Soft Computing (2022) 26:10707–10716
https://doi.org/10.1007/s00500-022-06875-6

FOCUS

A reliable wireless communication mechanisms and decision support system for the IoT networks

Bo Jin[1] · Fazlullah Khan[2] · Ryan Alturki[3] · Mohammed Abdulaziz Ikram[4]

Accepted: 1 February 2022 / Published online: 2 March 2022

Abstract
Due to the overwhelming characteristics of the IoT (Internet of Things), it has been used in different application areas to monitor various activities continuously. However, the development of a reliable decision support system (DSS) and communication approach are among the core issues associated with the traditional networking infrastructures in general and IoT in particular. Numerous communication mechanisms have been reported in the literature to address these issues in traditional and resource constraint networks. In this paper, a networking parametric ensemble-based wireless communication approach is presented to ensure reliable transmission of the packets from source to destination in the IoT networks. The proposed approach bounds every member device to collect valuable data from the neighboring devices, preferably those with minimum hop count value, to find the most optimal neighboring device and enforce an optimal path for onward communication in the IoT networks. Additionally, a reliable and efficient DSS is presented preferably for servers to refine the captured data before processing which enhances the accuracy. Simulation results have verified the exceptional performance of the proposed DSS on real-time and benchmark datasets in terms of various evaluation metrics in the IoT networks, with the accuracy of the proposed DSS being around 95%.

Keywords Internet of Things · Wireless communication · Decision support system · Routing · Data fusion

1 Introduction

During the last decade, technological advancements in micro-electro-mechanical systems (MEMS) have enabled researchers and scientists to develop smart sensing enable monitoring systems. These systems can assist human beings in controlling various industrial processes, preferably hazard activities. Internet of Things (IoT) is a network of these devices C_i, preferably MEMS-based sensors and actuators, with self-organization capabilities. These IoT-enabled networks are used to automate numerous activities through decision support systems (DSS) in smart cities, smart grids, agriculture, telemetric, agriculture and industrial processes etc., Rahim et al. (2021). Every member device C_i of the IoT network interacts directly with the environment and captures the desired data after a defined time interval transmitted to the concerned server S_j via a wireless communication medium. The communication approaches adopted by these devices C_i are single-hop (if devices are in direct communication range) or multi-hop if direct communication with the intended server module S_j is impossible. Usually, single-hop communication among various devices C_i (preferably sever and member device) is simpler than multi-hop communication where other devices are used as relaying devices in the IoT networks. These mechanisms should be smart enough to enable simultaneous communication of various interested devices C_i preferably with a common server module S_j in the IoT network Jan et al. (2020).

Communicated by Tiancheng Yang.

✉ Fazlullah Khan
fazlullah@awkum.edu.pk

[1] School of Information and Communication Engineering, Beijing University of Posts and Telecommunications, Beijing 100876, China

[2] Department of Computer Science, Abdul Wali Khan University Mardan, Mardan 23200, KPK, Pakistan

[3] Department of Information Science,College of Computer and Information Systems, Umm Al-Qura University, Makkah, Saudi Arabia

[4] Computer Science Department, Al Jumum University College, Umm Al-Qura University, Makkah, Saudi Arabia

In the literature, various communication approaches have been presented to address this issue (preferably with available resources and infrastructure) and ensure the establishment of reliable communication sessions among various interested devices C_i in the IoT networks. The shortest path-enabled wireless communication approaches were reported to ensure successful transmission or delivery of packets in the multi-hop communication infrastructure. In these mechanisms, every device C_i is bound to find and enforce the shortest path, a path with minimum possible hops from source to destination modules, in the IoT networks Cheng et al. (2018). These approaches are ideal solutions for scenarios or application areas where timely data delivery is preferred over the lifetime of devices or networks such as military or border monitoring. These approaches are extremely useful for achieving a maximum delivery ratio with minimum possible delay as packets are forwarded via the most feasible path in the IoT networks. However, a common problem with shortest-path enabled approaches are that devices on these paths consume their onboard battery more rapidly. However, it is challenging when multiple devices C_i share these paths Singh et al. (2010). The literature reported multiple traffic distribution approaches to resolving the issue associated with the shortest path-enabled approaches. Usually, these schemes enforce every device to distribute overall traffic across the IoT networks uniformly. Residual energy E_r is one of the common metrics that is used by various devices in selecting an appropriate relaying device in the IoT networks Laouid et al. (2017); Kim (2016); Kamal and Hamid (2017); Sari and Caglar (2018). A biased traffic distribution approach was presented in Khan (2019); Zheng et al. (2020) where every device is bound to compute the vulnerability of its neighboring devices. Every source device is enforced to transmit or forward packets via those paths or neighbors where the probability of vulnerable devices is preferably low if not zero. For this purpose, the vulnerability or criticality of neighboring devices is computed before the network becomes operational, and thus, every device has information about its vicinity. Likewise, a similar approach with different parameter metrics and operational statistics were presented in Khan et al. (2019) where four optimal paths are identified. Then member devices are bound to use the two best optimal paths for communication until a specific threshold of their onboard battery. However, a common problem associated with these approaches is how to realize the computational vulnerability process, which seems not realistic in the IoT networking infrastructures.

