Multimedia Tools and Applications (2021) 80:16805–16825
https://doi.org/10.1007/s11042-020-09050-x

A re-organizing biosurveillance framework based on fog and mobile edge computing

Mohammad Al-Zinati[1] · Reem Alrashdan[1] · Basheer Al-Duwairi[2] · Moayad Aloqaily[3]

Received: 30 December 2019 / Revised: 27 April 2020 / Accepted: 7 May 2020 /
Published online: 23 May 2020

Abstract
Biological threats are becoming a serious security issue for many countries across the world. Effective biosurveillance systems can primarily support appropriate responses to biological threats and consequently save human lives. Nevertheless, biosurveillance systems are costly to implement and hard to operate. Furthermore, they rely on static infrastructures that might not cope with the evolving dynamics of the monitored environment. In this paper, we present a reorganizing biosurveillance framework for the detection and localization of biological threats with fog and mobile edge computing support. In the proposed framework, a hierarchy of fog nodes are responsible for aggregating monitoring data within their regions and detecting potential threats. Although fog nodes are deployed on a fixed base station infrastructure, the framework provides an innovative technique for reorganizing the monitored environment structure to adapt to the evolving environmental conditions and to overcome the limitations of the static base station infrastructure. Evaluation results illustrate the ability of the framework to localize biological threats and detect infected areas. Moreover, the results show the effectiveness of the reorganization mechanisms in adjusting the environment structure to cope with the highly dynamic environment.

Keywords Mobile edge computing · Fog computing · Biosurveillance systems · Edge cloud data management

1 Introduction

With the emergence of the recent COVID-19 outbreak, several contact-tracing applications have been proposed to alert users if they have come in close contact with someone who

✉ Mohammad Al-Zinati
mhzinati@just.edu.jo

Extended author information available on the last page of the article.

tested positive for COVID-19. For instance, Google and Apple launched a joint COVID-19 tracing tool for iOS and Android that employs Bluetooth technology to alert users if they have come in close contact with someone who has tested positive for COVID-19. The government of Singapore, China, and Austria also launched similar applications for contact tracing.

Nevertheless, none of the proposed applications has considered the possibility of a contaminated environment and its role in transmitting the disease. According to a recent report from the world health organization [56], it is vital to include environmental sampling as part of the comprehensive outbreak investigation and combine environmental sampling with the results of COVID-19 patient investigations. Nonetheless, the suggested protocol for sampling the environment is limited to the hospitals and other health care facilities that have a high possibility of being contaminated with the virus. Other possibly contaminated areas of the environment, such as grocery stores, service areas, and workplaces, are not considered. As the proposed framework in this paper is able to identify and localize such infected areas, it can provide a tool for epidemiological investigation teams that supports the efficient sampling of the environment to detect potential threats. Effective localization of these threats can help in applying the required actions or the appropriate quarantine necessary to contain the spread of the infection promptly.

Over the past years, researchers and practitioners have made significant efforts to develop effective biosurveillance systems. The purpose of these systems is to early detect biological threats before being clinically recognized [9, 15]. Research findings suggest that effective biosurveillance systems largely support appropriate responses to biological incidents and alleviate their threats [36, 37].

Rapid Syndrome Validation Project (RSVP) [4], Real-Time Outbreak Disease Surveillance (RODS) [51], BioSense [17], and Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE) [13] are examples of popular real-world biosurveillance systems that rely on monitoring information combined from from various sources. Nevertheless, according to the Centers for Disease Control and Prevention (CDC), many countries are still incapable of implementing and deploying effective biosurveillance systems due to several economic and technological factors [18].

To overcome this limitation, researchers investigated building scalable and reliable biosurveillance systems that integrate the use of wearable sensors technologies with mobile-edge and cloud computing platforms [2, 3, 50]. However, none of these systems is capable of localizing the origin of biological threats.

In this paper, we propose a reorganizing biosurveillance framework for the localization of biological infections. The framework is organized as a hierarchy of agent-based infrastructural elements. At the lower-level, wearable biosensors and personal smartphones continuously monitor and analyze the humans' vital signs. At the higher-level, a hierarchy of software agents deployed on fog nodes are responsible for aggregating monitoring data within their assigned regions and detecting potential threats. Moreover, the framework provides an adaptive multi-agent system for reorganizing the monitored environment structure to cope with the evolving dynamics and to alleviate the consequences of the static hosting infrastructure.

We organize the rest of this paper as follows. In Section 2, we discuss existing related works. In Section 3, we illustrate the architecture of the framework and its incorporated threat detection technique. In Section 4, we present the reorganization mechanism. In Section 5, we discuss the experiments we designed to evaluate our framework and present the results. Finally, we conclude the paper and give future work directions in Section 6.

2 Related work

Early detection and immediate response to bioterrorism attacks and disease outbreaks are among the highest priorities in today's modern societies and represent a significant issue at the national security level [25]. Dealing with emerging epidemics and bioterrorism attacks requires real-time tracking of infectious diseases, continuous surveillance, and very fast, highly accurate data analysis [21]. An efficient biosurveillance system would have the benefit of enhancing the quality of healthcare, reducing healthcare costs, and controlling disease outbreaks. Traditional biosurveillance systems depend on analyzing data collected about epidemic diseases (Syndromic Surveillance Systems), data collected from medical lab tests (Laboratory Surveillance Systems), or through environmental monitoring (Environmental Surveillance Systems). Recently, with the remarkable advancements in smart healthcare technology, several edge computing, and IoT-based frameworks have been proposed for biosurveillance. In the following subsections, we discuss the main research efforts in each category.

2.1 Syndromic surveillance systems

Several systems have been developed in recent years to gather and analyze syndromic data obtained from patient records and social media about major epidemic diseases such as influenza-like illness, West Nile virus, Ebola virus, Zika virus, et. The proposed systems in this category rely on data gathered from various sources such as emergency rooms, clinical and hospital records, ambulance dispatch calls, and pharmaceutical retail sales [52]. These systems work by analyzing the gathered data to extract distinctive patterns that characterize well-known health threats [16, 20].

Popular examples of these systems include BioSense [17], Real-Time Outbreak Disease Surveillance (RODS) [51], Rapid Syndrome Validation Project (RSVP) [4], New York City syndromic surveillance systems [24], Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE) [13], National Bioterrorism Syndromic Surveillance Demonstration Program (NBSSD) [29], Oak Ridge Bio-surveillance Toolkit (ORBiT) [41], Integrated Forecast and Early Enteric Outbreak (INFERNO) [34],and the CDC's Early Aberration Reporting System (EARS) [27].

Despite their exciting results, syndromic surveillance systems require access to patients' private health records [30]. Moreover, they might generate high false-positive rates [59]. Finally, there is no evidence that they can work well for global surveillance. An interesting discussion about the challenges of syndromic surveillance systems is given in [8].

2.2 Laboratory surveillance systems

Medical lab tests provide a reliable source of information about infection cases. Therefore, laboratory surveillance systems work by combining accurate and confirmed test results to detect possible infection outbreaks. For laboratory surveillance systems to operate, it is necessary to create a network of specialized medical labs that are capable of sharing and exchanging test results about a specific health security threat.

For example, the California Department of Health Services (CDHS) deployed an automated laboratory-based disease reporting system [10]. Moreover, a cloud computing-based hospital automated laboratory reporting system was proposed in [55] to efficiently exchange medical laboratory test results about infectious diseases.

It is important to note here that laboratory surveillance systems can be combined with syndromic surveillance systems to increase the accuracy of disease outbreak detection. Nevertheless, laboratory surveillance systems require a considerable amount of time to operate and produce useful results. As such, they are not fit to meet the timely response requirement in case of biological attacks. Furthermore, as these systems work as unified networks, the varying capacities of member labs and their different information sharing regulations greatly influence the overall effectiveness of threat detection efforts [54].

2.3 Environmental biosurveillance systems

Due to the privacy issues of personal health information, several efforts have investigated using data collected by specialized environmental sensors distributed over different areas of the monitored environment [19, 28].

