range of values is $[0, 1]$. For non consumed services $s_j$, we have $q_{i,k}(j) = 0$. We model the QoS of monitored devices at discrete time $k$ as
a set $S_k$ of $n$ points in a space $E = [0,1]^d$, with $d \geq 1$, called the QoS space. The position of device $j$ at time $k$ is represented by point $p_k(j) = (q_{1,k}(j),\ldots,q_{d,k}(j))$. Note that in the following we interchangeably use terms device and point to speak about the position of a device in the QoS space $E$. The state $S_k$ of the system at discrete time $k$ is $S_k = (p_1(k),\ldots,p_k(n))$. Each monitored device $j$ has also access at any time $k$ to an error detection function $a_k(j)$ such that $a_k(j) = \text{true}$ if at time $k$ there is at least one service consumed by device $j$ whose variation of quality of service is too large to be considered as normal. Error detection functions provide some meaningful predictions of what should be the next output value based on the sequence of past input values. Different kinds of error detection functions exist, ranging from simple threshold based functions to more sophisticated ones like the Holt-Winters forecasting or Cusum methods [6], [12], [10]. Note that implementation of function $a$ is out of the scope of the paper.

As said in the introduction, the impact of errors on devices can either be locally restricted (that is, each error affects a few number $\tau$ of devices, with $\tau$ a configuration parameter) or spread over a large number of devices (i.e., more than $\tau$ devices). By construction, a set of devices whose positions in the QoS space $E$ are very close to each other exhibit a similar QoS. We make the assumption that if a set of devices, exhibiting a similar QoS at time $k-1$ are impacted by the same error then they will undergo the same QoS variation. Thus, at time $k$ their modified positions in $E$ will still be close to each other. This closeness assumption is modelled by the presence of points in a ball of radius $r$. In the following $r$ is called the consistency impact radius. Prior to formally modelling the impact of errors or events on devices, we first present the notions we will intensively use in the following.

B. Terminology and Notations

For the sake of simplicity, we use the uniform norm $\| \cdot \|$ defined for any $x = (x_1,\ldots,x_d) \in E$ by $\|x\| = \max\{x_1,\ldots,x_d\}$. As we consider a finite dimension space, all norms are equivalent and thus all the results in the paper would still work even when using a different norm.

**Definition 1 (r-consistent set):** For any $r \in [0,1/4)$, a subset $B \subseteq [1,n]$ is said to be $r$-consistent at time $k$ if the maximal distance between any $i,j \in B$ is not larger than $2r$, that is,

$$\forall(i,j) \in B^2, \|p_k(i) - p_k(j)\| \leq 2r.$$  

**Definition 2 (Maximal r-consistent set):** For any $r \in [0,1/4)$, a subset $B \subseteq [1,n]$ is a maximal $r$-consistent set at time $k$ if and only if $B$ is an $r$-consistent set at time $k$ and $\forall j \in [1,n] \setminus B, B \cup \{j\}$ is not an $r$-consistent set at time $k$.

Figure 1 illustrates these two above notions. It depicts the position of six devices $\{1,2,3,4,5,6\}$ at time $k$ in a one dimension QoS space $E$ (i.e., the number of accessed services is equal to one). The distance between any two devices of $B_1 = \{1,2,3,4\}$ (resp. of $B_2 = \{1,2,3,5,6\}$) is not larger than $2r$ and thus they belong to the same $r$-consistent set.

Fig. 1. The two maximal $r$-consistent sets $B_1 = \{1,2,3,4\}$ and $B_2 = \{1,2,3,5,6\}$ containing point 1. Any subset of $B_1$ and any subset of $B_2$ is an $r$-consistent set.

The two $r$-consistent sets $B_1$ and $B_2$ containing device $1$ are maximal because adding device $5$ or $6$ to $B_1$ or adding $4$ to $B_2$ would make them non $r$-consistent.

From these two above notions, we derive the concept of consistent motions. A motion reflects the fact that the QoS of a set of devices keep close to each other at successive discrete times. Formally,

**Definition 3 (r-consistent motion):** For any $r \in [0,1/4)$, a subset $B \subseteq [1,n]$ has an $r$-consistent motion in the time interval $[k−1,k]$ if $B$ is an $r$-consistent set at both times $k−1$ and $k$. Moreover, a subset $B \subseteq [1,n]$ has a maximal $r$-consistent motion in the time interval $[k−1,k]$ if $B$ has an $r$-consistent motion in the time interval $[k−1,k]$ and $\forall j \in [1,n] \setminus B, B \cup \{j\}$ does not have an $r$-consistent motion in the time interval $[k−1,k]$.

**Remark 1:** If $B$ has an $r$-consistent motion in the time interval $[k−1,k]$, either $B$ has a maximal $r$-consistent motion or there exists $B' \subseteq [1,n], B \subseteq B'$ such that $B'$ has a maximal $r$-consistent motion.

Finally, we classify $r$-consistent motions according to the number of devices that belong to these motions. This notion will be central for the modelling of errors or events.

**Definition 4 (τ-dense and τ-sparse motions):** For any $\tau \in [0,1/4)$, $\tau \in [1,n−1]$, and for any subset $B \subseteq [1,n]$ having an $r$-consistent motion in the time interval $[k−1,k]$, if $|B| > \tau$ then $B$ is said to have a $\tau$-dense $r$-consistent motion (or simply a $\tau$-dense motion) in $[k−1,k]$, otherwise $B$ has a $\tau$-sparse $r$-consistent motion (or simply a $\tau$-sparse motion) in $[k−1,k]$.

C. Modelling the Impact of Errors

As said in Section III-A, each device $j$ at time $k$ feeds an error detection function $a_k(j)$ with $p_k(j)$ where $p_k(j) = (q_{1,k}(j),\ldots,q_{d,k}(j))$. If the variation of quality is considered as abnormal, this function returns true$^1$. We model the impact of an error on a device by an abnormal trajectory of this device in the quality space $E$.

**Definition 5 (Abnormal Trajectory):** A point $j \in [1,n]$ has an abnormal trajectory in the time interval $[k−1,k]$ if $a_k(j) = \text{true}$. The subset of points having an abnormal trajectory in the time interval $[k−1,k]$ is denoted by $A_k$. Formally,

$$A_k = \{j \in [1,n] | a_k(j) = \text{true}\}.$$  

As previously argued, the main objective of this work is to give each device – whose QoS of consumed services has been

$^1$It is important to note that only the (abnormal) variation of QoS matters, not the period of time during which the modified QoS is exhibited.
impacted by some error – the capability to accurately decide whether such an error has also affected many other devices or solely a few of them. This boils down for each device to locally determine the presence of similarity features in the abnormal behaviour of other devices. As presented above, this is achieved by modelling devices QoS by points in the QoS space, and the temporal evolution of their QoS by trajectories in the QoS space so that, at each time \( k \), state \( S_k \) represents the QoS of all devices. We show in the following that each device only needs to know the trajectories of devices that are at no more than \( 4 \tau \) from itself. A wider knowledge – as the one got by an omniscient observer that samples at each time \( k \) the system state, i.e., \( S_k \) – does not bring any additional information and thus does not provide a higher error detection accuracy (see Theorems 5, 6, and 7 and Corollary 8 in Section V).

