International Journal of Innovative Computing, Information and Control
Volume **16**, Number **3**, June **2020**

ICIC International ©2020 ISSN 1349-4198
pp. 1047–1058

A NEW SMART ALGORITHM TO PROVIDE AN INTEGRITY PATH IN NETWORKS FOR IMPROVING THE ABROAD HEALTHCARE SURGERY SETTING

Radwan Saoud Abujassar

School of Information Technology and Computing Technology
Arab Open University, Kuwait Branch
PO.BOX 830, Alardiya Area 92400, Kuwait
r.abujassar@aou.edu.kw

Received January 2020; revised April 2020

Abstract. *The Internet of Things (IoT) is a paradigm based on the networks that comprise many interconnected technologies. The current demand for better control, monitoring and management in many areas, as well as ongoing research in this field, have led to the appearance and creation of multiple systems such as smart homes, smart healthcare, smart cities and smart grids. The IoT is rapidly becoming a global phenomenon, with many issues such as standardization. However, there is not a robust and secure network routing system. Various MANET or IGP routing protocols have been proposed by researchers which could be utilized in the development of enhanced routing protocols for the IoT. Thus, studying these routing protocols in the MANET or IGP network will provide direction to the development and incorporation of reliable paths between the source and the destination in the network through the application of IoT features. In this paper, we propose a new algorithm for managing lead emergency data traffic in healthcare surgery settings from a far distance. In other words, we show how a trusted and smart algorithm can manage traffic in less time and without losing any information. The reported experimental results show an acceptable level of feasibility and effectiveness. In addition, we present an initial evaluation of the lightweight enhanced routing protocol policies and their integrity on the IoT.*

Keywords: Component, Quality of service (QoS), Mobile ad hoc network (MANET), Internet of Things (IoT), Medical surgery

1. Introduction.

The IoT currently is one of the major topics connected with new smart urban technology, such as smart cities. The IoT can be defined as a set of interconnected things (humans, tags, sensors, security, policy and so on) over the Internet, which have the ability to compute, communicate and act all over the world. The main idea behind the IoT is to gain information about our environment to understand, control and act on it. The IoT can aid us in our daily lives [2]. Furthermore, the IoT is suitable for smart units for ambient assisted living. The relation between IoT and cloud computing is that both are offered convenient, on-demand and scalable network access to a pool of configurable computing resources [1]. The proposed approach does not focus on such scenarios involving the suitability or limitations of the IoT and MANET or interior gateway protocol (IGP). However, our aim is to try to offer a practical vision through which to integrate current components of some routing protocols and the IoT. We are also aware of the current limitations of IoT devices, especially embedded devices. Thus, although we have surveyed different cloud technologies to improve these, the software for embedded devices is a key challenge in the pursuit of the desired integration. In addition to the limitations

DOI: 10.24507/ijicic.16.03.1047

of such devices, the IoT also requires applications in critical and real-time systems where low latency and low-bandwidth usage are key requirements. We have taken account of the latter and tried to survey a form of integration which addresses these requirements. For the deployment, management and monitoring of different platforms, we have surveyed different network infrastructures. Lastly, we have surveyed several IoT middleware to extract those IoT devices with underlying heterogeneity. IoT integration provides new storage, processing, scalability and networking capabilities which are, to date, limited on the IoT due to its characteristics [2]. Given the trend towards ubiquitous computing, everything is moving towards being connected to the Internet, with its data to be used for different progressive issues [3]. There is currently a push to integrate the IoT with cloud computing. This is because of the huge number of data that the IoT could generate and the demand to balance permissions for virtual links and resources with utilization and storage capacity, as well as to make it possible to derive more usefulness from the data generated by the IoT and develop smart applications for end users. Integration of the IoT and cloud computing is referred to as Cloud of Things in this paper. This integration is not that straightforward and raises some key issues, which, along with their respective potential solutions, are also highlighted in our research paper.

The rest of the paper is organized as follows. In Section 2, we describe related works on incentive schemes including previous work about the IoT and how it relates to improvements in network QoS. In Section 3 we describe our proposed technique and its mechanisms as well as some mathematical modelling with theoretical analysis concerning this proposal. The results are then reported and the performance of the proposed technique is evaluated in Section 4. Finally, a conclusion is given in Section 5.

2. **Related Works.**

The IoT has been proposed by Kevin Ashton in 1998 and refers to the future of the Internet and ubiquitous computing [2]. This technological revolution represents the future of connectivity and reachability from anywhere in the world. On the IoT, ‘things’ refer to any object on the face of the planet, whether it is a communicating device or not. From a smart device to a leaf node of a tree or a bottle of beverage, anything can be part of the Internet [4]. The objects become communicating nodes over the platform.

Smart communication and IoT sensors produce data that need to be analyzed in real time using deep studying and learning approaches, or we can use them to train deep learning for smart models. Edge computing is a viable way to facilitate good and better computation, given the low-latency requirements of edge devices, as well as offering additional advantageous in terms of privacy, bandwidth efficiency, and scalability.