In addition to the flat networking infrastructures, hierarchical or tree-enabled wireless communication mechanisms were reported to resolve coverage area problems, limited communication range, the burden on a particular device and utilization of the onboard batteries in the IoT-enabled networks Nori and Sharifian (2020). In these approaches, every ordinary device is bound to be the nearest cluster head (CH) member in the resource-limited network. Member nodes can communicate directly with the intended server or CH module as these nodes are deployed close to the concerned CH. Furthermore, CH may either communicate directly with the base station (if it is deployed within the expected wireless communication range of the transceiver module) or through other CH modules nearer to the base station. However, various issues are tightly coupled with these approaches, such as failure of a cluster head (CH) or transmission of packets simultaneously to a common destination module, CH selection process, ordinary devices and CH's in the IoT networks. Apart from traffic distribution, the design and development of a reliable DSS are challenging issues. A technology-assisted DSS for the monitoring of orange orchards was presented in Khan et al. (2018) to automate irrigation activity. Sensor nodes were deployed in the agriculture field to capture real-time data and share the captured data with the base station after a defined time interval. Furthermore, a DSS was implemented on the server-side to ensure detection of the needy plot on time. Although this approach has automated the irrigation activity effectively, it did not mention how the system would respond if the number of deployed sensors were increased as there were currently three operational sensors deployed in the field. Thus, a reliable and efficient communication approach is needed to be developed to address most of the issues mentioned above associated with existing schemes. Furthermore, it should be integrated with the DSS to automate various activities in the IoT networks.

In this paper, a DSS-enabled reliable communication is presented to ensure timely delivery of the captured data with a minimum possible delay. The DSS is smart enough to activate the concerned module when the threshold value is matched. Initially, the proposed system ensures timely delivery of the captured data by bounding every member device to transmit via the most optimal paths available in the IoT networks. Secondly, DSS is smart enough to activate the concerned unit when requirements are met. The contribution of this research work are

1. A novel wireless communication approach with minimum possible delay and maximum average packet delivery ratio for the IoT networks.
2. A mechanism to enforce every member device, C_i, to transmit its packets via the most optimal paths or neighbors in an IoT-enabled network.
3. Development of smart decision support system for the IoT network to ensure activation of the concerned unit.

The rest of the paper is organized according to the following pattern. In Sect. 2, the literature review is discussed in detail. In Sect. 3, the proposed scheme is presented followed by results and discussion in Sect. 4. Finally, the paper is concluded in Sect. 5.

2 Literature review

In this section, a comprehensive literature review about reliable communication is presented to guarantee timely delivery of the captured data with minimum possible end-to-end delay IoT-enabled networks Wieland et al. (2019). The least-cost or shortest path-enabled wireless communication approaches were reported to resolve the issues mentioned above and are quite common in the Military application area of the IoT networks. In these approaches, member devices or sensor nodes are bound to find the most optimal path (preferably with minimum possible hop count value) and enforce it onward with the intended server or cluster head module. The network's lifetime and ordinary nodes are among the common issue associated with these approaches. These become even more complicated if multiple sensor nodes(preferably source modules) share a common path in the operational resources constraint network.

An alternative approach, that is, uniform distribution of traffic, is one of the ideal approaches to an enhanced lifetime of both individual nodes and networks. Thus, a gradient-enabled traffic distribution and communication scheme is reported to address the lifetime issue of the resource-limited networks. In this mechanism, CH or sink is bound to find a feasible communication path ad enforce its member devices to utilize it for onward communication with the BS or CH. This process is continuously applied or followed unless one or more member devices consume their onboard battery completely Cheng et al. (2014). As shortest path-enabled approaches rely on an individual communication path, its lifespan is short because sensor nodes residing on these paths consume their energy more rapidly and thus cannot perform accordingly. Once a path becomes compromised, another optimal path is found and enforced by the concerned module for onward communication in the operational networking infrastructures. However, selecting and reinforcing the feasible alternative path is complex and time-consuming. A biased network traffic distribution approach was presented in Khan (2019); Zheng et al. (2020) where every member device is bound to compute vulnerability or criticality. The critically is defined as susceptibility of the network from a longer connectivity perspective of its neighboring devices. Every source device is enforced to transmit or forward packets via those paths or neighbors where the vulnerable devices or nodes are preferably low if not zero. For this purpose, the vulnerability or criticality of neighboring devices is computed, a one-step computation process that is performed only once as soon as the network is deployed, before the network becomes operational. Thus every device has information about its vicinity. Likewise, a similar approach with different parameter metrics and operational statistics were presented in Khan et al. (2019) where four optimal paths are identified. Then member devices are bound to use the two best optimal paths for communication until a specific threshold of their onboard battery. However, a common problem with these approaches is realizing the computational vulnerability process, which seems unrealistic in IoT networking infrastructures. Likewise, a traffic distribution approach which is based greedy-growing algorithm was presented to ensure a uniform traffic distribution across the network Kim et al. (2008). Similarly, Touray et al. Touray et al. (2012) have presented a biased traffic or load distribution mechanism to guarantee packets transmission uniformly across multiple available paths in the constraint oriented networking infrastructure. These traffic distribution approaches are quite well in those application areas where the priority of the network lifetime is higher than the expected delivery time of the captured data. Furthermore, these mechanisms have an approximately lower APDR ratio of the total transmitted packets in the operational networks. Likewise, multiple paths-based wireless communication approach was reported by Liu et al. Liu et al. (2019) where nature inspires mechanism is adopted to find reliable wireless communication paths., this procedure is repeated for every member device. A traffic distribution strategy that is based on the tree data structure is reported to enhance the lifespan of the underlined networks Daflapurkar et al. (2017). In this approach, every leaf node or device is forced to choose one of the parent nodes as its relaying node, which will be responsible for forwarding its captured data to the concerned destination module. Selection of the relaying parent node is subject to the residual energy and APDR ratio of the concerned device in the operational network. However, a challenging issue tightly coupled with these approaches is the failure of the concerned relaying node, i.e., single-point failure, which results in partitioning the entire network. Shah et al. Shah and Rabaey (2002) have reported a probabilistic and energy-aware traffic distribution approach for the ad-hoc networks. This mechanism has considerably enhanced the lifetime of the resource-limited networks with minimum possible additional overheads. Likewise, C. Schrugher et al. Schurgers and Srivastava (2001) have described three different ways, i.e., stochastic, stream-based and energy-based, to distribute traffic across various available paths and thoroughly examined which mechanism has the potential to increase the lifetime of the underlined networks with the available resources. They have concluded that energy-based traffic distribution is ideal for resource constraint networks. A weighted and optimal path-enabled traffic distribution mechanism was reported by Yousif et al. Khalid et al. (2018) to ensure how uniform traffic distribution is achieved. Although various techniques discussed here have resolved the enhanced lifetime issues, these approaches have compromised various other performance metrics such as end-to-end delays.