From these periodic samplings of the system state, one can construct several plausible scenarios of errors that would explain the trajectories of each device. For instance if a group of points follow the same abnormal trajectories at different observations, it should be caused by the same error. Similarly, if some point shows an abnormal trajectory that moves it away from its previous neighbours it should be due to some isolated error. On the other hand, there are scenarios of errors that cannot be captured by periodic snapshots, as for example the fact that some device has been hit by simultaneous or temporally close errors between two successive snapshots. We encapsulate these indistinguishable scenarios of errors by imposing the following restrictions on the impact of errors on devices QoS.

**R1:** In the time interval \([k-1,k]\), the abnormal trajectory of each device \( j \in A_k \) is due to a single error.

**R2:** An error has a similar effect on the abnormal trajectories of all impacted devices. In particular if a set of devices belonging to the same \( r \)-consistent set are impacted by a given error in the time interval \([k-1,k]\) then all these devices will undergo the same abnormal trajectories and thus by Definition 3 will follow the same \( r \)-consistent motion in \([k-1,k]\).

**R3:** If strictly less than \( \tau + 1 \) devices have an abnormal trajectory due to the same error then none of these devices can belong to a \( \tau \)-dense motion. Moreover, if a device belongs to a \( \tau \)-dense motion then this device has necessarily been impacted by an error that has impacted many other devices (not necessarily those following the same motion).

Note that a single error can impact devices whose QoS can be arbitrarily different. Restrictions R1, R2 and R3 are taken into account by partitioning the set of devices in \( A_k \) into \( \tau \)-dense motion subsets and \( \tau \)-sparse motion subsets such that (i) all the \( \tau \)-sparse motion subsets are sufficiently "far" from each other so that any combination of several of them cannot form \( \tau \)-dense motion subsets, and (ii) any single \( \tau \)-sparse motion subset is sufficiently "far" from any \( \tau \)-dense motion one so that this \( \tau \)-sparse motion subset cannot merge with a \( \tau \)-dense one. This partitioning of \( A_k \) is formally defined as follows.

**Definition 6 (Anomaly partition \( P_k \)):** For any \( k \geq 1, \tau \in [1,n-1], r \in [0,1/4) \), the partition \( P_k \) of \( A_k \) is said to be an anomaly partition at time \( k \) if it is made of non-empty and disjoint \( r \)-consistent motions \( B_1, \ldots, B_t \) that verify conditions C1 and C2 below. Subsets \( B_1, \ldots, B_t \) are called anomalies.

**C1:** \( \forall B \subseteq \bigcup_{|B_i| \leq \tau} B_i, \) \( B \) has a \( \tau \)-sparse motion or \( B \) has not an \( r \)-consistent motion.

**C2:** \( \forall i \in [1,t], B_i \) has a \( \tau \)-dense motion \( \Rightarrow \forall B \subseteq \bigcup_{|B_i| \leq \tau} B_j, B \cap B_i \) has not a \( r \)-consistent motion.

By extension, for any point \( j \in A_k, P_k (j) \) represents the (unique) subset \( B \in P_k \) such that \( j \in B \).

In spite of the apparent complexity of Definition 6, the following lemma shows that given \( A_k, S_{k-1}, S_k, \tau \) and \( r \), there always exists at least one anomaly partition.

**Lemma 2:** For any \( k \geq 1, \) for any \( A_k \neq \emptyset, \) for any system states \( S_{k-1} \) and \( S_k, \tau \in [1,n-1] \) and \( r \in [0,1/4) \), there exists at least one partition \( P_k \) of \( A_k \) such that \( P_k \) is an anomaly partition. In the general case, it is not unique.

**Proof:** We first prove the existence of anomaly partitions, and then their non-uniqueness.

A simple way to build an anomaly partition \( P_k \) of \( A_k \) is described in Algorithm 1. After having initialized \( P_0 \) to an empty set and \( S \) to \( A_k \), all the points of \( S \) are examined as follows. Let \( j \) be any random point taken from \( S \), and \( B \) any subset of \( S \) that has a maximal \( r \)-consistent motion in \( S \) involving \( j \). \( B \) is added to \( P_k \) and all the elements of \( B \) are removed from \( S \). The size of \( S \) is monotonically decreasing and thus this algorithm terminates. We now prove by induction that at each iteration, \( P_k \) satisfies conditions C1 and C2 of Definition 6. The first element added in \( P_k \) has a maximal motion. Being the first element of \( P_k \), both conditions C1 and C2 hold. Now suppose that up to iteration \( n \geq 1 \) both conditions C1 and C2 hold. At the end of iteration \( m = n + 1 \), the new element \( B \) of \( P_k \) has a maximal \( r \)-consistent motion among all the remaining points of \( S \). By construction, \( \forall j \in [1,n], B_j \in P_k \) has a maximal \( r \)-consistent motion among all the remaining points of \( S \). Thus, by Definition 3, \( \forall j \in S \setminus \bigcup_{i \leq t} B_i, B_j \cup \{j\} \) has not an \( r \)-consistent motion. In particular, \( \forall j \in B, B \cup \{j\} \) has not an \( r \)-consistent motion. Thus conditions C1 and C2 hold, and by the induction hypothesis, C1 and C2 hold for all iteration.
Algorithm 1: Constructing an anomaly partition from $A_k$.

Data: $S_{k-1}, S_k, \tau \in [1, n-1], r \in [0, \frac{1}{2})$.

Requires: $A_k$

Output: An anomaly partition

1 begin
2 $S \leftarrow A_k$;
3 $P_k \leftarrow \{\}$;
4 while $S \neq \emptyset$ do
5     Take any $j \in S$;
6     Let $B \subseteq S$ be such that $j \in B$ and $B \notin P_k$ and $B$ has
7     a maximal $r$-consistent motion in $S$;
8     $S \leftarrow S \setminus B$;
9     $P_k \leftarrow P_k \cup \{B\}$;
10 return $P_k$;

steps. Finally, as $A_k$ is non empty, for any $j$ in $A_k$, it exists a subset $B \in P_k$ such that $j \in B$. By construction of $P_k$, each element of $A_k$ belongs to only one element of $P_k$ and thus $P_k$ is a partition of $A_k$, which completes the proof.