This paper has an important aim which is to provide a comprehensive review of the current state of edge computing with the use of smart end devices [5]. This paper also presents an overview of applications where deep learning technology is used at the network edge, discusses different methodologies for quickly executing deep learning inference across a combination of end devices, edge servers and the cloud, and describes the methods for training deep learning models across multiple edge devices [6].

Healthcare applications using the IoT have rapidly increased in number and started to be widely used by a diverse range of end users. This is because of the scale of development of smart devices [7]. IoT devices are employed in remote health monitoring and emergency notification systems. In healthcare, monitoring devices are vital and range from blood pressure and heart rate monitors to advanced devices capable of monitoring specialized implants such as pacemakers, FitBit electronics, risk bands or advanced hearing aids. The IoT uses the Internet to enable the transmission of real-time data on the critical parameters of the patient. In the case of a substantial change in these critical parameters, an emergency alert is sent. This phenomenon has been the focus of initial IoT-based healthcare research efforts. Integrity makes sure that received video data are not disconnected and distorted while in transit by an adversary. The IoT is based on data exchanges between various kinds of devices such as IGP or MANET networks. It is important to ensure data accuracy by using a virtual path with a high-priority label when the data are received from the right sender as well as to determine whether the data have been tampered with during the process of transmission. In [8], the author has done an experiment that performed a study to show that the reliability and performance of the investigated clouds are beneath the expectations. Hence, the author mentioned in his research that the cloud computing is inadequate and inefficient for scientific computation comprehensively, although it shows a dire adaptation based on temporarily and immediate resources. Therefore, the enhancement of existing clouds concerned with computer networks and the identification of a novel research direction has been analyzed by the present study. Future work can extend this work by implementing other cloud services such as a database, private cloud, queue service, and storage.

The network layer of the IoT offers functionality in terms of real-time traffic data routing and transmissions to different IoT hubs or devices over the IGP or MANET. Internet gateways, switching and routing devices, among others, operate with the application of the most recent technologies such as WiFi, LTE, Bluetooth, 3G, ZigBee, OSPF, OSLR AODV in order to provide heterogeneous network services at this layer. The network gateways serve as a mediator between different IoT nodes by aggregating, filtering and transmitting data to and from different sensors [8].

This paper will also discuss the different challenges related to network efficiency and performance as well as technologies. The reader will take away the following concepts from this paper: understanding the network scenarios where deep learning at the network edge can be useful, understanding common techniques for speeding up deep learning inference, performing distributed training on edge devices, and understanding recent trends and opportunities.

Existing research work has tended to concentrate on the field of real-time traffic data control by finding the best historical nodes which can provide the most trusted path based on their history – this will be addressed by our algorithm. In [1], the detection of delay or failure, which demonstrates a hazardous traffic pattern, as in the case of operations over the IoT involving real-time data, has been discussed, along with abnormal traffic situations and the propagation of information. In this paper, we propose an algorithm to detect high-emergency real-time data which must be passed from destination to receiver nodes, to make way for these data and to clear all other unnecessary traffic using nodes with a high-priority label. We configure inquiry packet detection, in order to detect the presence of labelled data traffic by using our algorithm, and describe a low-cost solution for speech recognition.

Increased traffic has caused so many problems, which affect the daily life of an individual. To avoid much time being wasted on the roads, it is very important to control the traffic [9]. The number of road accidents has also increased due to traffic. The proposed algorithm uses the detection of high-emergency real-time data traffic to report to the next station using cloud computing. Two mechanisms are used to enable data transfer between server and client. Several works have been carried out in the field of traffic engineering. In the proposed system, data transfer is accomplished by using the TCP/IP protocol [10].

3. **Problem Definition.**

Traffic is a problem for mankind, due to its capacity to waste time and effort. In the case of high-priority real-time traffic, such as emergency situations or where high speed is critical, such as performing surgery via live video streaming, this

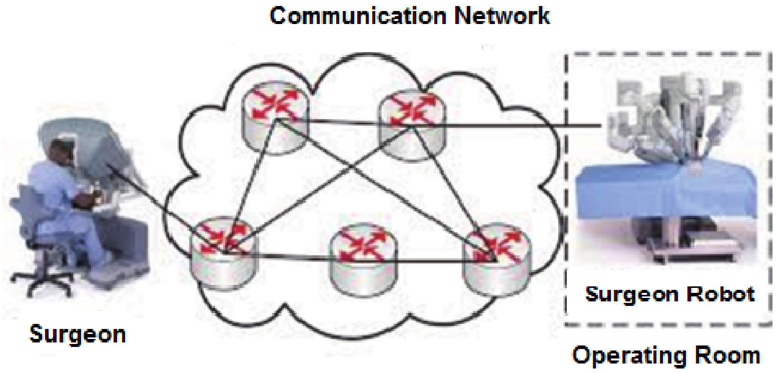

Figure 1. Routing algorithm with IoT integrity

problem may cause severe issues. Traffic paths may not work effectively due to congestion in the network. High-priority traffic will experience extra delays and could threaten the life of a patient. In Figure 1, we present an example where robotics is used to carry out a surgical operation based on the instructions of a doctor located in another area. There are many problems that can occur during surgery, and we have created a new algorithm to rebuild a path with high reliability. The focus problem here is currently some surgeries can be done live streaming, and we use this example regarding to the accurate and emergency data that need to be received with less time. Additionally, the proposed algorithm is coming to reduce the delay time for exchanging data and guarantee that the connection will be up until the session time terminates.