Ant colony-enabled traffic distribution mechanism was reported where a pseudo-random mechanism is utilized to find an optimal path. Furthermore, this approach is well suited to increase pheromone trail, and uniform energy consumption Li et al. (2019). Similarly, a broadcasting scheme, which is an opportunistic enable approach, is utilized to minimize the energy consumption overhead in the operational networks. Likewise, energy and gauge node-based traffic distribution strategy was reported to distribute traffic uniformly across the network Adil et al. (2020). However, the ratio of the gauge node and their deployments are among the challenging issues associated with this mechanism. Finally, a Path & distance-based traffic distribution mechanism was reported by Aissa et al. Ben et al. (2019) to resolve the aforementioned issues. However, it is effective in a closed building infrastructure only. In addition to the flat networking infrastructures, hierarchical or tree-enabled wireless communication mechanisms were reported to resolve coverage area problems, limited communication range, burdens on a particular device and utilization (preferably efficient) of the onboard batteries in the IoT-enabled networks Nori and Sharifian (2020). In these approaches, every ordinary device is bound to be a member of the nearest cluster head (CH) in the resource-limited network. Member nodes can communicate directly with the intended server or CH module as these nodes are deployed in close proximity of the concerned CH. Furthermore, CH may either communicate directly with the base station (if it is deployed within the expected wireless communication range of the transceiver module) or through other CH modules nearer to the base station. However, various issues are tightly coupled with these approaches, such as failure of a cluster head (CH) or transmission of packets simultaneously to a common destination module, CH selection process, ordinary devices and CH‘s in the IoT networks. Rajaram and Kumaratharan (2020). Multiple attributes-based load balanced and optimized clustering approach is proposed to enhance the lifetime of the operational WSNs Rajpoot and Dwivedi (2020). However, complexity is a common issue associated with these schemes. However, most of these schemes have various issues, i.e., application specificity, overlay complex and expensive due to change in existing technological infrastructure. Therefore, a reliable communication infrastructure with proper DSS is needed to resolve these issues, particularly available resources.

3 Proposed methodology: ensemble-based communication for IoT networks

This section presents a detailed description of the proposed parametric ensemble-enabled wireless communication mechanism designed specifically for IoT networks. The proposed scheme enables every member device C_i in the IoT networks to achieve a maximum APDR ratio with minimum possible end-to-end delivery ratio. Furthermore, every device C_i is bound to collect valuable information from the neighboring devices C_i to select and enforce a least-cost path for onward communication with the intended server or base station module S_j in the IoT networks. The proposed scheme is comprised of three phases (1) hop count discovery phase, (2) Information collection and path identification phase (3) communication phase. A detailed description of these phases is provided below.

3.1 Hop count discover phase in the IoT networks

In this phase, server module or base station S_j is forced to broadcast a control message preferably in the form of a packet, Msg_{hc} where the value of parameter hop count $H_c = 0$ in the payload. Usually, this message is received by devices C_i residing in the direct coverage area of the concerned server module‘s transceiver according to the Euclidean distance measure as described in Eq. 1.

$$\begin{cases} \forall_{i=0\ldots n} \ \dfrac{\sqrt{(C_{x_i}-C_{x_{i+1}})^2+(C_{y_i}-C_{y_{i+1}})^2}}{(x_i \, + \, y_j)} \ < \ \delta \\ \exists_{i=0\ldots n} \ \dfrac{\sqrt{(C_{x_i}-C_{x_{i+1}})^2+(C_{y_i}-C_{y_{i+1}})^2}}{(x_i \, + \, y_j)} \ == \ \delta \end{cases} \tag{1}$$

where C_i & C_{i+1} represents neighboring devices preferably with different hop count values in the IoT network.