We now show with a counter-example that given $A_k$, $S_{k-1}$ and $S_k$, the anomaly partition that moves the state space from $S_{k-1}$ to $S_k$ is in the general case not unique. Consider Figure 2 that shows the variation of QoS of a service consumed by ten devices $S = [1,10]$ in the time interval $[k-1,k]$. Suppose that the density threshold $\tau$ is equal to 3 and all devices in $S$ have abnormal trajectories. Four maximal $r$-consistent motions $C_1, C_2, C_3, C_4$ are depicted. By direct application of Algorithm 1, if device 1 is first chosen, $C_1$, then $C_3$ and $C_4$ and finally $\{4\}$ constitutes the members of a possible anomaly partition. We have: $P'_k = \{\{1,2,3\}, \{4\}, \{5,6,7,8,9\}, \{10\}\}$. Now if device 4 is initially chosen, we have $P'_k = \{\{1\}, \{2,3,4\}, \{5,6,7,8,9\}, \{10\}\}$. This completes the proof.

Finally, according to the number of devices belonging to each $B_1, \ldots, B_t$ of $P_k$, we differentiate between isolated anomalies and massive anomalies. Specifically,

**Definition 7 (Massive / Isolated Anomalies):** Let $P_k$ be an anomaly partition. An element $B \in P_k$ is called a **massive anomaly** in the time interval $[k-1,k]$ if $|B| > \tau$. Otherwise it is called an **isolated anomaly**. The set of devices impacted by a massive anomaly in the time interval $[k-1,k]$ is denoted by $M_{P_k}$. Formally, we have $M_{P_k} = \{j \in A_k \mid |P_k(j)| > \tau\}$. Similarly, the set of devices impacted by an isolated anomaly in the time interval $[k-1,k]$ is denoted by $I_{P_k}$. We have $I_{P_k} = \{j \in A_k \mid |P_k(j)| \leq \tau\}$.

To summarize, let $P_k$ be an anomaly partition, we have

$$A_k = M_{P_k} \cup I_{P_k} \text{ and } M_{P_k} \cap I_{P_k} = \emptyset.$$  \hspace{1cm} (1)

We suppose in the following that all the errors or events that occur in the system respect restrictions R1, R2 and R3. In this (ideal) context, there exists an anomaly partition that reconstructs exactly what really happens in the system. In the following we denote by $R_k$, $k \geq 1$, this real scenario of errors, and by respectively $M_{R_k}$ and $I_{R_k}$ the set of devices that have been involved in respectively massive and isolated anomalies. We show in Theorem 3, that even in this ideal context, an omniscient observer is not always capable of building $M_{R_k}$ and $I_{R_k}$ if it has not access to $R_k$.

### IV. The Addressed Problems

Consider an omniscient observer that is able to read, at any time $k$, the state vector $S_k$, and knows for any point $j \in S$ the output of the error detection function $a_{x_k}(j)$. Based on this knowledge, the goal of the omniscient observer is to infer the set of devices that have been involved in massive and isolated anomalies. The question that naturally crosses our mind is whether these inferred sets exactly match both $M_{R_k}$ and $I_{R_k}$.

We reformulate this question as the Anomaly Characterization Problem (ACP). Specifically, for any $k \geq 1$, for any system states $S_{k-1}$ and $S_k$, for any $A_k$, and $\tau \in [1, n - 1]$, let $M_k$ and $I_k$ be the two sets built by the omniscient observer.
that contained all the devices that have been impacted by respectively massive and isolated anomalies.

**Problem 1 (Anomaly Characterization Problem (ACP)):** Is the omniscient observer always capable of building $M_k$ and $I_k$ such that $M_k = M_{R_k}$ and $I_k = I_{R_k}$ without knowing $R_k$?

**Theorem 3 (ACP Impossibility):** ACP cannot be solved, that is, the omniscient observer cannot always build $M_k$ and $I_k$ such that $M_k = M_{R_k}$ and $I_k = I_{R_k}$ without knowing $R_k$.

**Proof:** Proof by counter-example. We consider the scenario depicted in Figure 3 which illustrates the variation of QoS of a service consumed by five devices $S = \{1, 2, 3, 4, 5\}$ in the time interval $[k-1, k]$. We suppose that $\tau = 3$ and that all the devices in $S$ have abnormal trajectories. The two maximal $r$-consistent motions $C_1 = \{1, 2, 3, 4\}$ and $C_2 = \{2, 3, 4, 5\}$ are represented. Let $P_k^1 = \{\{1, 2, 3, 4\}, \{5\}\}$ and $P_k^2 = \{\{1\}, \{2, 3, 4, 5\}\}$ be the two anomaly partitions of $A_k$. Now, given $\tau = 3$, we have by definition that $M_{P_2} = \{1, 2, 3, 4\}$ and $M_{P_2} = \{2, 3, 4, 5\}$. An omniscient observer is unable to tell whether $P_k^1 = R_k$ or $P_k^2 = R_k$, and thus does not know whether $M_{P_1} = M_{R_k}$ or $M_{P_2} = M_{R_k}$. The same argument applies for $I_{R_k}$. Thus ACP cannot be solved.

We have just shown that there exist configurations that do not allow an omniscient observer to decide with certainty which devices have been impacted by massive anomalies and which ones have been impacted by isolated ones. We propose to relax Problem 1 by partitioning $A_k$ into three sets $M_k$, $I_k$ and $U_k$ such that $M_k$ and $I_k$ contain all the devices for which it is certain that these devices have been impacted by respectively massive and isolated anomalies. We have

\[ I_k = \{\ell \in A_k \mid \forall P_k, |P_k(\ell)| \leq \tau\} \quad (2) \]
\[ M_k = \{\ell \in A_k \mid \forall P_k, |P_k(\ell)| > \tau\} \quad (3) \]

Thus, whatever the anomaly partition $P_k$, $M_k \subseteq M_{P_k}$ and $I_k \subseteq I_{P_k}$. In particular $M_k \subseteq M_{R_k}$, $I_k \subseteq I_{R_k}$. On the other hand, set $U_k$ contains all the other devices $j \in A_k$ for which an omniscient observer cannot decide with certainty whether $j$ belongs to a massive anomaly or an isolated one. Formally,

**Definition 8 (Unresolved configuration):** Any device $j \in A_k$ is in an unresolved configuration if there exist two anomaly partitions $P_k$ and $P_k'$ such that $j \in I_{P_k}$ and $j \in I_{P_k'}$. The set of devices belonging to an unresolved configuration in the time interval $[k-1, k]$ is denoted by $U_k$.