Biowatch is an example of an environmental biosurveillance system that uses a network of aerosol sensors deployed in 31 major US cities [42]. In [61], Yang et al. proposed a similar system that uses a wireless sensor network for the real-time monitoring of CO concentration. The system employs a low-frequency modulation method to improve the detection accuracy based on the CO concentration readings collected by the specialized sensors.

As discussed above, environmental biosurveillance systems do not violate the privacy of humans as they do not rely on any personal data. However, their installation, operation, and maintenance costs are relatively high, and their coverages are only limited to the locations where the sensors are deployed.

2.4 IoT-based surveillance systems

The rapid developments in the area of the Internet of Things (IoT) and their integration with fog, edge, and cloud computing technologies provide an ideal platform for a new generation of advanced surveillance systems. To this end, several IoT-based surveillance systems were proposed in recent years (e.g., [7, 11, 12, 46, 49, 50, 53, 58]). In these systems, IoT based sensors and other edge devices collect and initially process raw data. After that, they transmit the initially processed data to nearby fog devices that are capable of performing further processing. Ultimately, fog nodes send the aggregated data to cloud computing platforms that implement more in-depth analysis and events correlation to extract useful health information.

For instance, Salahuddin et al. [43] proposed a health care system based on an edge computing model. In their model, they define an edge layer composed of smart edge gateway devices serving as a bridge between a wireless sensor network and a public connected network. The used edge devices can analyze data and issue appropriate warnings in case of emergency conditions.

Besides, several other research efforts have focused on addressing scalability and performance issues resulting from the massively collected data [1, 32, 35, 38–40, 57, 60], and on enhancing the security level through addressing privacy-related issues of these systems [1, 31].

In addition to the above-discussed frameworks, recent studies have investigated the possibility of utilizing recent advances in IoT-Based bio-sensors, fog, and cloud computing to implement a variety of health monitoring systems. Table 1 provides a summary of these studies. As illustrated in the table, most of these systems use a combination of bio-sensors,

Table 1 Related IoT-based surveillance systems

System	Purpose	IoT	Fog	Cloud
Giger et al. [23]	Healthcare monitoring	N	N	N
Gia et al. [22]	Cardiac diseases monitoring	Y	Y	Y
Sandhu et al. [45]	MERS-COV prediction	Y	N	Y
Sandhu et al. [44]	H1N1 monitoring	N	N	Y
Bhatia and Sood [14]	ICU monitoring	Y	N	Y
Hossain and Muhammad [26]	Emergency healthcare	Y	Y	Y
Nandyala and Kim [33]	IoT based healthcare	Y	Y	Y
Sareen et al. [46]	Zika virus monitoring	Y	Y	Y
Sood et al. [48, 49]	Chikungunya virus monitoring	Y	Y	Y
Sood and Mahajan [50]	Mosquito-Borne Diseases monitoring	Y	Y	Y
Sood et al. [47]	Dengue fever monitoring	Y	Y	Y

fog, and cloud computing technologies to gather and aggregate health information. The collected data is then used to classify and monitor the infection status of individual people with specific diseases.

Despite the effectiveness of the proposed systems in classifying the type of infection for individual cases, none of these systems propose a mechanism to localize the origin of these infections. Localization of threat origins becomes very important in the case of purposeful biological attacks. Furthermore, all of the proposed systems rely on the existing static base station infrastructure that is fixed at predefined locations. Nevertheless, in the case of biological attacks, the monitored environment becomes highly dynamic, and some areas might become overloaded while other regions might become empty. In this case, the benefits gained by using the edge and fog platforms might be wasted. Extending the existing systems to adapt to the highly dynamic nature of the monitored environment is a challenging task that still needs further investigation.

In this paper, we present a reorganizing biosurveillance framework for the detection and localization of biological threats. We organize the elements of the proposed framework in a hierarchical architecture. At the lower-level, wearable sensors continuously monitor and analyze humans vital signs. At the higher-levels, a hierarchy of fog nodes aggregate and process monitoring data to detect possible infections. The choice of fog computing platforms allows for future extension of the framework to support real-time proactive system for warning population close to infectious threats and guide them to safe places in case of emergencies. Although traditional fixed base stations host our fog nodes, the framework continuously reorganizes the monitored environment structure to cope with the evolving environmental conditions.

3 The initial framework for biological threats localization

In this section, we present our initial framework for the localization of biological infections that we built by extending our earlier framework that is presented in [5]. We start by describing the framework's architecture, and we discuss its incorporated threat localization technique. After that, we explain the limitations of our earlier framework and address the need for its extension to overcome its current limitations.

3.1 Architecture of the framework

As depicted in Fig. 1, we define the proposed Framework as a hierarchy of infrastructural computing elements. At the lower level, wearable sensors continuously measure the vital signs of monitored humans. The readings are then captured and initially processed at the edge by *personal agents* hosted on the accompanying smartphones to detect possible abnormalities. Bio-surveillance systems are known to be costly to implement. As such, we are proposing to utilize ubiquitous smartphone devices and existing base stations infrastructure to deploy our framework and implement its functionalities. Concerning the wearable biosensors technology, it is important to mention here that these sensors are not limited to special textiles that are equipped with biosensors. Tech companies recently started to incorporate smartphone accessories, such as earbuds and smartwatches, with biosensors that can easily capture several vital signs and transmit them to an attached smartphone.

As we are utilizing the existing base station infrastructure, we partition the environment into a set of smaller areas named cells. The cell size is defined by the district that is covered by the base station. Moreover, we assign each cell a *Cell Manager* agent that is responsible for collecting monitoring data within its cell. The cell manager periodically sends the aggregated data to the corresponding higher-level *Regional Manager* agent that combines the received data to detect potential threats within its region.

It is important to note here that cell and regional managers can be deployed on any distributed computational platforms. However, the choice of a fog computing platform allows for future extension of the framework to support real-time proactive system for warning population close to infectious threats and guide them to safe places.

As the environment might contain multiple infected areas, it is necessary to cluster cells with related infection information into the same regions. To this end, we define the *Coordinator* agent to oversee the distribution of cells within regions and redistributes them again when necessary to create regions with focused information. As the coordinator requires global knowledge about the whole monitored environment to operate, we opt to install the coordinator on a cloud infrastructure. The effect of latency issues between the coordinator and regional managers are marginal to the work of the coordinator. Moreover, a

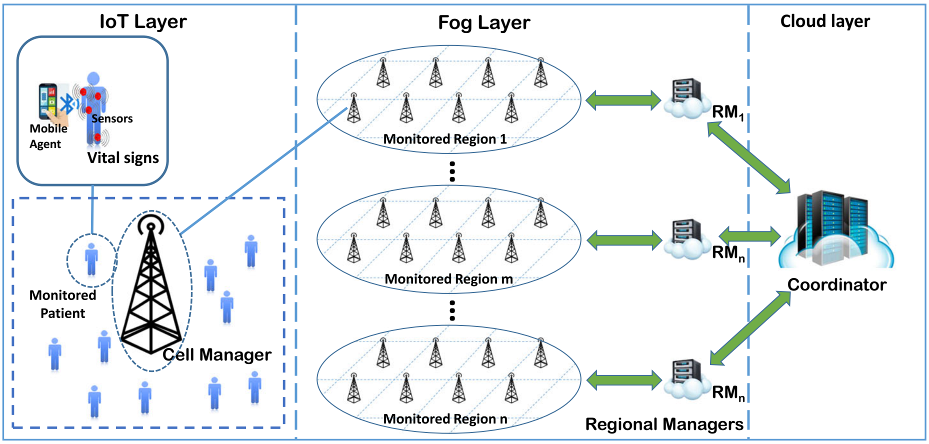

Fig. 1 Architecture of the proposed framework

cloud platform provides powerful resources that can support the scalability of the overall framework.

3.2 Identifying infected areas

While performing their daily chores, monitored humans might navigate different cells of the environment. Once a human passes by a biologically infected area, he will become infected. Nevertheless, abnormal vital signs will not immediately appear. Instead, they will reveal after a variable amount of time that depends on the strength of their immunity systems.

As more infected humans cross a cell, there is a higher possibility for this cell to be infected. In the same manner, as more non-infected humans cross a cell, there is a lower possibility for this cell to be contaminated. Also, as more humans get infected without crossing a specific cell, it is more likely that this cell is not contaminated.