These devices C_i store hop count value of the concern server module S_j and update value of parameter hop count to 1, i.e., $H_c = 1$. Furthermore, these devices C_i wait for the defined time interval, that is, the time required to receive such message from all neighbors, preferably those with similar hop count values, according to Eq. 2.

$$T_{\text{wait}} = \sum_{i=0}^{m} (T_b + T_p + T_d) \mid (C_i \in \text{Neighbors}) \tag{2}$$

where m represents neighbors of the particular device and T_b is the backoff time that a device C_i is bound to wait before broadcasting its packet. Likewise, parameters $T_p \& T_d$ represent propagation time and average transmission delay, respectively. As soon as the waiting time is expired, the concerned device is ready to broadcast the updated message. However, it is bound to postpone transmission of this packet until the backoff time T_b is expired, as depicted in Eq. 3. their H_c values accordingly and broad-cast an updated version of Msg_{hc}, i.e., with value of $H_c = 1$. A backoff timer-based approach is adopted to minimize the probability of collisions where every node C_i holds its packets until the backoff timer is expired. The backoff timer is selected randomly using Eq. 3.

$$T_b(C_i) = \text{rand}(0 - 1000)\ u\ \text{sec} \tag{3}$$

Backoff timer is used to ensure a collision-free transmission of packets because it is highly likely that multiple neighboring devices C_i have received and updated this packet Msg_{hc} concurrently. Thus in the proposed mechanism, back off timer T_b is utilized to resolve simultaneous transmission of packets that result in a collision. Furthermore, if a collision is detected, both devices are bound to repeat the procedure as mentioned above. This mechanism, i.e., receive and update of Msg_{hc}, is repeatedly applied by every device in the operational IoT networks and continues until the very last member device C_i repeats this procedure. Thus, every device $C_i \in IoT$ has computed its hop count value and equally received hop count of the neighboring devices C_i in the IoT networks.

3.2 Data collection and path identification phase in the IoT network

In this phase, every device C_i is forced to collect valuable information about its neighboring devices C_i, which is used to find the most optimal or least-cost path in the IoT networks. For this purpose, devices C_i with a hop count value of 1 generate a message Msg_{data} with three different parameters such as several neighbors N_k, turn around time TAT as described in Eq. 4, and received signal strength indicator (RSSI) as depicted in Eq. 6. In addition, however, these devices must be used back off timers to minimize the collision probability, described in Eq. 3.

$$\text{TAT}(C_i) = 2 * T_p(C_i, C_{i-1}) \tag{4}$$

However, path loss ratio of the concerned neighboring device C_{i+1} is needed to be computed using Eq. 5 which is given below.

$$P(d) = P(d_0) - 10nlog\frac{d}{d_0} - X_\sigma \tag{5}$$

Where $P(d)$ represents the average path loss ratio which is an important parameter in computing RSSI value of a particular devices C_i in the operational IoT networks. As soon as the value of $P(d)$ is calculated then it is used to find RSSI of the neighboring device C_{i+1} using Eq. 6.

$$\text{RSSI}(S_j) = P_t - P_{\text{loss}}(d) \tag{6}$$

Every neighboring device C_i, preferably those that reside in the direct communication range of the source device, receive this message and generate an updated version of this message where values are assigned the different parameters in the Msg_{data}. However, these devices C_i do not send their messages immediately rather wait for the backoff timer to expire, which is depicted in Eq. 3. Therefore, this mechanism is repeatedly applied by every member device in the operational IoT network to collect neighboring information.

Once a device C_i collects the desired information about its neighboring devices, then optimal neighboring device C_i is selected using equation 7 given below.

$$C_{\text{opt}} = \min\left(\sum_{i=1}^{l}(H_c + N_k + TAT + RSSI)\right) \mid C_i \in \text{Neighborhood} \tag{7}$$

where l represents neighboring devices of the concerned source device C_i in the IoT network. It is to be noted that these parameters have different values, therefore, these values are needed to be normalized before applying Eq. 7. For normalization of these values, the following function is used to normalize these parameters.

$$x_{\text{norm}} = \frac{x - x_{\min}}{x_{\max} - x_{\min}} \tag{8}$$

where x_{norm}, x_{min} and x_{max} are used to represent normal, minimum and maximum values restively.

As soon as every device C_i finds its optimal neighboring device then it share this device with other neighboring devices in the IoT networks. Thus, every source device C_i finds an optimal path using Eq. 9 as presented below.

$$O_{\text{path}} = \text{Min}\left(\sum_{i=0}^{n} C_{\text{opt}}\right) \tag{9}$$

Thus, every device C_i finds the most optimal path (preferably least-cost path in this case) and enforces it for onward communication, i.e., the transmission of packets.

3.3 Communication phase in the IoT network

Every device C_i (“X”) captured the required data by interacting with the phenomenon in this phase. Device X is needed to send this data to the server module, say server “Y”, via the most optimal path selected and enforced in the previous phase. As soon as device X capture data value and generate a packet, the next step is to ensure a collision-free transmission of this packet. For this purpose, device X generates a random number using an Eq. 3 as described in the previous phase and waits for the time interval T_b to expire. Back off timer is necessary as it is highly likely that another device may be interested in starting a communication session with the concerned neighboring device, or maybe another device

C_{i+1} may share the same least cost path with source device X. In order to avoid or at least minimize the collision probability, the backoff timer parameter is utilized in the operational IoT networks. Re-transmission is a costly mechanism as it directly correlates with the average throughput of the networks as described in Eq. 10

$$R_{\text{avg}} = \frac{\sum_{i=0}^{m}(Y_i)}{\sum_{i=0}^{n}(T_x + P_{rTx})} \tag{10}$$

Where R_{avg}, Y_i, T_x and P_{rTx} represent average throughput, successfully delivered packet, transmitted and retransmitted packets respectively. Therefore, the proposed scheme bounds every device C_i to wait for backoff timer expiry prior to transmitting actual data in the IoT network. Moreover, if the collision is detected, then both devices are forced to repeatedly apply the procedure mentioned above to ensure successful and collision-free delivery of the captured data using a multi-hop communication mechanism. A collision may occur if two or more two devices initiate a communication session with a common destination device simultaneously, as described in Eq. 11

$$Tx_{C_i} + \sum_{i=1}^{4}(\text{delay})(C_i) == TxC_{i+1} + \sum_{i=1}^{4}(\text{delay})(C_{i+1}) \tag{11}$$

where TX and delay represents transmission time and end-to-end delay, receptively.