**Corollary 4:** For any time $k \geq 1$,

\[ U_k = \emptyset \implies \text{ACP can be solved.} \]

**Proof:** Suppose that $U_k = \emptyset$. By Definition 8, it means that for any $j$ in $[1, n]$, either $j$ belongs to $M_k$ or $j$ belongs to $I_k$. Let us suppose that $j$ belongs to $M_k$. The same argument applies if $j$ belongs to $I_k$. By Relation 2, $j \in M_k \iff \forall P_k, |P_k(j)| > \tau$. In particular, $\forall P_k, M_{P_k} = M_{R_k}$. Any execution of Algorithm 1 allows us to build an anomaly partition $P_k$, and thus $M_{P_k}$.

We now formulate a relaxed version of ACP. Specifically, for any $k \geq 1$, for any system states $S_{k-1}$ and $S_k$, for any $A_k$, and $\tau \in [1, n-1]$, let $M_k, I_k$ and $U_k$ be respectively the set of devices involved in massive and isolated anomalies and those being in an unresolved configuration.

**Problem 2 (Relaxed ACP):** Is the omniscient observer always capable of building $M_k$, $I_k$ and $U_k$ such that

\[ M_k \subseteq M_{R_k} \text{ and } I_k \subseteq I_{R_k} \text{ and } M_k \cup I_k \cup U_k = A_k \]

without knowing $R_k$?

Section V presents necessary and sufficient conditions for any device $i \in A_k$ to belong to one of these three sets.

V. **Locally Deciding Whether One Belongs to $M_k$, $I_k$, or $U_k$**

In this section, we show how each device $j \in A_k$, $k \geq 1$, decides whether it belongs to $M_k$, $I_k$ or $U_k$. A naive approach consisting in generating all admissible anomaly partitions and then in deciding for each device whether it belongs to $M_k$, $I_k$, or $U_k$ is clearly impractical. Indeed, the number of these partitions is proportional to the Bell numbers, which is itself a sum of Stirling numbers of the second kind that is equal to $S(n, t) = \frac{1}{n!} \sum_{j=0}^{t} (-1)^{t-j} (t)^n$, where $n$ is the number of devices and $t$ the number of sets of the partition. Therefore, $S(n, t)$ grows exponentially with $n$. We propose to solve the relaxed ACP through a cheaper and local computation which relies uniquely on the knowledge of all the maximal $r$-consistent motions $j$ is involved in. Theorem 5 provides a necessary and sufficient condition (NSC) for $j \in A_k$ to belong to $I_k$. Theorems 6 and 7 give respectively a sufficient condition and a NSC for $j \in A_k$ to belong to $M_k$. Finally, Corollary 8 exhibits a NSC for $j \in A_k$ to belong to $U_k$.

A. **Necessary and Sufficient Condition to Belong to $I_k$**

We introduce the following two families $\mathcal{W}_k(j)$ and $\mathcal{W}_k(j)$ representing the family of all $\tau$-dense motions (resp. maximal $\tau$-dense motions) $j$ belongs to. We have

\[ M_k(j) = \{B \subseteq A_k \mid j \in B \text{ and } B \text{ has a } r\text{-consistent motion}\} \]
\[ \mathcal{W}_k(j) = \{B \in M_k(j) \mid B \text{ has a maximal } \tau\text{-dense motion}\} \]
\[ W_k(j) = \{B \in M_k(j) \mid B \text{ has a } \tau\text{-dense motion}\} \]

**Theorem 5:** For any $k \geq 1$, and for any $j \in A_k$, we have

\[ \mathcal{W}_k(j) = \emptyset \iff j \in I_k. \]
Proof: \((\Rightarrow)\) Let \(j \in A_k\). By assumption of the theorem, \(\overline{W}_k(j) = \emptyset\). Now, for any subset \(B \subseteq [1, n]\) having an \(r\)-consistent motion there exists a subset \(B' \subseteq [1, n]\) such that \(B \subseteq B'\) and \(B'\) is maximal (See Definition 3 and Remark 1). Thus, \(\overline{W}_k(j) = \emptyset \Rightarrow \forall k \in \mathbb{N}\). Therefore, by Definition 4, \(j\) solely belongs to \(\tau\)-sparse motions, and by Definition 5, for any anomaly partition \(P_k\), we have \(|P_k(j)| \leq \tau\). Therefore, by Definition 7, \(j\) can only be impacted by an isolated anomaly in the time interval \([k-1, k]\), thus \(j \notin I_k\).

\((\Leftarrow)\) We prove that \(\forall k \in \mathbb{N}\) \(\overline{W}_k(j) \neq \emptyset \Rightarrow j \notin I_k\). Suppose that \(\overline{W}_k(j) \neq \emptyset\). Thus, \(j \notin A_k\) and \(\overline{W}_k(j) \neq \emptyset\). Let subset \(B\) be such that \(B \in \overline{W}_k(j)\). We run Algorithm 1 by initially selecting \(j\) and \(B\) such that \(j \in B\) and \(B\) has a maximal \(r\)-consistent motion. By Lemma 2, Algorithm 1 builds a valid anomaly partition \(P_k\), such that \(B\) is an element of \(P_k\). We have, \(P_k(j) = B\). By construction of the proof, \(B \in \overline{W}_k(j)\), thus \(|B| > \tau\). We have exhibited an anomaly partition for which \(P_k(j) > \tau\). By Relation (2), \(j \notin I_k\), which completes the proof.

In the following we give a necessary and sufficient condition for \(j\) to belong to \(M_k\) (Theorem 7). Before that, we provide a sufficient condition for \(j\) to belong to \(M_k\). The rationale of this weaker condition (Theorem 6) is that, from a computation point of view, it is more efficient than the NSC one and meanwhile, misses to detect that \(j \in M_k\) in a very small number of scenarios (simulations show that in average less than 0.4% of the scenario are not covered by Theorem 6).