To decide the likelihood of a cell of being contaminated, we use the observations mentioned above to assess the similarity between the traversal information of a specified cell and the infection patterns of humans who traversed that cell. As the Jaccard similarity coefficient realizes all of the above perceptions, we opt to use it to evaluate this similarity. As the traversal information of a specified cell is more similar to the infection pattern, the specified cells are more likely to be infected. In our framework, we consider the computed Jaccard similarity as the suspiciousness score of the cell for being infected, and we calculate it as follows:

$$Suspiciousness(C) = \frac{I_T(C)}{I_T(C) + I_U(C) + N_T(C)} \tag{1}$$

where, $I_T(C)$ is the number of infected persons who navigated C, $I_U(C)$ is the number of infected persons who did not navigate C, and $N_T(C)$ is the number of not infected persons who navigated C.

The regional managers continuously compute ordered lists of cells in their regions according to their Suspiciousness scores. The higher the order of a cell, the more likely it is infected.

For instance, Fig. 2 illustrates an example of a monitored environment with 9 equally-sized cells and three monitored humans. The spot highlighted in yellow inside cell 5

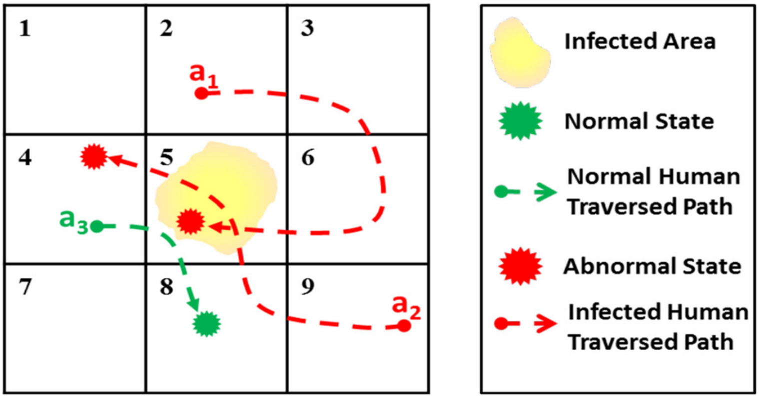

Fig. 2 Example of a monitored environment

Table 2 The aggregated data and the suspicion score in all cells

Cell	1	2	3	4	5	6	7	8	9
N_{TI}	0	1	1	1	2	1	0	1	1
N_{UI}	2	1	1	1	0	1	2	1	1
N_{TN}	0	0	0	1	1	0	0	1	0
Suspicion score	0	0.5	0.5	0.3333	0.6667	0.5	0	0.3333	0.5
Suspicion rank		2	2	3	1	2		3	2

represents an infected area. As a human passes an infected area, he will become infected (a_1 and a_2) after a variable incubation time. On the other hand, other humans who do not pass infected areas (a_3) will not be infected (represented by green dashed lines).

Table 2 illustrates the results of suspicion scores computed for all cells using (1). As can be seen from the results, cell 5 has the highest suspicion score and, as such, has the highest possibility of containing an infected area. These results conform to the actual infected area, as shown in Fig. 2.

3.3 Multiple-threat detection

In the case of the existence of multiple infected areas in the environment, it is common that variant numbers of humans cross different infected areas. Therefore, infected areas with a relatively small number of crossing humans will be ranked low in the suspiciousness list. The problem becomes more visible as the variance in the number of humans crossing different infected areas increases.

The framework solves the issue of the variant distribution of humans across the monitored environment by grouping cells related to the same threat inside the same region. To this end, the cell managers gather infection information from monitored humans within their areas. Then, they work with region managers to measure the distance between the collected data using an exclusive representation. Finally, they pass the calculated measures to the coordinator that rearranges the regions to group related cells within the same regions. The region managers can then use the newly formed regions to localize biological threats within each region. Detailed information on measuring the distance between monitoring information and creating focused regions can be found in [5].

3.4 Limitations of the initial framework and motivations for extension

The proposed framework assumes a fixed cell size. However, it is evident through experiments that the cell size significantly impacts the effectiveness of the framework. A larger cell size causes monitored humans to cross cells that contain infection threats but without actually crossing the particular infected portion of the cell. Hence, the monitoring agent will mark the cell as clear of infections while it is infected. The wrong specification of cell status will negatively impact the accuracy of the results.

On the other hand, using a smaller cell size results in an additional number of cells. In this case, infected areas might span more cells, and the same problem starts to appear.

Moreover, minimizing the cell size improves the accuracy of the results to a specific limit. Further minimization of cell size will negatively affect the accuracy of the framework, as indicated by the results. This effect is related to the additional number of cells that results in noise in the collected monitoring information.

It is important to mention here that the continuous evolving conditions of the moving humans and the randomness of biological attacks make it impossible to define an optimal cell size in advance. Given the previously mentioned conflicting objectives, there is a crucial need for developing a reorganizing technique that adjusts the cell size to adapt to the evolving nature of the monitored environment.

4 A Reorganizing biosurveillance framework

We start this section by providing an overview of the proposed framework, and then we present its re-organization methods.

4.1 General overview

The re-organization process starts by gathering the monitoring information from the personal agents. As discussed in Section 3, personal agents continuously capture the recorded vital signs and process them to detect any abnormality. After that, the cell managers periodically aggregate monitoring information from Personal agents within their cells. Periodically, the Coordinator regularly oversees the distribution of cells over regions and re-distribute them, if necessary, to improve the accuracy of the framework. After receiving the aggregated monitoring-information, regional managers use the information within their regions to find a cell structure setting that improves the effectiveness of localizing infected areas. For this sake, the regional manager progressively splits the identified suspicious cells into a set of smaller cells to find a cell structure setting that improves the overall accuracy of the framework. As the information of the monitored environment continuously evolves, the framework regularly repeats the re-organization process to cope with the dynamic nature of the environment.

Our initial framework description in [5] contains detailed information on the process of re-organizing cells across regions. In this section, we focus our discussion on the process of re-organizing the cells within each region to find its best cell structure settings.

4.2 Re-organization within the region

At initialization time, the monitored environment is initially divided into a set of cells. The original cell size is defined by the maximum area that can be covered by the base station that hosts the cell manager. To improve the accuracy of the framework, the regional manager periodically re-organizes the cell structure settings within its region. Algorithm 1 illustrates the re-organization process.

In the remainder of this section, we use the case study in Fig. 3 to illustrate the various steps of the re-organization algorithm. Figure 3 presents an example of a monitored environment that consists of 32 equally sized cells organized into two regions according to the technique discussed in Section 3. Each regional manager is responsible for individually implementing Algorithm 1 to re-organize the cell structure settings within its region.

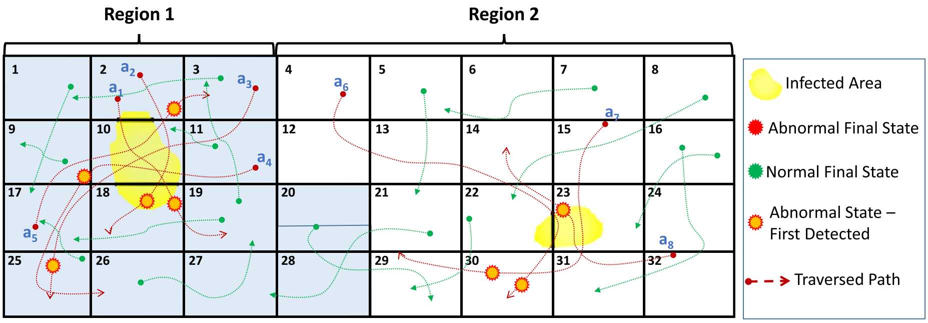

Fig. 3 A monitored environment that consists of 32 cells organized into two regions

Algorithm 1 Reorganization within the region.

```
1  Procedure REORGANIZEWITHINREGION
   input  : $\mathcal{C}_{\mathcal{RG}}$
   output: $\Re$
2  begin
3      $\Re \leftarrow$ SUSPICIONRANKING($\mathcal{C}_{\mathcal{RG}}$)
4      $\Omega \leftarrow$ MAXIMUMRANK($\Re$)
5      repeat
6          $\mathcal{C}'_{\mathcal{RG}} \leftarrow$ SPLITCELLS($\mathcal{C}_{\mathcal{RG}}$)
7          $\Re' \leftarrow \Re$
8          $\Re \leftarrow$ SUSPICIONRANKING($\mathcal{C}'_{\mathcal{RG}}$)
9          $\Omega' \leftarrow \Omega$
10         $\Omega \leftarrow$ MAXIMUMRANK($\Re$)
11     until $\Omega' > \Omega$
12     return $\Re'$
```

Region 1 contains a single infected area (highlighted in yellow) that spans cells 2, 10, and 18. In the same manner, region 2 has one infected area that spans cells 22 and 23. As humans pass any of the infected areas, there will become infected after a variable amount of time. A red dashed line represents the traversal path of an infected human. The yellow circle on the path represents the point in time when the personal agent first detects the infection state. On the other hand, solid green lines represent the traversal paths of non-infected humans.