Even if the path is clear, there are some variations or disturbances emanating from the network which we cannot control, leading to the escalation of problems. Thus, in the proposed system, traffic control is performed automatically with the help of the IoT with necessary action undertaken to resolve these problems. We have created a smart algorithm which can first read high-emergency traffic and then start to open a session between the source and the destination until the live streaming ends. We have configured our algorithm to wait for a period of time; if no more packets are received, our algorithm will stop booking the path and return to the normal network.

3.1. **Proposed technique and algorithm.** We have proposed a novel path-protecting technique by using p-cycle heuristic algorithm to protect the main path between the source and the destination in the network design. There are two basic approaches for network survivability: protection and restoration. Protection guarantees full recovery and fast speed, while the restoration method may outperform in terms of resource utilization efficiency. The significant advantage of p-cycle-based path protection over link protection is the node failure recovery capability.

Integer linear programming was used to study the optimal path performance of the p-cycle technique and the network design, based on path protection. Integer linear programming is useful for finding an optimal solution for small networks with static traffic. For large networks, there are many obstacles, such excessive time consumption and the need for a large amount of variables and constraints for path protection. Hence, these reasons function as strong incentives to develop faster p-cycle-based path protection. In the case of a path-protecting p-cycle heuristic algorithm for a given network topology and traffic demand matrix, the objective is to minimize the total spare capacity. The main intention is to select the most efficient p-cycle among all the candidate cycles. We have two kinds of path as follows.

- Path cycle relationship check, which determines that the path span is disjointed for a given p-cycle if the path does not have a common span on the p-cycle. However, the path may have one or more common nodes other than end nodes with the p-cycle.
- Paths' mutual relation check, which determines if they lack common spans but have common nodes other than end nodes and whether the paths are mutually and fully disjointed. The path cycle relation check determines if there is a span failure, when the path is fully disjointed.

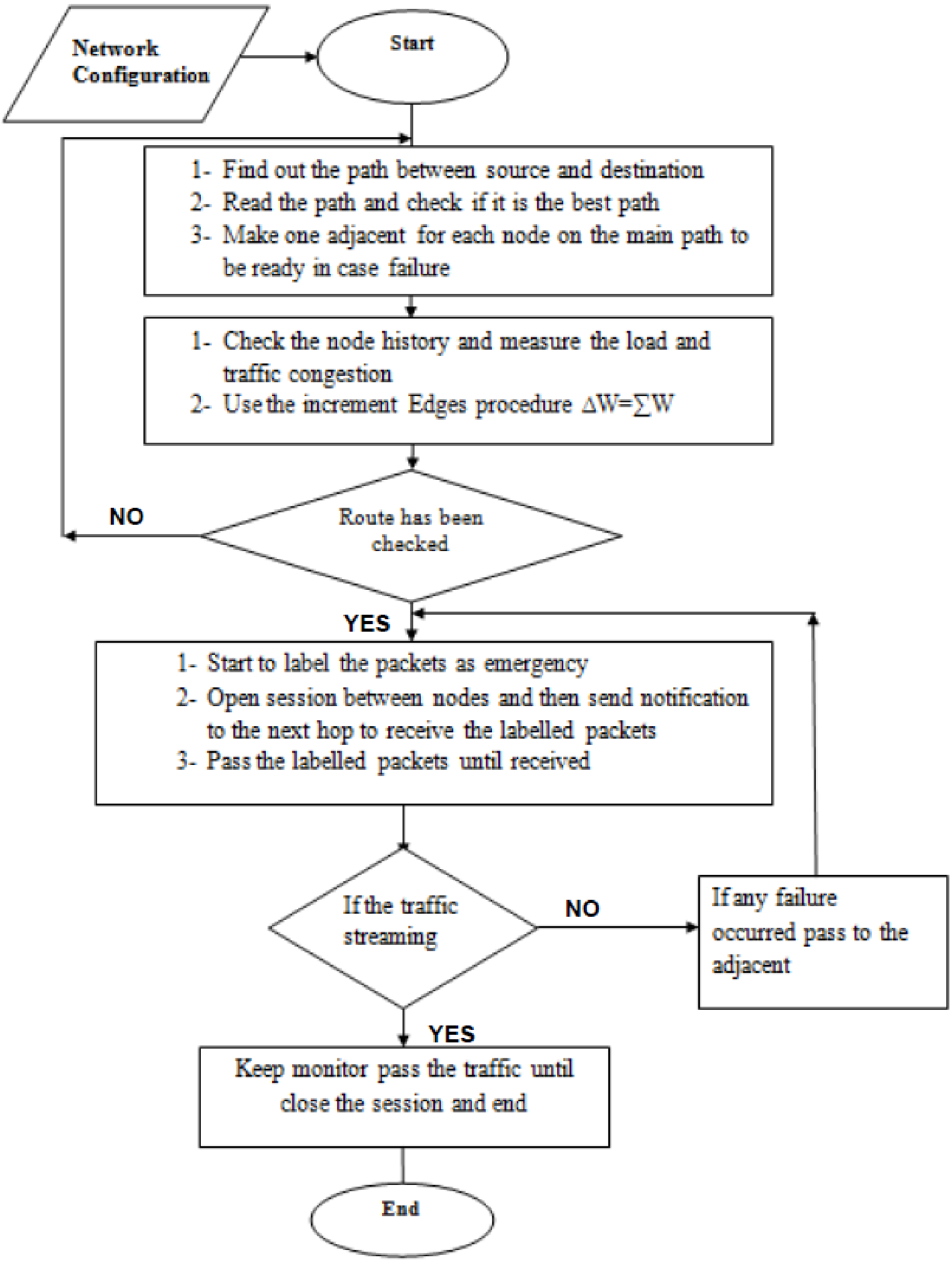
Network Configuration
Start
1- Find out the path between source and destination
2- Read the path and check if it is the best path
3- Make one adjacent for each node on the main path to be ready in case failure
1- Check the node history and measure the load and traffic congestion
2- Use the increment Edges procedure ΔW=∑W
NO
Route has been checked
YES
1- Start to label the packets as emergency
2- Open session between nodes and then send notification to the next hop to receive the labelled packets
3- Pass the labelled packets until received
If the traffic streaming
NO
If any failure occurred pass to the adjacent
YES
Keep monitor pass the traffic until close the session and end
End