**B. A Sufficient Condition to Belong to \(M_k\)**

We have just shown that if there are not enough devices in the vicinity of \(j\) that belong to dense motions, then \(j\) has necessarily been impacted by an isolated anomaly. Suppose now that \(\overline{W}_k(j) \neq \emptyset\), that is \(j\) belongs to a family of \(\tau\)-dense motions, and denote by \(D_k(j)\) the set of all these devices that belong to \(\overline{W}_k(j)\). We have

\[
D_k(j) = \bigcup_{B \in \overline{W}_k(j)} B.
\]

We split set \(D_k(j)\) into two subsets \(J_k(j)\) and \(L_k(j)\), such that the former one contains all the devices for which all their maximal \(\tau\)-dense motions also contain \(j\), while the latter one contains all the devices that have at least one maximal \(\tau\)-dense motion that does not contain \(j\). Notice that we have \(j \in J_k(j)\) and \(j \notin L_k(j)\). Formally,

\[
J_k(j) = \{\ell \in D_k(j) \mid \exists B \in \overline{W}_k(\ell), j \in B\},
\]

\[
L_k(j) = \{\ell \in D_k(j) \mid \exists B \in \overline{W}_k(\ell), j \notin B\}.
\]

Figure 4 illustrates for device 4 \(\in S\) the decomposition of its neighbourhood \(D_k(4)\) into \(J_k(4)\) and \(L_k(4)\) for different configurations. We assume that \(\forall i \in S, i \in A_k\) and \(\tau = 2\). In Figure 4(a), \(S = \{1, 2, 3, 4, 5\}\). In this configuration, we have \(\overline{W}_k(4) = \{1, 2, 3, 4, 5\}\) and thus \(D_k(4) = \{1, 2, 3, 4, 5\}\). By definition, device 4 \(\in J_k(4)\). Devices 1 and 3 have a single maximal \(\tau\)-dense motion \(C_1 = \{1, 2, 3, 4\}\), and \(C_1\) contains 4. Thus 1, 3 \(\in J_k(4)\). In the same way, device 5 has also a single maximal \(\tau\)-dense motion \(C_2 = \{1, 2, 3, 4, 5\}\), \(C_2\) contains 4. Thus 5 \(\in J_k(4)\). Finally, by applying the same argument for device 2, we get 2 \(\in J_k(4)\). Putting altogether, we have \(J_k(4) = \{1, 2, 3, 4, 5\}\) and \(L_k(4) = \emptyset\).

In Figure 4(b), \(S = \{1, 2, 3, 4, 5, 6, 7\}\). Device 5 belongs to both \(C_2 = \{2, 4, 5\}\) and \(C_3 = \{5, 6, 7\}\), while device 4 does not belong to \(C_3\). Thus \(J_k(4) = \{1, 2, 3, 4\}, L_k(4) = \{5\}\).

Based on this neighborhood division, we enunciate the following theorem.

**Theorem 6:** For any \(k \geq 1\) and for any \(j \in A_k\),

\[
\exists B \in \overline{W}_k(j) \text{ such that } B \subseteq J_k(j) \implies j \in M_k
\]

**Proof:** The proof is done by contradiction. Let \(B\) be a set such that \(B \in \overline{W}_k(j)\) and \(B \subset J_k(j)\). Suppose that there exists an anomaly partition \(P_k = \{B_1, \ldots, B_t\}\) such that \(j \in I_{P_k}\). Two cases must be considered.

1) Let \(\ell \in B\) be such that \(|P_k(\ell)| > \tau\). By Definition 6, \(P_k(\ell)\) has a \(r\)-dense motion, thus \(P_k(\ell) \in \overline{W}_k(\ell)\). By Remark 1, let \(L\) be a set of \(\overline{W}_k(\ell)\) such that \(P_k(\ell) \subseteq L\). By assumption of the theorem, \(B \subseteq J_k(j)\), and thus, for any set of \(\overline{W}_k(\ell)\), \(j\) belongs to this set, and in particular \(j \notin I_{P_k}\). Therefore, \(P_k(\ell) \cup \{j\} \subseteq L\). By assumption of the proof, \(j \in I_{P_k}\), therefore \(j \notin P_k(\ell)\). Therefore, we have \(P_k(\ell) \cup \{j\} \neq L\) and so \(P_k(\ell) \cup \{j\}\) has an \(r\)-consistent motion, and its size is greater than \(\tau + 1\). Hence \(P_k(\ell) \cup \{j\}\) is \(\tau\)-dense, which contradicts condition C2 of Definition 6.

2) Suppose now that for any \(\ell \in L, |P_k(\ell)| \leq \tau\). We have \(B \subseteq \bigcup_{\ell \in B} P_k(\ell) \subseteq \bigcup_{|B| \leq \tau} B_i\). By assumption, \(B \subseteq \overline{W}_k(j)\). Therefore, \(B\) is a \(\tau\)-dense motion, which contradicts condition C1 of Definition 6.

Both contradictions conclude the proof.

We now present a necessary and sufficient condition that finds all the devices that belong to \(M_k\). Note that this condition is more intricate and requires substantially more computation than the necessary one exhibited in Theorem 6.

**C. Necessary and Sufficient Condition to Belong to \(M_k\)**

We first give an intuition of this condition by exhibiting the type of scenario that Theorem 6 does not cover. Figure 5 shows a system \(S = \{1, 2, 3, 4, 5, 6, 7, 8\}\) where each device in \(S\) belongs to \(A_k\). Suppose that \(\tau = 3\). We focus on device 1. The same argument holds for the other devices by symmetry of
the system states. We have $\overline{W}_k(1) = \{\{1, 2, 3, 4\}, \{1, 2, 7, 8\}\}$ and $D_k(1) = \{1, 2, 3, 4, 7, 8\}$. By definition, $J_k(1) = \{1, 2\}$ and $L_k(1) = \{3, 4, 7, 8\}$. As $|J_k(1)| < \tau$, there are no $\tau$-dense motions made of devices of $J_k(1)$. Thus the sufficient condition of Theorem 6 does not hold. Nevertheless, device 1 belongs to $M_k$ as for any anomaly partition $P_k$ of $A_k$, we have $|P_k(1)| > \tau$. Indeed, the only two anomaly partitions $P_k$ and $P_i$ of $A_k$ for $\tau = 3$ are respectively equal to $\{\{1, 2, 7, 8\}, \{3, 4, 5, 6\}\}$ and $\{\{1, 2, 3, 4\}, \{5, 6, 7, 8\}\}$. In both cases, we have $|P_k(1)| = |P_i(1)| > \tau$. Thus we have a configuration where device 1 belongs to $M_k$ while one cannot build a dense motion with devices in $J_k(1)$. The following theorem provides a necessary (and sufficient) condition for a device to belong to $M_k$.