The regional manager starts by using the original cell structure settings in its region to compute the suspicion ranking ($\Re$) of the cells within its territory (see Algorithm 1 (line 3)). Table 3 illustrates the results of the suspicion calculation using the original 32 cell-structure. As shown in the results, cell (10) is ranked as the most suspicious cell in region 1 with a suspicion score of 0.8333 followed by cells (2, 18, 9, 11, 17, 25, 3). On the other hand, cell (23) is ranked as the top suspicious cell in region 2 with a suspicion score of 0.75 followed by cells (30, 31, 4, 12, 13, 14, 15, 32, 22). The regional manager then records the maximum reached suspicion rank (Ω) within its region (see Algorithm 1 (line 4)). The results in Table 3 show that the maximum reached suspicion rank in region 1 is 7 while the maximum rank in region 2 is 5.

As the reorganization process will generate a large number of cells, it is not feasible to display the suspicion ranking results using a table. Therefore, we demonstrate the suspicion

Table 3 Suspicion scores and ranks for region 1 and region 2

Region 1

Cell	$I_T(C)$	$I_U(C)$	$N_T(C)$	Suspiciousness (C)	Suspicion rank
10	5	0	1	0.833333333	1
2	3	2	1	0.5	2
18	2	3	1	0.333333333	3
9	2	3	2	0.285714286	4
11	2	3	2	0.285714286	4
17	2	3	3	0.25	5
25	1	4	1	0.166666667	6
3	1	4	2	0.142857143	7

Region 2

Cell	$I_T(C)$	$I_U(C)$	$N_T(C)$	Suspiciousness (C)	Suspicion rank
23	3	0	1	0.75	1
30	2	1	1	0.5	2
31	2	1	1	0.5	2
4	1	2	0	0.333333333	3
12	1	2	0	0.333333333	3
13	1	2	1	0.25	4
14	1	2	1	0.25	4
15	1	2	1	0.25	4
32	1	2	1	0.25	4
22	1	2	2	0.2	5

ranks using a colored map, as depicted in Fig. 4. The cells colored in dark red represent the most suspicious cells, while less suspicious cells have brighter colors.

After that, the regional manager progressively splits each infected cell into four equally sized cells (see Algorithm 1 (line 6)). Then, it uses the new cell structure settings ($\mathcal{C}_{\mathcal{RG}}$) to compute the suspicion rank of the new cells ($\mathfrak{R}$) (see Algorithm 1 (line 8)). Finally, the regional manager computes the highest reached suspicion rank (Ω) in $\mathfrak{R}$ (see Algorithm 1 (line 10)). In case the new highest reached is larger than the old one, the regional

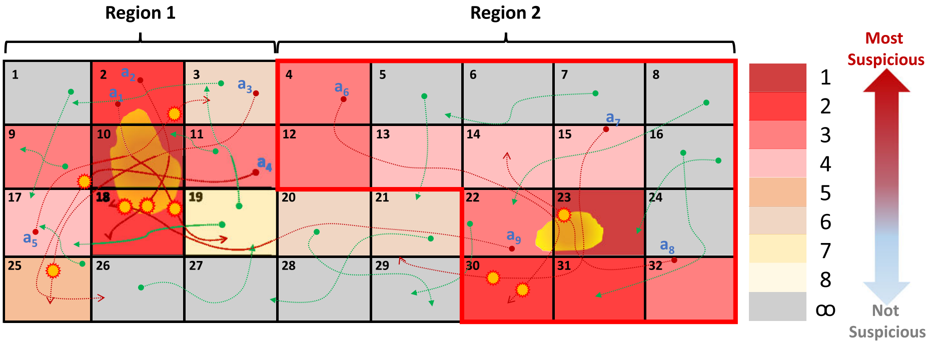

Fig. 4 Suspicion ranking of cells using the original cell structure (Level-0)

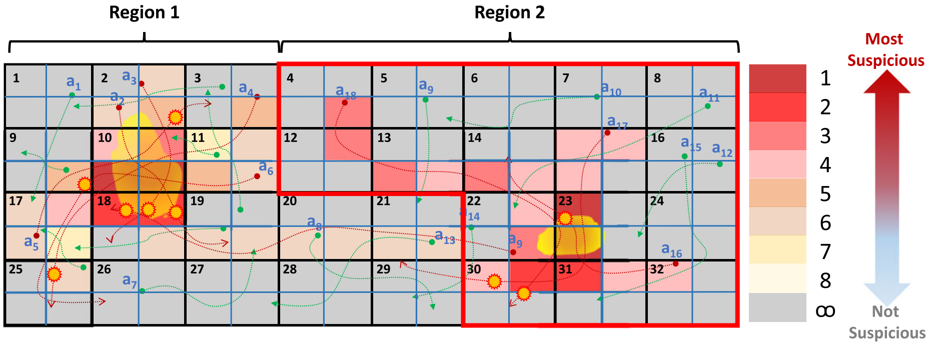

Fig. 5 Suspicion ranking of cells after splitting the infected cells for the first time (Level-1)

manager repeats the split process (Algorithm 1 (line 5 to 11)). The regional manager continues to split infected cells until the obtained highest reached rank (Ω) becomes lower than its previous value(Ω').

Figure 5 shows the two regions after the first split operation. As illustrated in the figure, the regional manager split each infected cell into four equally sized cells, and computes the suspicion scores and ranks accordingly. For instance, cell 10 is ranked as the most suspicious cell when using the original cell structure. After the first split, cells 10.3 and 10.4 are listed as most suspicious (colored in dark red), and cells 18.1 and 18.2 are ranked second.

Cell 18.3 is originally part of cell 18 that was initially ranked second. Nevertheless, cell 18.3 is not identified suspicious after splitting the cells. This observation conforms with the actual span of the infected area, which does not cover cell 18.3. Therefore, minimizing cell size helps in excluding non-infected territories that are included in the case of large cell size and consequently makes the framework more precise.