Figure 2. Flowchart of the proposed algorithm

In Figure 2, we present our new algorithm which is a method for finding the required path, based on the history of each node and the fault tolerance capacity. Algorithm 1 shows how the nodes are selected after the main routing table is created. Hereafter, the algorithm will be working on the network before we start the surgery and keep monitoring the nodes adjacent to it in order to provide the required information about each node in the network and keep a record once the inquiry packets start to be distributed. The IoT smart technique, based on the collection of information and the registered record, will enable our algorithm to start to determine the path between the source and the destination in order to begin sending and receiving the data. The path will only be available for the label packets and for the required amount of time, as determined by the IoT surgery people.

Algorithm 1 *Checkingpath* p-cycle paths

```
procedure $FindTrustNode(T_r, s, d, edges\_to\_avoid)$
$T_r$: Routing table with each adjacent node
$V$: The nodes and their weight $G(V, E)$
$\Gamma(v)$: Number of nodes $v$
$s$: Packets starting from this node and $d$ is destination $s$: source
$d$: The receiver
$p_a(s, d) \leftarrow \emptyset$ path from source start to be checked from the adjacent
if $s \neq d$ then
    $q_{sub} \leftarrow \emptyset$ the buffer that we store all required adjacent nodes
    $Q \leftarrow \emptyset$
    $Enqueue(Q, (q_{sub}, s))$ the buffer that stores the nodes for the surgery path
    while $Q \neq \emptyset$ and $p_a(s, d) = \emptyset$ do
        $(q_{sub}, x) \leftarrow Front(Q)$
        for all $k \in \Gamma(x)$ do
            $e \leftarrow (x, k)$
            if $(q_{sub} \cup e) \cap edges\_to\_avoid = \emptyset$ and $P_r(T_r, k, d) \cap edges\_to\_avoid = \emptyset$ then
                $p_a(s, d) \leftarrow q_{sub} \cup e \cup P_r(T_r, k, d)$ $k$ is the intermediate node between source
                and destination
            else
                $Enqueue(Q, (q_{sub} \cup e, k))$
            end if
        end for
        $Dequeue(Q)$
    end while
    $Q \leftarrow \emptyset$
end if
return $p_a(s, d)$
end procedure
```

Our Algorithm 1 can work with any routing protocol; as we explained, the routing protocol is responsible for creating the routing table and then our algorithm is configured according to the following steps inside the routing protocol. In our protocol, we will assume that the all nodes on the primary path connect with an adjacent node, which has secured all our protocol constraints as follows.

- All nodes are selected by our algorithm to be included in the booked path between the source and the destination, which should be tracked and possess a very good history.

- Each node on the main path should have an adjacent node and be ready for any problem that could occur, as our algorithm will use this adjacent node to reroute the traffic in case of any failure (it is not on the primary path between the source and the destination).
- The adjacent node must have a path to the destination, which is disjointed in relation to the primary path or at least can pass traffic to next-next hop after the failure.
- In the case of link failure, each node connected directly with that link will know about the failure through layer 2; this is considered to be the most effective way for detecting failure when there is no signal.
- The new path should have enough capacity to tolerate additional packets from the other node in the case of failure.
- The delay for each link in the topology must be less than or equal to the delay on the primary path.

This mechanism is described into two tasks; first, it looks and checks all paths in the main routing table between nodes; second, it is constructed path from the main routing table (if possible), or searches for an alternative one through the adjacent nodes we make the algorithm to check the LS database for each node to check the historical information for each node. Based on Algorithm 1, each node sends an inquiry packet for all nodes. Figure 2 shows the flowchart for the computing virtual path via the proposed algorithm, and the way it computes its own routing table from the adjacent nodes. Each node will take a place in its area network. When there is more than one adjacent node, then it begins to check which adjacent node has an available path to the destination to construct a required path. However, the computation algorithm evaluates an appropriate route using the primary routing table from source to destination.