**Theorem 7:** For any time $k \geq 1$ and for any $j \in A_k$, $j \in M_k$ if and only if $\overline{W}_k(j) \neq \emptyset$ and for all collections $C$ of pairwise disjoint sets defined by $C = \{B \in W_k(\ell) \mid \ell \in L_k(j), j \notin B\}$ one of the following two relations holds:

$$\exists A \in W_k(j) : A \subseteq D_k(j) \setminus \bigcup_{B \in C} B,$$

$$\exists B \in C : B \cup \{j\} \in W_k(j).$$

**Proof:** For both senses of the equivalence, their contrapositive is proven.

- Suppose that $j \notin M_k$. This means that there exists at least one anomaly partition $P_k = \{B_1, \ldots, B_t\}$ such that $|P_k(j)| \leq \tau$. Consider the collection $C_1$ defined by $C_1 = \{B \in P_k \mid |B| > \tau\}$. By definition of an anomaly partition, we have $\forall B, B' \in C_1, B \cap B' = \emptyset$. Now, by condition C2 of Definition 6, $\forall B \in C_1, B \cup \{j\}$ is not a $\tau$-consistent motion. As a consequence, $B \cup \{j\} \notin W_k(j)$.

Moreover, by definition of $C_1$, $\forall \ell \in D_k(j) \setminus \bigcup_{B \in C_1} B$, we have $|P_k(\ell)| \leq \tau$. Thus, $D_k(j) \setminus \bigcup_{B \in C_1} B \subseteq \bigcup_{B \in C_1} B$. By condition C1 of Definition 6, $\forall B \subseteq \bigcup_{B \in C_1} B$, $B$ is not a $\tau$-dense motion, and thus $B \notin W_k(j)$. Hence, we have $\forall A \in W_k(j), A \notin D_k(j) \setminus \bigcup_{B \in C_1} B$, which concludes the first part of the proof.

- We prove the second contrapositive.

1) Suppose that $W_k(j) = \emptyset$. By Theorem 5, $j \in I_k$ and thus we have $j \notin M_k$.

2) Suppose that $W_k(j) \neq \emptyset$ and $\exists C_1 \subseteq \{B \in W_k(\ell) \mid \ell \in L_k(j) \land j \notin B\}$ satisfying $|B \cap B'| = \emptyset, \forall B, B' \in C_1$ such that the following two relations hold:

$$\forall A \in W_k(j), A \notin D_k(j) \setminus \bigcup_{B \in C_1} B,$$

$$\forall B \in C_1, B \cup \{j\} \notin W_k(j).$$

Coming back to the example shown in Figure 5, we have $L_k(1) = \{3, 4, 7, 8\}$, and thus the family of sets $\{B \in W_k(\ell) \mid \ell \in L_k(1) \land 1 \notin B\}$ is equal to $\{\{3, 4, 5, 6\}, \{5, 6, 7, 8\}\}$. Two cases need to be considered.

1) $B = \{3, 4, 5, 6\}$.

2) $B = \{5, 6, 7, 8\}$.

Thus we have a $\tau$-dense motion and device 1 belongs to a massive anomaly in this configuration.

Therefore, as there are no other configuration satisfying $L_k(j) \neq \emptyset, \forall B, B' \in C_1$, all collections have been tested and thus device 1 $\notin M_k$.

**D. A Necessary and Sufficient Condition to Belong to $U_k$**

We end this section, by enunciating a corollary that derives from both Theorems 6 and 7. This corollary gives a necessary and sufficient condition for a device to belong to an unresolved configuration.

**Corollary 8:** For all times $k \geq 1$ and $j \in A_k$, $j \in U_k$ if and only if $W_k(j) \neq \emptyset$ and it exists a collection $C$ of pairwise disjoint sets defined by $C = \{B \in W_k(\ell) \mid \ell \in L_k(j), j \notin B\}$ such that the following two conditions hold:

$$\forall A \in W_k(j), A \subseteq D_k(j) \setminus \bigcup_{B \in C} B,$$

$$\forall B \in C : B \cup \{j\} \notin W_k(j).$$

**Proof:** Straightforward from case 2) of the proof of Theorem 7.

To summarize, we have derived conditions that allow any impacted device to decide whether many other devices have been impacted by the very same error or not. We have shown that concomitant errors may lead to unresolved configurations, that is states in which they cannot tell whether they have been impacted by a massive error or not. Finally, we have shown that each device $j$ only needs to know the trajectories that are at no more than $4\tau$ from itself to decide. A larger radius of knowledge – as the one got by an omniscient observer that samples at each time $k$ the system state, i.e., $S_k$ – does not bring any additional information and thus does not provide a higher error detection accuracy. The following two sections present respectively the local algorithms run by impacted devices, and the performance of these algorithms in terms of accuracy and complexity through extensive simulations.
Algorithm 2: j.maxMotions(N(j), i, ℓ, Mk(j))

Data: N(j); set of devices whose positions are at no more than distance 2r from j in E at both time k = 1 and time k;
Mk(j): current family of maximal r-consistent motions j belongs to; i: current dimension; ℓ = 0 current configuration, ℓ = 1 previous one.

Output: Mk(j)
1 begin
2 if i > d and ℓ = 0 then
3 ℓ ← ℓ + 1;
4 i ← i + 1;
5 else if N(j) \∈ Mk(j) and i ≤ d and ℓ ≤ 1 then
6 x_{set} ← \{ q_{k, \ell−1}(x) | x \in N(j) \};
7 x_m ← \min(x_{set});
8 N ← \{ x \in N(j) | x_m \leq q_{k, \ell−1}(x) \leq x_m + 2r \};
9 while x_{min} < q_{k, \ell−1}(j) and N \neq \emptyset do
10 Mk(j) ← j.maxMotions(N,i,ℓ,Mk(j));
11 x_{set} ← x_{set} \{ x_m \};
12 x_m ← \min(x_{set});
13 N ← \{ x \in N(j) | x_m \leq q_{k, \ell−1}(x) \leq x_m + 2r \};
14 else if \forall M \in Mk(j), N(j) \not\in M then
15 Mk(j) ← \{ M \in Mk(j) | M \not\subset N(j) \};
16 Mk(j) ← Mk(j) \cup \{ N(j) \};
17 return Mk(j);

VI. ALGORITHMS

This section presents the local algorithms implementing Theorems 5, 6, and 7 and Corollary 8.