After the first split of infected cells (level-1), the highest reached ranks in regions 1 and 2 are 7 and 5, respectively. As the highest reached ranks for the two regions are equal to the previous ranks at level-0 (i.e., before splitting), the regional managers further split (level-2) the infected cells within both regions. Figure 6 shows the two regions after reaching level-2. As can be noticed, the area of suspicious cells is narrowed down to better match the infected areas. Using level-2, the highest reached ranks in regions 1 and 2 are 7 and 3, respectively. As can be noticed from the figure, the gradients in the suspicion rank of cells in region 2

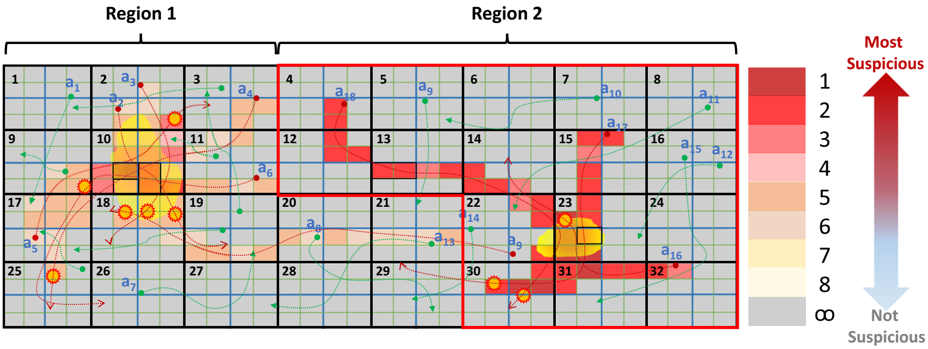

Fig. 6 Suspicion ranking of cells after splitting the infected cells for the second time (Level-2)

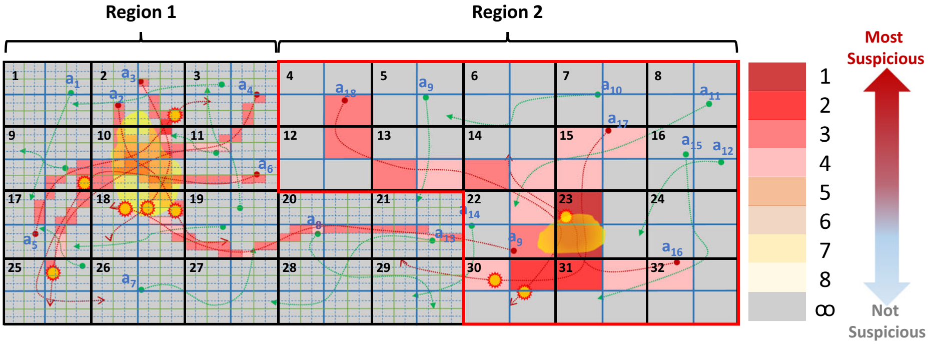

Fig. 7 Suspicion ranking of cells after splitting the infected cells of region 1 for the third time (Level-3) and reverting back the cells in region 2 to level-1

become very small. This convergence in results indicates that all suspicious cells have the same or close degree of suspiciousness. Consequently, using this cell structure wastes the improvement in efficiency gained by the split process.

As the previous highest rank in region 2 is larger than the new one, the split process in region 2 will be reverted to level-1. Therefore, the regional manager considers the suspicion scores and ranks computed according to the cell structure of level-1. On the other hand, the regional manager at region 1 further splits its cells to level-3 and computes the suspicion ranks accordingly (see Fig. 7).

According to the results given in Fig. 7, the highest reached rank in region 1 using the structure of level-3 is 4. As such, the regional manager reverts the cell structure to level-2, and the reorganization process stops at this level. Figure 8 captures the final cell structure settings after completing the reorganization process. As illustrated in Fig. 8, the most suspicious areas in region 1 are mainly focused within cell 10 and the lower parts of cell 2. Furthermore, the figure shows that the structure of the identified infected cells adapts to the actual spread of the infection and the infected humans' traversal information. Overall, the framework gives more precise results for region 1 in comparison to region 2. The improved accuracy in this example is expected as region 1 includes a larger number of monitored humans that generate added monitoring information.

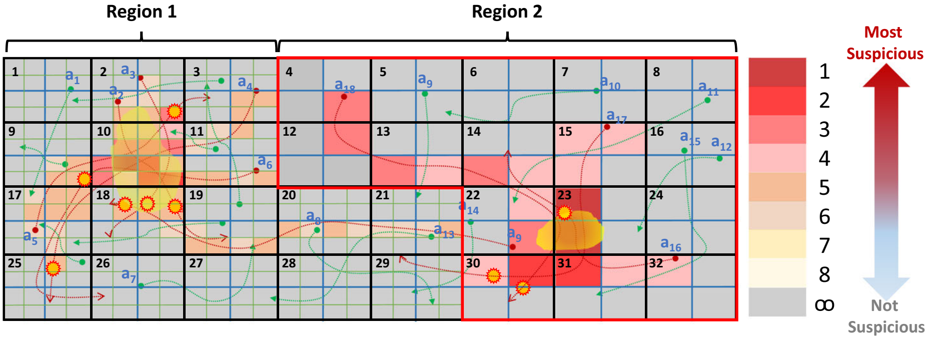

Fig. 8 The final cell structure settings after completing the re-organization process

5 Model implementation and evaluation

In this section, we discuss the experiments we used to evaluate our framework and to show its effectiveness. We start by presenting the experimental settings and the evaluation metrics. Then, we discuss the collected results.

5.1 Experiment setting

We implemented and integrated our framework using DIVAs 4 [6], a framework for the quick construction of agent-based simulation systems. Using the environment editing system integrated with DIVAs 4, we built a virtual city that consists of buildings, streets, trees, and other environmental objects. In all of our experiments, we fixed the simulated environment dimensions to 8000X8000 meters that we initially partitioned into 256 cells.

Moreover, we defined a circular biologically infected area at the center of the virtual city. We run the simulation scenarios using infected areas with a radius of 100, 200, 300, and 400 meters and with 1000, 2000, and 3000 simulated humans. At the start of the simulation, none of the simulated humans is infected. Nevertheless, as any of the humans crosses the infected area, he will become infected after a variable amount of time. The incubation period depends on the strength of the immunity level for the infected human. For this sake, we assign a random immunity level values for each of our simulated humans that range from 1 to 5. The higher the value, the longer the time it takes the infection signs to appear.

For each combination of the above settings, we ran the simulation scenario 10 times. For each computed split-level, we calculated the following:

- **The percentage of the inspected environment**: This value refers to the rank of the last infected cell in the generated cell divided by the total number of cells in the environment. In other words, this value refers to the percentage of the environment area that must be inspected to detect all infected cells.
- **Reached rank**: The highest generated rank in the last.
- **Percentage of false negatives**: This value corresponds to the number of undetected infected cells divided by the total number of cells.
- **Percentage of false positives**: This value refers to the percentage of uninfected cells that the framework wrongly identifies them as infected. As the framework generates an ordered list of suspicious cells, we count the number of false positives until we reach the last actual infected cell in the generated list.

5.2 Results & evaluation

Figure 9 shows the percentage of the inspected area for all experiment settings. The results show that the percentage of the inspected environment increases as the threat radius increases. This increment is expected as the increase in the threat radius increases the overall infected area.

Figure 9 also shows that with any number of monitored humans, the rate of inspected environment significantly drops from level (0) to level (2). After level (2), the decrease becomes marginal. Minimizing the size of the cell will result in adding new cells in the environment. This addition will cause the monitored humans to traverse more cells. As not all of the newly created cells are infected, crossing these cells will result in collecting false pieces of evidence that affects the accuracy of the model.