3.2. **IoT architecture.** The idea behind the IoT evolved at the Massachusetts Institute of Technology (MIT) following work at the Auto-ID Center in 1999. The MIT has undertaken much research on networked radio identification (RFID) and emerging sensing technologies (Wikipedia: The Free Encyclopedia, November 2014). Recently, one million devices or more were connected online, although the actual number is estimated to be on the increase [11]. However, with the rapid proliferation of smartphones and tablets over the years, there are about one billion devices connected online as of 2010. Figure 3 depicts how the IoT plays an important role by controlling a robotic device while the doctor gives it necessary instructions. As we discussed, the IoT facilitates two important mechanisms in our proposed algorithm. Firstly, it supports the transport of emergency packets from source to destination without any distortion. Secondly, it enables the robotic device to work, based on the instructions it receives from the doctor.

Recently, the ratio of devices per person was almost one person to two devices, i.e., smartphones, tablets and smartwatches. Today, we are witnessing an increase in technological innovation and the continuous growth in the market for smartphones. In a study conducted in China, the authors showed that the Internet doubles its size every 5.32 years. As such, it is obvious that the number of devices that are online and communicating with each other (M2M) will be quite large, which underlines the need to have secure communication in this context [12]. Currently, the IoT is a prominent topic, while it is being widely applied to creating smart cities. Given the thriving nature of research in this field, both in academia and industry, this technology is set to revolutionize the way we do many things. Figure 4 shows how the IoT starts to be used in smart cities and also around the world. The IoT model involves a three-layered structure defined by its functions, consisting of a perception layer, a network layer and an application layer [13]. This is further explained below.

- Perception layer: This is the sense organ of the IoT. It aims at recognizing objects and gathering information. This layer includes RFID tags, 2D bar code labels and readers, terminals, GPS, cameras, sensors and sensor networks.
- Network layer: This layer represents the nucleus of the IoT. It processes and transmits information received from the perception layer to the application layer. The network layer comprises the following: information centre, intelligent processing centre, Internet network system and network management centre.