From an algorithmic point of view, the determination of maximal r-consistent motions allows us to efficiently derive all the sets or families of sets needed to determine for each device j ∈ A_k whether it belongs to Mk, Ik, or to an unresolved configuration U_k. Algorithm 2 presents the pseudo-code run by any device j ∈ A_k to build the family Mk(j) of maximal r-consistent motions j belongs to (see Section V-A). The set N_j \in [1, n] contains all the devices whose positions are at no more than distance 2r from j in E at both time k = 1 and time k. N(j) is initialized to N_k(j) ∩ N_{k−1}(j). We denote by S_k(j) and S_{k−1}(j) the sets of their respective positions. Recall that E is a d-dimensional space. The core of the algorithm lies in moving, along each of the d dimensions, two sliding-windows W_{k−1} and W_k of width 2r with dimension d (i.e., hyper-rectangle of dimension d) over all the points in respectively S_{k−1}(j) and S_k(j) and in updating progressively Mk(j) with the new set of points B covered by the sliding-windows. Specifically, the position of a device ℓ in S_k(j) is given by p_k(ℓ) = (q_{1, \ell}(ℓ), q_{2, \ell}(ℓ), \ldots, q_d, \ell(ℓ)). Sliding-window W_k is initially positioned at pivot p_0 at position p_k(p_0) = (x_1, \ldots, x_d) with \forall i \in [1, d], x_i = \min_{j \in N_k(j)} q_{i, \ell}(j). The same construction applies for the initial positioning of W_{k−1} at pivot p_{k−1}(0). Mk(j) is fed with the set of points that are covered by both sliding-windows W_k and W_{k−1}. Then W_k is moved to its next pivot p_1 whose position is given by p_k(p_1) = (p_{1,k}(p_1), x_2, \ldots, x_d) with p_{1,k}(p_1) = \min_{j \in N_{k−1}(j)} q_{1, \ell}(ℓ) | q_{1, \ell}(ℓ) > p_{1,k}(p_0)), and the set of points that are covered by both sliding-windows W_k and W_{k−1} are appended to Mk(j). Note that if this new set B includes an existing one B’ in Mk(j) then B replaces B’ (lines 17–19). Sliding-window W_k continues to move along the first dimension until either the first coordinate of the pivot is equal to p_{1,k}(j) or the intersection between W_k and W_{k−1} is empty. At this point, W_k is moved to its next position along the second dimension and the same process is reiterated until W_k has been moved along the d dimensions. If N_k(j) ∩ N_{k−1}(j) \not\subset Mk(j) then sliding-window W_{k−1} is moved to its next pivot (which is computed as for W_k) and W_k is re-positioned to its initial pivot p_k(0). This is achieved in a recursive way.

Algorithm 3 presents the pseudo-code run by any device j ∈ A_k to determine whether it has been impacted by an

Algorithm 3: j.characterize()

Data: N(j) = N_k(j) ∩ N_{k−1}(j); set of devices whose positions are at no more than distance 2r from j in E at both time k = 1 and k; τ: density threshold.

Output: Type of the anomaly impacting j (i.e., I, M, or U)
1 begin
2 Mk(j) ← j.maxMotions(N(j),0,{},());
3 W_k(j) ← \{ M \in Mk(j) | |M| > τ \};
4 if W_k(j) = \emptyset then
5 anomaly ← Isolated;
6 else
7 J ← 0;
8 L ← 0;
9 for M \in W_k(j) do
10 for ℓ \in M do
11 Mk(ℓ) ← j.maxMotions(N(ℓ),0,{},());
12 W_k(ℓ) ← \{ M' \in Mk(ℓ) | |M'| > τ \};
13 if \exists M' \in W_k(ℓ) such that j \notin M' then
14 L ← L \cup \{ ℓ \};
15 else
16 J ← J \cup \{ ℓ \};
17 if \exists M \in W_k(j) such that |M \cap J| > τ then
18 anomaly ← Massive;
19 else
20 anomaly ← Unresolved;
21 return anomaly;

Algorithm 4: j.fullcharacterize()

23 S ← \bigcup_{ℓ \in I} D_k(ℓ);
24 S ← S \setminus \{ j \};
25 C ← \{ \};
26 R ← L;
27 while R \neq 0 and \neg j.check(C) do
28 Take any ℓ \in R;
29 R ← R \setminus \{ ℓ \};
30 C ← j.isolate(S,L \setminus \{ ℓ \},C,ℓ);
31 if j.check(C) then
32 anomaly ← Unresolved;
33 else
34 anomaly ← Massive;
isolated anomaly (lines 4–5, direct application of Theorem 5), by a massive one (lines 6–21, direct application of Theorem 6) or whether it is in an unresolved configuration (line 23). In the latter case, if \( j \) wants to know whether it has impacted by a massive anomaly then it runs the necessary and sufficient condition presented in Theorem 7. This consists in replacing line 20 of Algorithm 3 by the pseudo code presented in Algorithm 4. This algorithm iterates over all the devices in \( L_k(j) \) and looks for a collection of dense motions containing devices in \( L_k(j) \) (procedure isolate()) until one satisfies Relation 8 of Corollary 8 which is achieved by procedure check().

### VII. Performance Evaluation

#### A. Simulation settings

This section is devoted to the performance study of our algorithms. Four main aspects have been analysed. The complexity in time has been evaluated by measuring the average number of operations executed per device to be able to take a decision (i.e., Isolated/Massive/Unresolved). Then the effectiveness of Theorem 6 with respect to Theorem 7 has been analysed by measuring the percentage of massive anomalies that Theorem 6 misses to detect. The adaptivity of our algorithms to various sampling frequencies has been studied. Finally, the pertinence of our model with respect to a ground truth has been evaluated by measuring the number of isolated errors that are considered as massive ones due to restriction R3 of the model. All these results have been obtained by running extensive simulations. We have tested around 10,000 different settings of the following parameters: \( n \), the number of devices in the system, \( \tau \) the threshold that distinguishes massive from isolated anomalies, and \( r \) the consistency impact radius. The number of services \( d \) accessed by each devices has been set to 2, leading to a 2-dimensional QoS space \( E \). The initial distribution of the devices in \( E \) follows a uniform distribution, denoted by \( S_0 \). Then for each discrete time \( k \geq 1 \), configuration \( S_k \) is generated as follows:

A number \( A \) of points with \( A \in [1, 80] \) are randomly chosen in \( S_{k-1} \). Then, for each chosen point \( j \), with probability \( G \) less than \( \tau \) points are randomly chosen in a ball of radius \( r \) centred at \( j \), and with probability \( 1 - G \), \( t \) points are randomly chosen in a ball of radius \( r \) centred at \( j \), with \( t \) varying from \( \tau \) to the number of points in this ball. This allows to respectively simulate isolated and network errors. In both cases, all these chosen points \( \ell \) are moved to another location uniformly chosen in \( E \), and \( a_{\ell}(j) \) is set to \( \text{true} \).