The proposed approach bound every device C_i to utilize those paths identified in the previous phase, as long as one or more devices consume their onboard battery completely. In those scenarios, a source device C_i must repeat the procedure as mentioned above to find another optimal path and enforce it for onward communication in the IoT networks.

3.4 Algorithm for the hop count discovery in the IoT network

Hop count parameter plays a vital role in the development of an efficient and reliable communication approach. Therefore, a simplified algorithm, as Algorithm 1, is presented below for the hop count discovery phase as described in the previous section. Likewise, the proposed parametric ensemble-enabled algorithm, as Algorithm 2, for finding and enforcing optimal or least-cost path is presented below, where it is assumed that the hop discovery phase is completed successfully. Furthermore, member devices are willing to cooperate and share valuable information with other neighboring devices in the operational IoT network.

The proposed optimal or leas cost path algorithm, Algorithm. 3 in this case, is represented below which guarantees reliable communication among source and destination devices in the IoT network.

Algorithm 1 Algorithm for the Hop Count Discovery in the IoT Networks

```
Require: Hop Count of Member Devices $C_i \in IoT$
Ensure: Hop Count Value for Every Device ($C_i \in IoT$)
    Server module $S_j$
      Generate $Msg_{hc}$
      set $H_c \leftarrow 0$
      broadcast $Msg_{hc}$
    for $C_i \leftarrow 0$ to n do
      if $(H_c(Msg_{hc}) > H_c(C_i)$ then
      set $H_c \leftarrow H_c(Msg_{hc}+1$
        if $(T_b == 0$ then
        broadcast $Msg_{hc}$
         else then
         wait for $T_b$ to expire
         end if
       elseif $(H_c(Msg_{hc}) <= H_c(C_i)$ then
         ignore or discard $Msg_{hc}$
         end if
     end for
       return $H_c$
   end hop count discovery
 end
```

Algorithm 2 Proposed Parametric Ensemble-enabled Wireless Communication Approach for the IoT Networks

```
Require: Optimal or Least Cost Path in the Operational IoT network
   where $C_i \in IoT$
Ensure: Optimal Path from Source Device $C_i$ to Destination $S_j$ in the
   IoT Networks
RSSI $(C_i) \leftarrow C_i$ 0
$TAT \leftarrow 0$
Number of Neighbors$N_k \leftarrow 0$
$H_c \leftarrow 0$
SourceDevice $C_i$ ()
    Packet← Generated or Received
    $H_c$ =Algorithm. 1
    $C_{opt} = NeighborDiscovery(N_k, TAT, RSSI(C_{i+1}))$
    $OpyC_i \rightarrow$ min($H_c$ =+$C_{opt}$)
     Packet→ $C_{opt}$
end SourceDevice
OPTNeighborDiscovery $(N_k, TAT, RSSI(C_{i+1}))$
    $C_{opt_{cur}} \leftarrow \infty$
    if $(E_r(C_i) > 20\%)$ then
    for $C_i \leftarrow 0$ to n do
      $C_{opt} \leftarrow N_k$ + TAT + $RTT(C_i)$
      if $(C_{opt} < C_{opt_{cur}})$ then
        $C_{opt_{cur}} \leftarrow C_{opt}$
      elseif $(C_{opt} = C_{opt_{cur}})$ then
        $C_{opt_{cur}} \leftarrow$rand$(C_{opt_{cur}}, opt_{cur})$
      end if
    end for
      return $C_{opt_{cur}}$
  end OPTNeighborDiscovery
end
```

Algorithm 3 Optimal Path Enforcement Algorithm

```
Require: Optimal Member Devices $C_i \in IoT$
Ensure: Least Cost Path ($C_i \in IoT$)
    Source Device $C_i$
      Generate $Msg_{data}$
      set $Opt(C_i) \leftarrow 0$
      broadcast $Msg_{hc}$
    for $Ci + 1 \leftarrow 0$ to n do
      set $Opt(C_i \leftarrow Opt(C_{i...k})$
      if $T_b == 0$ then
        broadcast updated $Msg_{data}$
      else $T_b\ != 0$ then
          wait for $T_b$ to expire
        end if
     end for
        return $Opt(C_i)$
   end Optimal Neighbors
end
```

3.5 Decision support system for the IoT networks

Decision support system (DSS), along with the IoT networks, play a vital role in developing automatically controlled infrastructure for various application areas such as industries, smart buildings and cities, agriculture, military etc. The proposed DSS is implemented on the IoT networks' server module or base station. The proposed DSS thoroughly examined captured data values received from various devices C_i, deployed to monitor the phenomenon. It classifies this data into two classes (1) accurate data values (2) outliers or noise. For this purpose, the proposed DSS approach uses Euclidean distance measure as described below in Eq. 11

$$d_{i,j} = \frac{\sqrt{(C_{x_i} - C_{x_{i-1}})^2 + (C_{y_i} - C_{y_{i-1}})^2}}{(x_i + y_j)} \tag{12}$$

if the value of di, j is 0.5, then it is added to the class where accurate data is stored; otherwise, it is added to the outliers class. Furthermore, these outliers are needed to be refined to improve the accuracy of the proposed DSS and minimize the data loss ratio. For this purpose, if a data value is identified as noise or outlier, then the average of the previously stored accurate value is computed first. Then, the noisy data value is replaced with the refined data value, i.e., the average of the previous two consecutive readings.