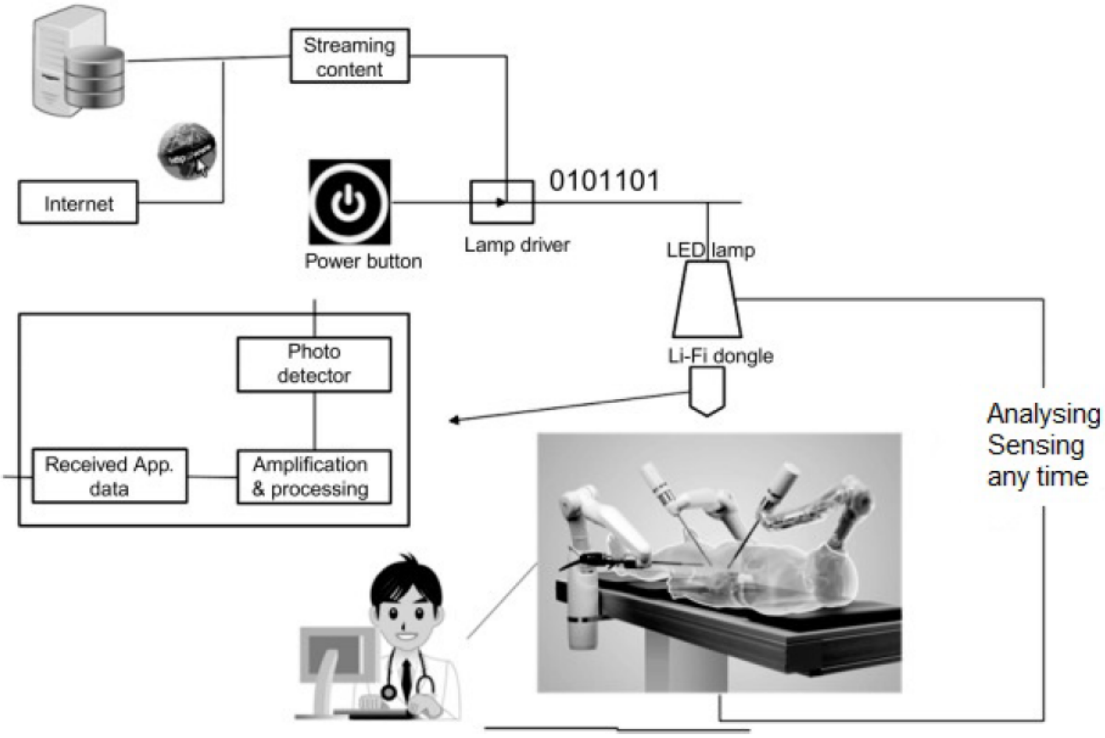

FIGURE 3. Surgery by an IoT robot

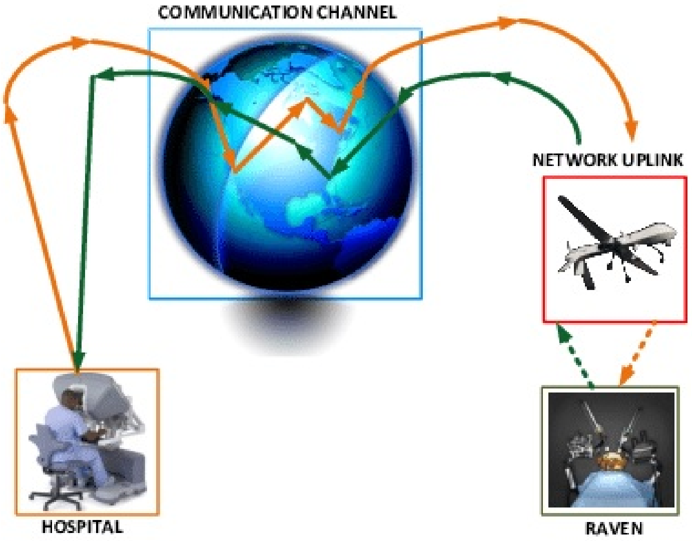

FIGURE 4. Channel routing

- Application layer: This layer is a fusion of the IoT's socio-business requirements in order to realize the in-depth capabilities of the technology. This layer represents the confluence of IoT and industrial technology with a mix of industrial needs and machine intelligence. Many researchers have worked to develop a proper understanding of the IoT and its two-system structure, i.e., the Internet and communications network should be analyzed in order to gain a better understanding of the IoT and hence create better architecture for the IoT [14].

4. **Simulation Environment.** Network simulation (NS2) was performed to evaluate the performance of the proposed long VPN path between the source and the destination in terms of receiving high-priority traffic for medical operations or any other important high-emergency traffic involving the on-demand protocol between nodes in the MANET networks. A comparison of the simulation results with and without failure was carried out for the algorithm with the routing protocol. The evidence gathered by the NS2 simulation offered good support for the transmission data in the networks. At the network link layer, the researcher used the IEEE 802 Ethernet. During the simulation, each node checked its adjacent history to form a full view of the network topology. Simulation was repeated 30 times and an average calculated. The packet size was 512 KB and the bit rate was set to 2 Mb/s. A traffic rate of 200 KB/s was generated from the source node to the destination during simulation.

Each graph illustrates a comparison made between the used proactive routing protocol without modification and with the enhanced and modify routing protocol by extending the code with the proposed algorithm, operated with and without computing an alternative next hop, in order to compute the required path while varying the number of nodes in each topology. Before evaluating the performance issues for the network topologies with respect to computing a next hop over different networks, it is important to determine which network parameters could affect the QoS of the streamed video traffic. Here, the research focuses on two parameters, which may better determine the effect of video traffic techniques:

- Packet loss ratio: This is the packet ratio between dropped and sent data packets.
- Average end-to-end delay: This is the average time between transmission and arrival data packets.

However, we have created an extension to the routing protocol by performing our Algorithm 1 in order to prepare an adjacent node to be next hop if faced with the required conditions. As we discussed before, we add enquiry packets with negligible sizes to find the next hop as an alternative to urgent packets.

Experimental results. To evaluate the performance of our algorithm in a smart city IoT environment, we modelled more than eight scenarios in NS2. Each scenario had a different number of nodes. We also considered the amount of traffic that could be passed on the network in each experiment. The topology started from 20 up to 200 nodes: the node at the beginning of the network acted as the tree root, while the one at the end of the network alternately generated one normal data packet and one urgent data packet, within a period of seconds; the node at the centre of the square acted as the tree root, while the nodes at the end of the branches alternately generated one normal data packet and one urgent data packet, within a certain period of time. We first evaluated the packet latencies.

In particular, we have observed the effect of MANET node density on real-time traffic delivery latency. We have simulated the reference scenarios by constantly increasing the number of randomly placed MANET nodes and repeated 30 runs for each test. The