We now precise how both parameters \( r \) and \( \tau \) are selected. As previously said in Section III-C, if strictly less than \( \tau + 1 \) devices have an abnormal trajectory due to the same error then none of these devices can belong to a \( \tau \)-dense motion. In other words, we need to tune parameters \( r \) and \( \tau \) in such a way that the probability of having more than \( \tau \) errors impacting devices, which are at no more than \( 2r \) from each other, is negligible. We denote by \( N_r(j) \) the random variable representing the number of devices in the vicinity of device \( j \) and by \( F_r(j) \) the random variable equal to the number of devices impacted by an isolated error in the vicinity of device \( j \). We have

\[
\mathbb{P}\{N_r(j) = i\} = \binom{n-1}{i} q_1^{(1-q_1)} (1-q_j)^{n-1-i},
\]

where \( b \) is the probability that an isolated error impacts a device and \( q_j \) the probability that a device \( \ell \) is in the vicinity of device \( j \). Given the position \( p(j) \) of device \( j \), the vicinity \( V \subset E \) of device \( j \) is defined by \( V = \{ x \in E \mid \|x - p(j)\| \leq 2r \} \). We are interesting in computing \( \mathbb{P}\{F_r(j) > \tau\} \). We have

\[
\mathbb{P}\{F_r(j) > \tau\} = 1 - \sum_{\ell=0}^{\tau} \mathbb{P}\{F_r(j) = \ell\}
\]

where

\[
1 - \sum_{m=0}^{n-1} \sum_{\ell=0}^{\tau+m} \mathbb{P}\{F_r(j) = \ell \mid N_r(j) = m\} \mathbb{P}\{N_r(j) = m\}
\]

\[
= 1 - \sum_{m=0}^{n-1} \sum_{\ell=0}^{\tau+m} \binom{m}{\ell} b^\ell (1-b)^{m-\ell} \mathbb{P}\{N_r(j) = m\}.
\]

Now, given a small constant \( \varepsilon \), \( r \) and \( \tau \) are tuned so that the probability of having more than \( \tau \) independent errors that impact close devices is negligible, that is \( \mathbb{P}\{F_r(j) \leq \tau\} < 1 - \varepsilon \). Figure 6(a) plots the curve of the cumulative distribution function of \( N_r(j) \) as a function of the size \( m \) of \( j \) neighbourhood and for different values of \( r \). This curve clearly illustrates the impact of \( r \) on the size \( m \) of \( j \) neighbourhood. An interesting value for a total population of \( n = 1000 \) devices is \( r = 0.03 \) which guarantees that for a value of \( m \) logarithmic in the size of the population of the system, the probability of having more than \( \tau \) independent errors that impact close devices is negligible. Figure 6(b) plots \( F_r(j) \) as a function of the system size \( n \) when \( r \) is set to 0.03. In the following \( r = 0.03 \) and \( \tau = 3 \).

#### B. What brings Theorem 7 with respect to Theorem 6

We have derived in Theorem 7 a necessary and sufficient condition for any device \( j \in A_k \) to decide with certainty that it
TABLE II

AVERAGE REPARTITION OF POINTS OF $A_k$ IN EACH SET $I_k$, $M_k$, AND $U_k$.

SETTINGS $A = 20$, $n = 1000$, $r = 0.03$, $\tau = 3$ AND $|\Lambda_k| = 95.7$.

<table>
<thead>
<tr>
<th>Algorithm (Theorem)</th>
<th>1.85</th>
<th>2,450,150</th>
<th>31,108</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm 3 (Theorem 6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Algorithm 4 (Theorem 7)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

TABLE III

AVERAGE COMPUTATIONAL COST FOR EACH DEVICE IN $I_k$, $M_k$, $U_k$.

SETTINGS $A = 20$, $n = 1000$ $\tau = 0.03$, $\tau = 3$ AND $|\Lambda_k| = 95.7$.

<table>
<thead>
<tr>
<th>Algorithm (Theorem)</th>
<th>1.85</th>
<th>2,450,150</th>
<th>31,108</th>
</tr>
</thead>
<tbody>
<tr>
<td>Algorithm 3 (Theorem 6)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Algorithm 4 (Theorem 7)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Any online detection system should be able to quickly identify the presence of isolated or massive anomalies to rapidly fix or confine the events or errors that lead to these anomalies. Typically, this largely depends on the frequency at which the system can sample the QoS information of the devices it monitors. In our approach, the frequency of QoS information sampling is locally tuned, and only depends on the local occurrence of anomalies. Thus by avoiding any kind of global synchronization, devices can efficiently provide a fine grain event/errors detection without impacting the rest of the system. An enjoyable consequence of this local tuning is that devices can afford to increase the frequency at which they sample their neighborhood, decreasing accordingly the number of concomitant errors and thus the number of unresolved configurations. This is illustrated in Figure 7. This figure shows the percentage of unresolved configurations as a function of the number of errors generated between two snapshots of the system and the type of errors (that is when $G = 1$, only isolated errors are generated, while for $G = 0$ up to all the devices in the vicinity of an impacted device can be impacted). This figure confirms the fact that when a single error (isolated or massive) is generated then no unresolved configurations exists. Now for an increasing number of errors, the number of unresolved configurations augments. Note that the impact of massive errors is more significant on the number of unresolved configurations because it increases the number of configurations where a device can belong to several maximal dense motions.

D. Pertinence of Restriction R3

We finally show that the impact of Restriction R3 on the accuracy of $I_k$ and $M_k$ is relatively weak. Indeed, to model the impact of errors, we have assumed that if a device belongs to a $\tau$-dense motion then this device has necessarily been impacted by an error that has impacted many other devices. While
relevant in many situations, we show in the following the proportion of devices for which the second part of Restriction R3 does not hold. Figure 8 shows the proportion of devices that claim to have been impacted by a massive error (in accordance with our model) although it was an isolated one, as a function of the frequency of the snapshots (represented by the number of generated errors between two snapshots). This figure shows that in the worst case, this proportion is less than 10%, and it remains constant whatever the number of errors. Which is an interesting result. Finally, Figure 9 shows that Restriction R3 has no impact on the number of unresolved configurations, which comes from the fact that unresolved configurations are essentially due to the superposition of massive errors.

VIII. CONCLUSION

This paper has been devoted to the on-line detection of errors or events in large scale systems according to the extent of their damage. We have proposed a new approach that fully relies on the local knowledge of each impacted device to provide the monitoring application the essential information that should help them to be continuously aware of the state of the system. This has been achieved by modelling the impact of errors on devices as consistent and close trajectories in a QoS space. We have derived necessary and sufficient conditions locally applicable. We have validated the pertinence of our model by comparing the output of our algorithms with a large spectrum of scenarios of errors. Finally, by design, our approach is scalable. As future work, we plan to extend our characterization to take into account malicious devices. In particular, we will study the presence of collusion of malicious devices whose aim would be to prevent an impacted device to be detected by the monitoring application.

REFERENCES