4 Results and performance evaluation

This section presents a detailed description of numerous possible simulation results. The proposed parametric ensemble-enabled wireless communication approach and field-proven approaches were implemented in OMNET++, an open-source networks simulation software, to verify the applicability of these approaches. Furthermore, these approaches were tested on various topological structures such as graph-enabled, tree, random top, random-centre, etc. Various simulation parameters and their possible values are provided in the table below. The energy required to transmit and receive a message is assumed to be different, i.e., 91.4 and 59.1 mW, respectively. Likewise, both static and deterministic deployments are utilized. They are used to evaluate the performance of these schemes, i.e., proposed scheme, vulnerability-based, vulnerability aware, multiple path-based, hybrid and opportunistic routing algorithms.

Table 1 Simulation Parameters for the Internet of Things

Parameters	values
Approximate rea where devices were deployed	600m * 600m
Member Devices	100 to 1000
Server Modules	five
Capacity of the On-board Battery (E_i)	52000 mAh
Residual Energy (E_r)	E_i-E_{con}
Packets Transmission Energy Consumption (P_{T_x})	91.4 mW
Channel-Delay (Ch_{delay})	25 milliseconds
Packets Receiving Energy Consumption (P_{R_x})	59.1 mW
Device in Idle Mode	1.27 mW
Device in Active Mode	15.4 μW
Transceiver Energy (T_i)	1 mW
Coverage Area (T_r)	500m
Turn Around Time (TAT_n)	4 msec
Packet Size (P_{size})	128 bytes
Hop Count (H_c) of Base Station	0
Initial Hop Count (H_c) of Sensor Nodes	∞
Sampling Rate of Source Devices	20 seconds
Topologies	Static and Random

4.1 End-to-End delay performance evaluation metric

End-to-end delay is one of the common evaluation metrics that is used by the research community to verify performance of the newly developed wireless communication mechanisms against benchmark approaches. For this purpose, both static and random deployment strategies of the IoT networks are adopted and the communication approach is examined thoroughly. Furthermore, a communication approach which has minimum possible ratio of the end-to-end delay metric is assumed as an ideal solution preferably in the resources constraint networks i.e., IoT and wireless sensor networks.

The proposed parametric ensemble-enable wireless communication approach is checked against field-proven approaches. The simulation result verifies that the proposed scheme is the best possible solution as far as end-to-end latency is concerned. The proposed scheme performs exceptionally well in both scenarios where the IoT network is

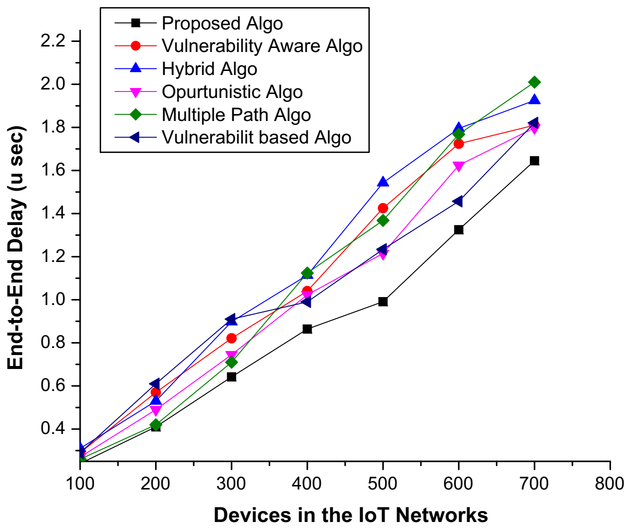

Fig. 1 End-to-end Delay Comparison with Benchmark Approaches in Deterministic Deployment IoT Network

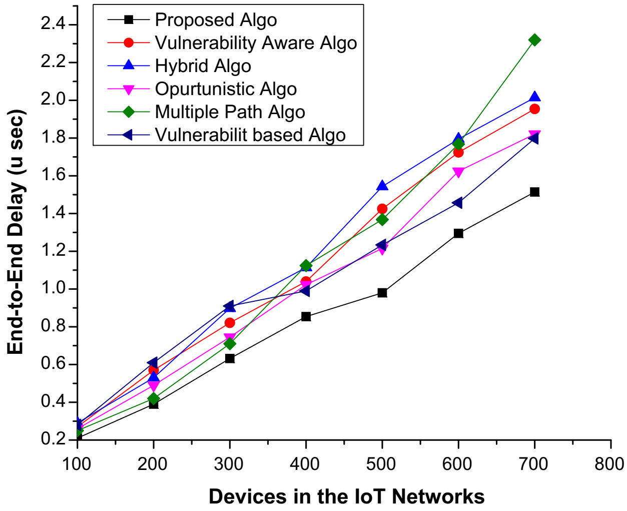

Fig. 2 End-to-end Delay Comparison with Benchmark Approaches in Random Deployment IoT Network

deterministic and random, as shown in Figs. 1 & 2. Furthermore, these results were obtained using different scalability of the IoT networks.