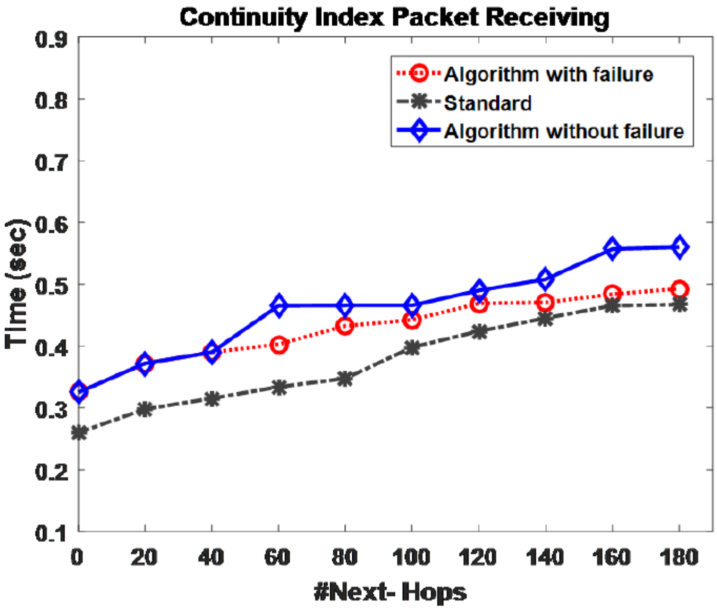

Figure 5. Continuity index for sending and receiving

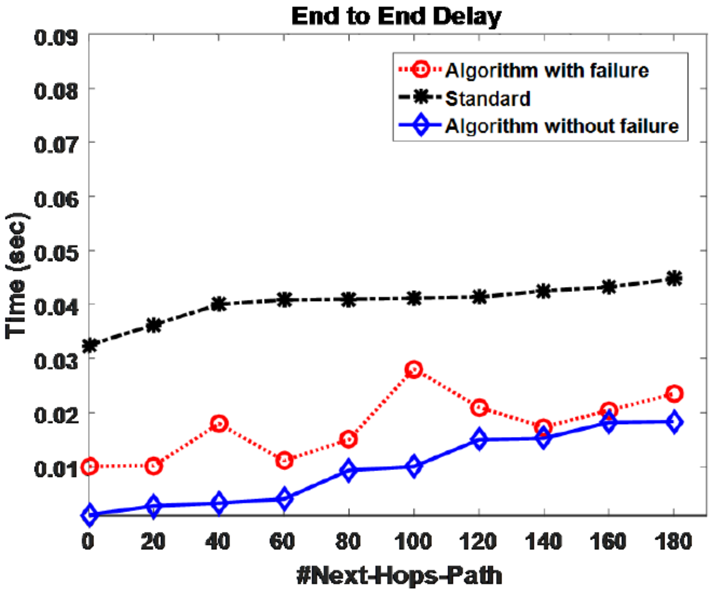

Figure 6. End-to-end delay

collected confidence intervals were always under ±5% of the estimated average. In Figure 5, we can see that our algorithm has improved in terms of receiving real-time data with or without failure. In addition, the data packets showed continuity improvements when passing between the nodes among the networks from the path, which, according to our algorithm, is booked between the source and the destination. However, in Figure 6, the delay time has also improved as we have ensured that the nodes are only passed to the emergency packets and reserved the long path until the session time is ended. The figure shows different cases such as where the topology might face sudden failure without notification.

In this case, the algorithm can reroute the traffic according to the adjacent node; although the delay time will increase, it will still show improvements compared to the standard one. The algorithm can perform these steps, depending on layer 2, by losing the signals, as we have assumed that the loss of signals means that failure is detected in less time and there is no response from the one that fails. As we can see in Figure 7, the throughput is based on the number of packets received among all experiments. Further, because the delay will be reduced and the path between the source and the destination will be reserved for the emergency packets, then the loss of packets will be reduced and the throughput will increase.

Figure 8 shows the simulations run during peak time. We found that the network had a huge number of traffic transfers in the networks. Meanwhile, we operationalized our algorithm in order to find the required path between the source and the destination.