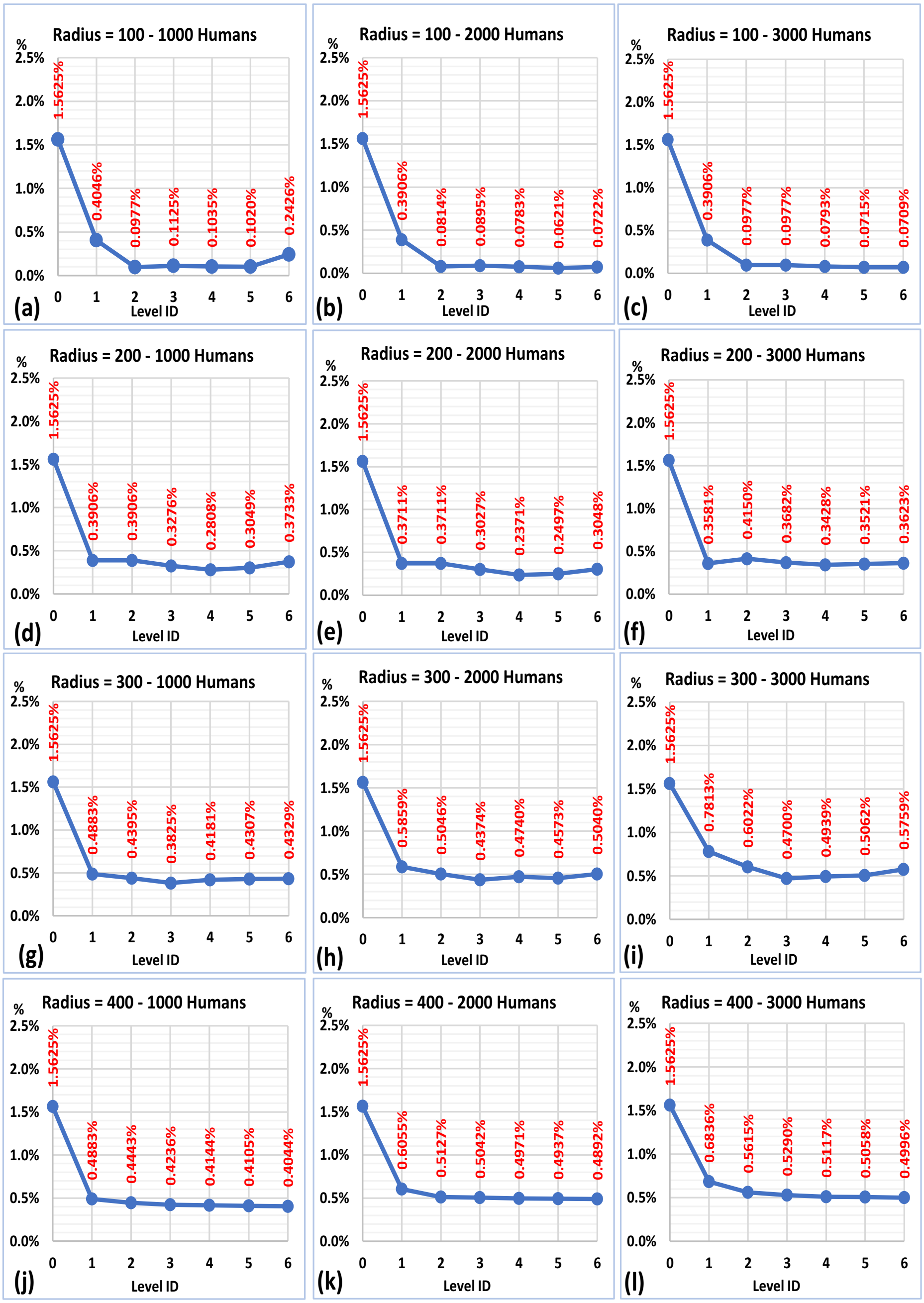

Fig. 9 Percentage of the inspected area of the environment with a threat radius of 100, 200, 300, and 400 and using 1000, 2000, and 3000 monitored humans

We can notice the same effect when using more monitored humans in the environment. Although monitoring more humans provides more pieces of evidence, there is a higher chance for those humans to navigate more cells that might not be infected. Consequently, the benefits gained by monitoring more humans will be lost. For instance, in case of a threat radius of 100, the minimum inspected percentage with 1000 is 0.102% and is achieved at level (5). In the case of using 2000 humans, the rate drops to 0.0621% and then increases again to 0.0709% in the case of 3000 humans. Despite the slight increase in the percentage of the inspected environment in case of the 3000 humans, the recorded results are comparable to the case of 2000 humans.

The results in Fig. 9 also show that the minimum percentage in case of the 100 infection radius occurs at levels (5) and (6). However, in the case of the 200 infection radius, the minimum percentage occurs at level (4). As we can notice from the results, the optimal cell size increases as the size of the infected area increases.

As the size of the infected area increases, there is a higher possibility of not traversing all infected cells in the environment. Consequently, the framework will not be able to identify all infected cells. Figure 10 captures this behavior and shows the percentage of false negatives with a threat radius of 300 and 400 and using 1000, 2000, and 3000 monitored humans. As can be seen in the Figure, with an infection radius of 300 or 400, the framework is unable to identify all infected cells in the environment. Nevertheless, as the cell size decreases, the percentage of false negatives also decreases. Yet, in case of monitoring more number of humans, the percentage of false negatives also deceases. For instance, the percentage of false negatives will drop to zero percent starting from level (3) in case of monitoring 3000 humans (see Fig. 10c). Although monitoring more humans might slightly affect the accuracy of the framework as discussed above, it will result in a higher chance of covering more infected areas. Consequently, it helps in minimizing the percentage of false negatives and in enhancing the reliability of the framework.

The results in Fig. 10 also show that, with an infection radius of 300 and 400 meters, the false negative rates in case of 1000 monitored humans are higher than the false negative rates with 2000 or 3000 humans. This fact explains why the percentage of the inspected

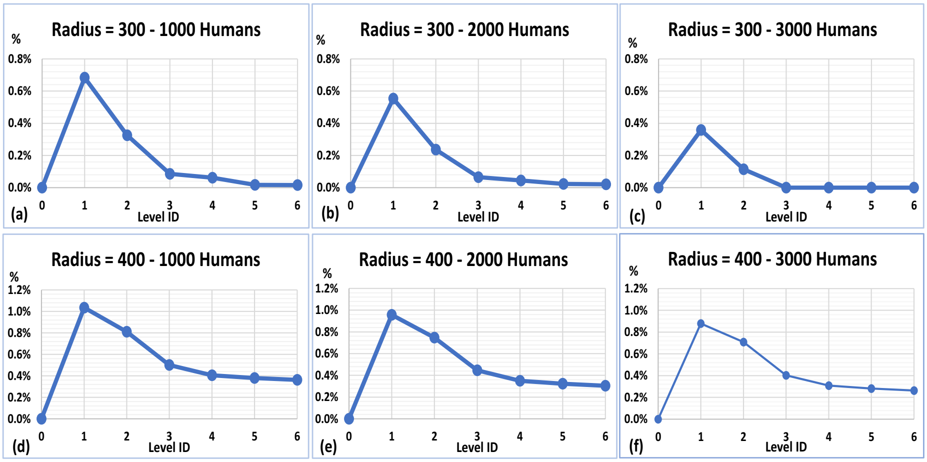

Fig. 10 Percentage of false negatives with a threat radius of 300 and 400 and using 1000, 2000, and 3000 monitored humans

environment with 1000 humans is less than the percentage when tracking 2000 and 3000 humans (see Fig. 9g–l).

Figure 11 shows the percentage of false-positive cases generated by the framework. As the cases of 300 and 400 meters infection radius have loss percentages, we restrict the results to the experiments with 100 and 200 meters infection radius. As illustrated in the figure, the framework does not generate any false-positives at level (0). Furthermore, the percentages of false-positives initially remain low and then start to increase as the level increases for any number of monitored humans. This increment is expected as the higher levels result in more cells in the environment. Accordingly, monitored humans traverse more cells, that might not be infected. Therefore, the number of false-positives increases.

The results in Fig. 11 also show that with an infection radius of 100 meters, tracking 1000 humans results in a very high percentage of false-positives in comparison to tracking 2000 and 3000 humans for the same infection radius (see Fig. 11a,b, and c). As discussed earlier, monitoring a larger number of humans provides more pieces of evidence and enhances the accuracy of the framework. The percentage of false-positives becomes higher in the case of small infection areas, as in the case of the 100 meter infection radius. This raise in false-positives happens because smaller infected areas have a lower chance of being covered by a small number of humans.

Nevertheless, the results in Fig. 11 show that with an infection radius of 100 meters, monitoring 2000 humans results in more false-positives in comparison to the case of 3000 humans. On the other hand, in case of the 200 meters infection radius, the percentage of false-positives in case of monitoring 3000 humans is higher than the case of 2000 humans. In the case of the 200 meters infection radius, the environment has a larger number of infected cells in comparison to the 100 meters infection radius. Hence, monitoring more humans results in more false positives as these humans have higher chances of traversing more infected cells.

Overall, we can notice from the results that the proposed framework maintained the lowest percentage of inspected areas. Furthermore, the results show that the framework dynamically reorganizes the cell partitioning to minimize the loss and false-positive rates.