4.2 Average throughput performance evaluation metric

Generally, in traditional networks, average throughput is defined as the ratio of packets or frames received by the intended destination device to the number of packets or frames generated or retransmitted. Apart from end-to-end delay, it is assumed to be another important metric to evaluate the performance of the communication approaches. Likewise, this metric is more valuable in application areas where

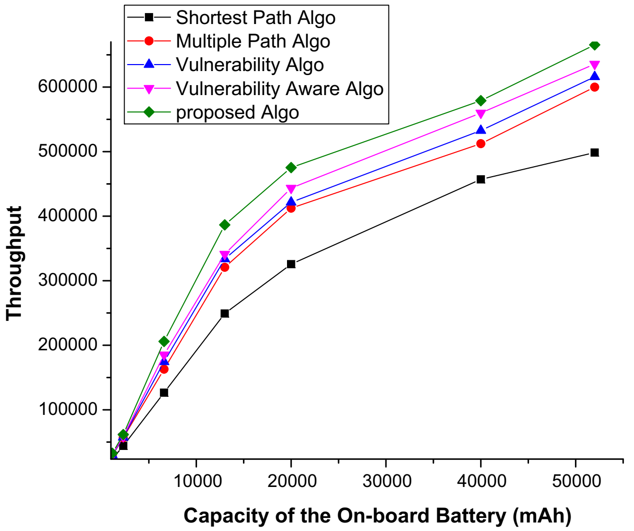

Fig. 3 Average throughput Comparison with Benchmark Approaches in Random Deployment IoT Network

capturing data has higher priority than a lifetime of the IoT networks. The proposed parametric ensemble-enabled wireless communication approach is compared against field-proven approaches for the average throughput performance metric. Simulation results showed that the proposed scheme had achieved maximum possible average throughput than its rival schemes, as shown in Fig. 3.

4.3 Lifetime performance evaluation metric

Generally, in resource-limited networks, lifetime is assumed as one of the vital performance evaluation metrics because a prolonged operational IoT network is always needed. Therefore, various mechanisms have been reported in the literature to enhance the lifetime of the operational IoT network. The proposed parametric ensemble-enabled wireless communication approach can increase the lifetime of IoT networks, as shown in Fig. 4. The proposed scheme primarily enforces member devices to use the shortest path (if possible) for communication. However, when this path is no longer available, then a secondary optimal or leas cost path is enforced for onward communication in the IoT networks. The proposed communication approach has considerably enhanced the lifetime of the operational IoT networks with available resources and sampling intervals.

4.4 Average Packet Delivery Ratio (APDR) performance evaluation metric

Ratio of packets or frames which are received successfully by the intended destination device is defined as average packet delivery ratio (APDR). A communication approach which has achieved maximum possible APDR is considered as the

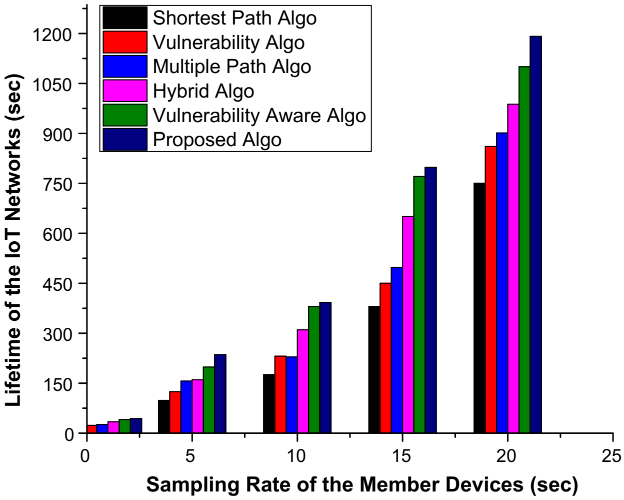

Fig. 4 Lifetime Performance Comparison with Benchmark Approaches in Random Deployment IoT Network

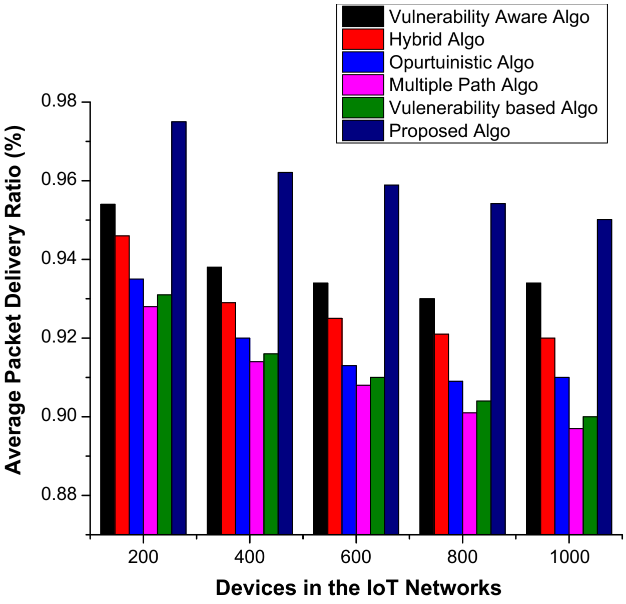

Fig. 5 APDR Performance Comparison with Benchmark Approaches in Random Deployment IoT Network

best suited solution for the IoT networks. The proposed parametric ensemble-enabled wireless communication approach is compared with various benchmark schemes and verifies that the proposed scheme is better than existing solutions preferably in terms of APDR as shown in Fig. 5.

4.5 Limitation of the proposed scheme

Although the proposed decision support system performs exceptionally well in terms of different evaluation metrics. However, excessive messages for the computation of hop count value and residual energy of the neighboring devices are challenging issues with the proposed scheme.