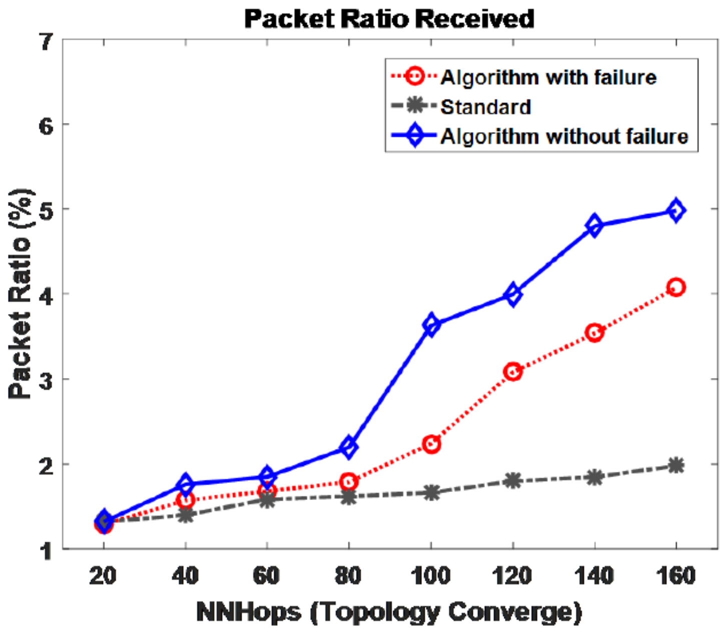

FIGURE 7. Throughput of received packets

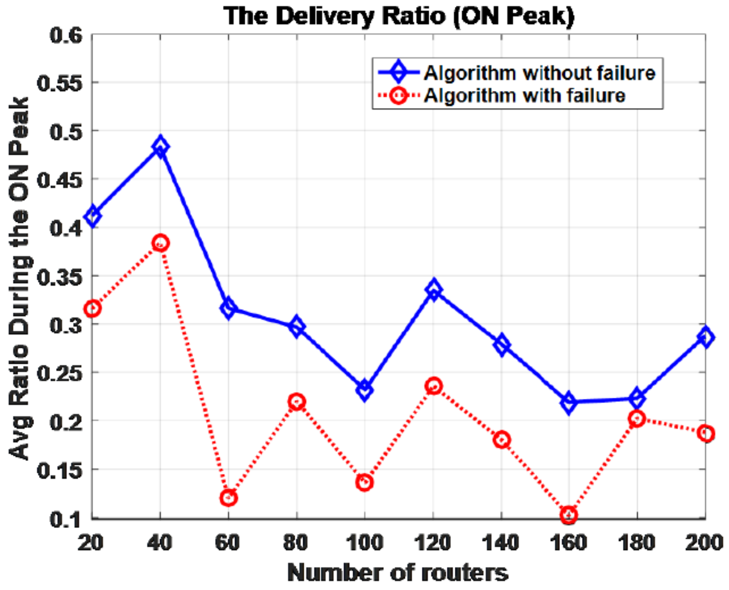

FIGURE 8. Ratio of received packets

Hence, we confirmed that the results were still acceptable in cases both with failure or without failure, but those without failure are still better as there is no need for the mechanism to reroute the traffic.

5. **Conclusion.** The paper proposes a trusted path and an ordered and speedy emergency navigation algorithm. To solve the problem of network congestion, delay time and throughput, and to minimize load on the required path along with evacuation time, the emergency evacuation problem is converted to a traditional network flow problem. The purpose here is to create a high-priority path by using an IoT smart algorithm to classify the traffic as an emergency. A reliable algorithm, i.e., an event-aware backpressure scheduling scheme with a multi-level priority approach, both solves the emergency problem and enables regular packets to deliver data on real-time live streaming from source to destination within the specified timeline. By assigning a priority to the packets, it becomes easier to control the congestion problem on the network. Our simulation results have shown that our scheme is better than the existing approaches in terms of network congestion, throughput, delay time, loss ratio and network overheads, as well as in terms of many other discussed factors.

Acknowledgements. This research was supported and funded by the Research Sector of the Arab Open University (Kuwait Branch) under Decision Number 19032.

REFERENCES

[1] K. Sha, T. A. Yang, W. Wei and S. Davari, A survey of edge computing based designs for IoT security, *Digital Communications and Networks*, 2019.

[2] M. Elkhodr, B. Alsinglawi and M. Alshehri, A privacy risk assessment for the Internet of Things in healthcare, in *Applications of Intelligent Technologies in Healthcare*, Springer, 2019.

[3] G. Rathee, A. Sharma, H. Saini, R. Kumar and R. Iqbal, A hybrid framework for multimedia data processing in IoT-healthcare using blockchain technology, *Multimedia Tools and Applications*, pp.1-23, 2019.

[4] M. Conti, P. Kaliyar, Md M. Rabbani and S. Ranise, Attestation-enabled secure and scalable routing protocol for IoT networks, *Ad Hoc Networks*, vol.98, 2019.

[5] A. A. AlZubi, M. Al-Maitah and A. Alarifi, A best-fit routing algorithm for non-redundant communication in large-scale IoT based network, *Computer Networks*, vol.152, pp.106-113, 2019.

[6] A. K. Chattopadhyay, A. Nag, D. Ghosh and K. Chanda, A secure framework for IoT-based healthcare system, in *Advances in Intelligent Systems and Computing*, M. Chakraborty, S. Chakrabarti, V. Balas and J. Mandal (eds.), Singapore, Springer, 2019.

[7] H. Kharrufa, H. A. A. Al-Kashoash and A. H. Kemp, RPL-based routing protocols in IoT applications: A review, *IEEE Sensors Journal*, vol.19, no.15, pp.5952-5967, 2019.

[8] M. Al Rawajbeh, Performance evaluation of a computer network in a cloud computing environment, *ICIC Express Letters*, vol.13, no.8, pp.719-727, 2019.

[9] F. Al-Turjman, H. Zahmatkesh and R. Shahroze, An overview of security and privacy in smart cities' IoT communications, *Trans. Emerging Telecommunications Technologies*, 2019.

[10] M. A. V. Paul, T. A. Sagar, S. Venkatesan and A. K. Gupta, Impact of mobility in IoT devices for healthcare, in *Lecture Notes on Data Engineering and Communications Technologies*, S. Patnaik, X. S. Yang, M. Tavana, F. Popentiu-Vlădicescu and F. Qiao (eds.), Cham, Springer, 2019.

[11] I. A. Alameri, MANETS and Internet of Things: The development of a data routing algorithm, *Engineering, Technology & Applied Science Research*, vol.8, no.1, pp.2604-2608, 2018.

[12] D. Giusto, A. Iera, G. Morabito and L. Atzori, *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*, Springer Science & Business Media, 2010.

[13] B. H. Al-Qarni, A. Almogren and M. M. Hassan, An efficient networking protocol for Internet of Things to handle multimedia big data, *Multimedia Tools and Applications*, pp.1-18, 2018.

[14] W. A. Jabbar, W. K. Saad and M. Ismail, MEQSA-OLSRv2: A multicriteria-based hybrid multipath protocol for energy-efficient and QoS-aware data routing in MANET-WSN convergence scenarios of IoT, *IEEE Access*, vol.6, pp.76546-76572, 2018.