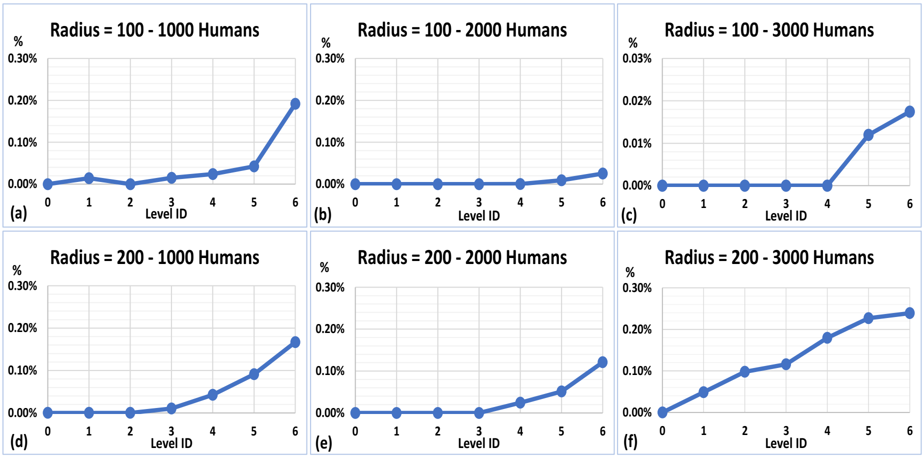

Fig. 11 Percentage of false positives with a threat radius of 100 and 200 and using 1000, 2000, and 3000 monitored humans

6 Conclusion and future work

In this paper, we presented a reorganizing biosurveillance framework for the precise detection of biological threats using fog and mobile edge computing support. In the proposed framework, a hierarchy of fog nodes are responsible for aggregating monitoring data within their regions and detecting potential threats. Although fog nodes are deployed on a fixed base station infrastructure, the framework provides an efficient technique for reorganizing the monitored environment structure to adapt to the evolving environmental conditions and to overcome the limitations of the static base station infrastructure.

The proposed framework is implemented and assessed in DIVAs 4, a framework for the rapid development of multi-agent simulation systems. Evaluation results illustrate the ability of the framework to localize biological threats and detect infected areas. Moreover, the results show the effectiveness of the reorganization mechanisms in adjusting the environment structure to cope with the evolving environmental conditions. As clearly noticed in the presented experimental results, the framework's main limitation is its inability to identify infected areas not covered by infected humans. In our future work, we are intending to investigate advanced techniques to anticipate these areas using information from neighboring infected areas. Such methods are vital to improve the accuracy of the framework and minimize the loss rate. Additionally, we intend to investigate the impact of the re-organization process on the performance of the framework.

References

1. Ahmad M, Amin MB, Hussain S, Kang BH, Cheong T, Lee S (2016) Health fog: a novel framework for health and wellness applications. J Supercomput 72(10):3677–3695
2. Ahmed E, Ahmed A, Yaqoob I, Shuja J, Gani A, Imran M, Shoaib M (2017) Bringing computation closer toward the user network: Is edge computing the solution? IEEE Commun Mag 55(11):138–144
3. Ahmed E, Rehmani MH (2017) Mobile edge computing: opportunities, solutions, and challenges. Future Gen Comp Syst 70:59–63
4. Al Z, Brillman J, Forslund DW, George JE, Zink S, Koenig S, Staab T, Simpson G, Umland E., Bersell K (2001) The rapid syndrome validation project (RSVP). In: Proceedings of the american medical informatics association annual AMIA symposium. American Medical Informatics Association, Washington, pp 771–775
5. Al-Zinati M, Al-Thebyan Q, Jararweh Y (2019) An agent-based self-organizing model for large-scale biosurveillance systems using mobile edge computing. Simul Model Pract Theory 93:65–86
6. Al-Zinati M, Araujo F, Kuiper D, Valente J, Wenkstern RZ (2013) DIVAs 4.0: a multi-agent based simulation framework. In: Proceedings of the 17th IEEE/ACM international symposium on distributed simulation and real time applications (DS-RT 2013), pp 105–114. Delft, Netherlands
7. Alabdulatif A, Khalil I, Yi X, Guizani M (2019) Secure edge of things for smart healthcare surveillance framework. IEEE Access 7:31010–31021
8. Althouse BM, Scarpino SV, Meyers LA, Ayers JW, Bargsten M, Baumbach J, Brownstein JS, Castro L, Clapham H, Cummings DAT et al (2015) Enhancing disease surveillance with novel data streams: challenges and opportunities. EPJ Data Science 4(1):17
9. Ansaldi F, Orsi GB, Altomonte F, Bertone G, Parodi V, Carloni R, Moscatelli P, Pasero E, Oreste P, Icardi G (2008) Emergency department syndromic surveillance system for early detection of 5 syndromes: a pilot project in a reference teaching hospital in genoa, italy. J Preventive Med Hygiene 49(4):131–5
10. Backer HD, Bissell SR, Vugia DJ (2016) Disease reporting from an automated laboratory-based reporting system to a state health department via local county health departments. Public Health Reports
11. Balasubramanian V, Wang M, Reisslein M, Xu C (2019) Edge-boost: enhancing multimedia delivery with mobile edge caching in 5g-d2d networks. In: 2019 IEEE international conference on multimedia and expo (ICME), pp 1684–1689. Shanghai, China

12. Bandopadhaya S, Dey R, Suhag A (2020) Integrated healthcare monitoring solutions for soldier using the internet of things with distributed computing. Sustainable Computing: Informatics and Systems, pp 100378
13. Betancourt JA, Hakre S, Polyak CS, Pavlin JA (2007) Evaluation of icd-9 codes for syndromic surveillance in the electronic surveillance system for the early notification of community-based epidemics. Mil Med 172(4):346–352
14. Bhatia M, Sood SK (2016) Temporal informative analysis in smart-icu monitoring: M-healthcare perspective. Journal of Medical Systems 40(8):190
15. Buehler JW, Berkelman RL, Hartley DM, Peters CJ (2003) Syndromic surveillance and bioterrorism-related epidemics. Emerging Infectious Diseases 9(10):1197
16. Clifton L, Clifton DA, Pimentel MAF, Watkinson PJ, Tarassenko L (2013) Predictive monitoring of mobile patients by combining clinical observations with data from wearable sensors. IEEE J Biomed Health Inf 18(3):722–730
17. Centers for Disease Control and Prevention. BioSense. https://www.cdc.gov/nssp/biosense/index.html. Accessed May 2018
18. Centers for Disease Control and Prevention (CDC).Global Health Protection and Security. https://www.cdc.gov/globalhealth/healthprotection/ghs/index.html. Accessed April 2019
19. Flanagan T, Beyeler W, Levin D, Finley P, Moses M (2019) Movement and spatial specificity support scaling in ant colonies and immune systems: application to national biosurveillance. In: Evolution, development and complexity. Springer, Berlin, pp 355–366
20. Fricker RD Jr, Chang JT (2008) A spatio-temporal methodology for real-time biosurveillance. Qual Eng 20(4):465–477
21. Gardy JL, Loman NJ (2018) Towards a genomics-informed, real-time, global pathogen surveillance system. Nat Rev Gen 19(1):9
22. Gia TN, Jiang M, Rahmani A-M, Westerlund T, Liljeberg P, Tenhunen H (2015) Fog computing in healthcare internet of things: a case study on ECG feature extraction. In: 2015 IEEE international conference on computer and information technology; ubiquitous computing and communications; dependable, autonomic and secure computing; pervasive intelligence and computing, pp 356–363. Liverpool, UK
23. Giger JT, Pope ND, Bruce Vogt H, Gutierrez C, Newland LA, Lemke J, Lawler MJ (2015) Remote patient monitoring acceptance trends among older adults residing in a frontier state. Comput Hum Behav 44:174–182
24. Heffernan R, Mostashari F, Das D, Besculides M, Rodriguez C, Greenko J, Steiner-Sichel L, Balter S, Karpati A, Thomas P et al (2004) New York City syndromic surveillance systems. Morbidity and Mortality Weekly Report, pp 25–27
25. Hoffman SJ, Silverberg SL (2018) Delays in global disease outbreak responses: lessons from h1n1, ebola, and zika. Am J Publ Health 108(3):329–333
26. Hossain MS, Muhammad G (2016) Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring. Comput Netw 101:192–202
27. Hutwagner L, Thompson W, Seeman GM, Treadwell T (2003) The bioterrorism preparedness and response early aberration reporting system (ears). Journal of Urban Health 80(1):i89–i96
28. Karwa M, Currie B, Kvetan V (2005) Bioterrorism: preparing for the impossible or the improbable. Crit Care Med 33(1):S75–S95
29. Katherine Yih W, Caldwell B, Harmon R, Kleinman K, Lazarus R, Nelson A, Nordin J, Rehm B, Richter B, Ritzwoller D et al (2004) National bioterrorism syndromic surveillance demonstration program. Morb Mortal Wkly Rep 2:43–46
30. Kman NE, Bachmann DJ (2012) Biosurveillance: a review and update. Advances in Preventive Medicine 2012(301408):9
31. Lomotey RK, Pry JC, Sumanth S (2017) Wearable iot data stream traceability in a distributed health information system. Pervasive and Mobile Computing 40:692–707
32. Mahmud R, Koch FL, Buyya R (2018) Cloud-fog interoperability in iot-enabled healthcare solutions. In: Proceedings of the 19th international conference on distributed computing and networking, ICDCN'18. Varanasi, India, pp 32:1–32:10
33. Nandyala CS, Kim H-K (2016) From cloud to fog and iot-based real-time u-healthcare monitoring for smart homes and hospitals. International Journal of Smart Home 10(2):187–196
34. Naumova E, Thompson W, Matthew Seeman G, Treadwell T (2003) The bioterrorism preparedness and response early aberration reporting system (ears). J Urban Health 80(1):i89–i96
35. Negash B, Gia TN, Anzanpour A, Azimi I, Jiang M, Westerlund T, Rahmani AM, Liljeberg P, Tenhunen H (2018) Leveraging fog computing for healthcare IoT. Springer, Cham, pp 145–169
36. Pinto VN (2013) Bioterrorism: health sector alertness. J Nat Sci Biol Med 4(1):24

37. Plianbangchang S (2005) Strategies of preparedness against the threat of biological w eat of biological w eat of biological warfare and bioterrorism in south-east asia. Asian Biotechnol Develop Rev 8(1):77–98
38. Quwaider M, Jararweh Y (2015) Cloudlet-based efficient data collection in wireless body area networks. Simul Model Pract Theory 50:57–71
39. Quwaider M, Jararweh Y (2016) A cloud supported model for efficient community health awareness. Pervasive and Mobile Computing 28:35–50
40. Rahmani AM, Gia TN, Negash B, Anzanpour A, Azimi I, Jiang M, Liljeberg P (2018) Exploiting smart e-health gateways at the edge of healthcare internet-of-things: a fog computing approach. Futur Gener Comput Syst 78:641–658
41. Ramanathan A, Pullum LL, Steed CA, Parker TL, Quinn SP, Chennubhotla CS (2013) Oak ridge bio-surveillance toolkit (orbit): integrating big-data analytics with visual analysis for public health dynamics. Technical report, Oak Ridge National Lab. (ORNL), Oak Ridge, TN (United States)
42. Regan JF, Makarewicz AJ, Hindson BJ, Metz TR, Gutierrez DM, Corzett TH, Hadley DR, Mahnke RC, Henderer BD, Breneman JW IV, et al. (2008) Environmental monitoring for biological threat agents using the autonomous pathogen detection system with multiplexed polymerase chain reaction. Analytical Chemistry 80(19):7422–7429
43. Salahuddin MA, Al-Fuqaha A, Guizani M, Shuaib K, Sallabi F (2017) Softwarization of internet of things infrastructure for secure and smart healthcare. Computer 50(7):74–79
44. Sandhu R, Gill HK, Sood SK (2016) Smart monitoring and controlling of pandemic influenza a (h1n1) using social network analysis and cloud computing. Journal of Computational Science 12:11–22
45. Sandhu R, Sood SK, Kaur G (2016) An intelligent system for predicting and preventing mers-cov infection outbreak. J Supercomput 72(8):3033–3056
46. Sareen S, Gupta SK, Sood SK (2017) An intelligent and secure system for predicting and preventing zika virus outbreak using fog computing. Enterprise IS 11(9):1436–1456
47. Sood SK, Kaur S, Chahal KK (2020) An intelligent framework for monitoring dengue fever risk using LDA-ANFIS. J Amb Intell Smart Environ 12(1):5–20
48. Sood SK, Mahajan I (2017) Wearable iot sensor based healthcare system for identifying and controlling chikungunya virus. Comput Ind 91:33–44
49. Sood SK, Mahajan I (2018) A fog-based healthcare framework for Chikungunya. IEEE Internet of Things Journal 5(2):794–801
50. Sood SK, Mahajan I (2018) Fog-cloud based cyber-physical system for distinguishing, detecting and preventing mosquito borne diseases. Futur Gener Comput Syst 88(2):764–775
51. Tsui F-C, Espino JU, Dato VM, Gesteland PH, Hutman J, Wagner MM (2003) Technical description of rods: a real-time public health surveillance system. J Am Med Inform Assoc 10(5):399–408
52. Uscher-Pines L, Farrell CL, Babin SM, Cattani J, Gaydos CA, Hsieh Y-H, Moskal MD, Rothman RE (2009) Framework for the development of response protocols for public health syndromic surveillance systems: case studies of 8 US states. Disaster Med Public Health Prep 3(S1):S29–S36
53. Verma P, Sood SK (2018) Fog assisted-iot enabled patient health monitoring in smart homes. IEEE Internet of Things Journal 5(3):1789–1796
54. Wagar EA, Mitchell MJ, Carroll KC, Beavis KG, Petti CA, Schlaberg R, Yasin B (2010) A review of sentinel laboratory performance: identification and notification of bioterrorism agents. Archives of Pathology & Laboratory Medicine 134(10):1490–1503
55. Wang M-H, Chen H-K, Hsu M-H, Wang H-C, Yeh Y-T (2018) Cloud computing for infectious disease surveillance and control: development and evaluation of a hospital automated laboratory reporting system. Journal of Medical Internet Research 20(8):e10886
56. World Health Organization. Surface sampling of coronavirus disease (covid-19): a practical how to protocol for health care and public health professionals. Technical documents, 2020
57. Xu B, Xu LD, Cai H, Xie C, Hu J, Bu F (2014) Ubiquitous data accessing method in iot-based information system for emergency medical services. IEEE Transactions on Industrial Informatics 10(2):1578–1586
58. Xu C, Dong M, Ota K, Li J, Yang W, Wu J (2019) Sceh: smart customized e-health framework for countryside using edge ai and body sensor networks. In: 2019 IEEE global communications conference (GLOBECOM), pp 1–6. Waikoloa, HI, USA
59. Yan SJ, Chughtai AA, Macintyre CR (2017) Utility and potential of rapid epidemic intelligence from internet-based sources. Int J Infect Dis 63:77–87
60. Yang G, Li X, Mäntysalo M, Zhou X, Pang Z, Xu LD, Kao-Walter S, Chen Q, Zheng L-R (2014) A health-iot platform based on the integration of intelligent packaging, unobtrusive bio-sensor, and intelligent medicine box. IEEE Transactions on Industrial Informatics 10(4):2180–2191
61. Yang J, Zhou J, Lv Z, Wei W, Song H (2015) A real-time monitoring system of industry carbon monoxide based on wireless sensor networks. Sensors 15(11):29535–29546

Publisher's note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Affiliations

Mohammad Al-Zinati[1] · **Reem Alrashdan**[1] · **Basheer Al-Duwairi**[2] · **Moayad Aloqaily**[3]

Reem Alrashdan
rmalrashdan15@cit.just.edu.jo

Basheer Al-Duwairi
basheer@just.edu.jo

Moayad Aloqaily
maloqaily@ieee.org

[1] Department of Software Engineering, Jordan University of Science and Technology, Irbid, 22110, Jordan

[2] Department of Network Engineering and Security, Jordan University of Science and Technology, Irbid, 22110, Jordan

[3] Al Ain University, Al Ain, UAE