5 Conclusion and future work

Internet of Things (IoT) networking infrastructures have been used in different application areas to monitor and control various activities which are hard to perform by human beings. Reliable communication among various member devices or servers is a challenging issue tightly coupled with the IoT networks. In this paper, we have proposed a reliable parametric ensemble-enabled wireless communication approach, specifically designed for the IoT networks, to address the aforementioned issues, preferably with available resources and infrastructures. Initially, server modules are bound to generate messages and broadcast them received by devices residing in the coverage area of the concerned server‘s transceiver module. Additionally, every member device is bound to collect valuable information from its neighboring devices to find a reliable path. However, it should be cheap as far as utilization of the available resource is concerned. In addition to the communication approach, a decision support system was implemented at the server-side to refine the captured data. The proposed and existing schemes were implemented in well-known simulation software, i.e., OMNET++. Simulation results have verified that the proposed scheme is ideal for IoT networks where maximum lifetime and minimum possible end-to-end delay are needed. In the future, we will try to implement and investigate the exceptional performance of the proposed parametric ensemble-enabled wireless communication approach in IoT networking infrastructure where either member devices or servers are mobile.

Funding The authors have not disclosed any funding.

Data Availability Statement Enquiries about data availability should be directed to the authors.

Declarations

Conflict of interest: All authors declare that they have no conflict of interest.

Ethical approval: This article does not contain any studies with human participants or animals performed by any of the authors.

References

Khan R, Mian Aham IA, Muhammad Z, Ghozani M (2021) A hybrid approach for a seamless and interoperable communication in the internet of things. *IEEE Neworks Magazine*

Jan Mian Ahmad, Khan Fazlullah, Khan Rahim, Mastorakis Spyridon, Menon Varun G, Alazab Mamoun, Watters Paul (2020) Lightweight mutual authentication and privacy-preservation scheme for intelligent wearable devices in industrial-cps. IEEE Trans Ind Inform 17(8):5829–5839

Cheng Long, Niu Jianwei, Luo Chengwen, Shu Lei, Kong Linghe, Zhao Zhiwei, Yu Gu (2018) Towards minimum-delay and energy-efficient flooding in low-duty-cycle wireless sensor networks. Comput Netw 134:66–77

Singh Shio Kumar, Singh MP, Singh Dharmendra K et al (2010) Routing protocols in wireless sensor networks-a survey. Int J Comput Sci Eng Surv (IJCSES) 1(2):63–83

Laouid Abdelkader, Dahmani Abdelnasser, Bounceur Ahcène, Euler Reinhardt, Lalem Farid, Tari Abdelkamel (2017) A distributed multi-path routing algorithm to balance energy consumption in wireless sensor networks. Ad Hoc Netw 64:53–64

Kim Hye-Young (2016) An energy-efficient load balancing scheme to extend lifetime in wireless sensor networks. Cluster Comput 19(1):279–283

Kamal Abu Raihan M, Abdul Hamid Md (2017) Supervisory routing control for dynamic load balancing in low data rate wireless sensor networks. Wirel Netw 23(4):1085–1099

Arif S, Ersin C (2018) Load balancing algorithms and protocols to enhance quality of service and performance in data of wsn. In *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, pages 143–178. Elsevier

Khan Rahim (2019) An efficient load balancing and performance optimization scheme for constraint oriented networks. Simul Model Pract Theory 96:101930

Zheng Xiuping, Idrees Asma, Khan Fazlullah, Lashari Saima Anwar, Khan Rahim, Li Meiling, Tahir Muhammad, Jan Mian Ahmad (2020) A reliable communication and load balancing scheme for resource-limited networks. IEEE Access 8:179921–179930

Khan Rahim, Zakarya Muhammad, Tan Zhiyuan, Usman Muhammad, Jan Mian Ahmad, Khan Mukhtaj (2019) Pfars: enhancing throughput and lifetime of heterogeneous wsns through power-aware fusion, aggregation, and routing scheme. Int J Commun Syst 32(18):e4144

Khademi NM, Saeed S (2020) Edmara2: a hierarchical routing protocol for eh-wsns. Wirel Netw 26(6):4303–4317

Khan Rahim, Ali Ihsan, Zakarya Muhammad, Ahmad Mushtaq, Imran Muhammad, Shoaib Muhammad (2018) Technology-assisted decision support system for efficient water utilization: a real-time testbed for irrigation using wireless sensor networks. IEEE Access 6:25686–25697

Wieland Marc, Li Yu, Martinis Sandro (2019) Multi-sensor cloud and cloud shadow segmentation with a convolutional neural network. Rem Sens Environ 230:111203

Dapeng C, Yingjie S, Yanyan M, Xiangrong W (2014) Lddp: A location-based directed diffusion routing protocol for smart home sensor network. In *Systems and Informatics (ICSAI), 2014 2nd International Conference on*, pages 510–514. IEEE,

Kim Namhoon, Heo Jongman, Kim Hyung Seok, Kwon Wook Hyun (2008) Reconfiguration of clusterheads for load balancing in wireless sensor networks. Comput Commun 31(1):153–159

Barra T, Jinn S, Johnson P (2012) Biased random algorithm for load balancing in wireless sensor networks (bralb). In:*Power Electronics and Motion Control Conference (EPE/PEMC), 2012 15th International*, pages LS4e–1. IEEE,

Liu Xuxun, Qiu Tie, Wang Tian (2019) Load-balanced data dissemination for wireless sensor networks: a nature-inspired approach. IEEE Internet Things J 6(6):9256–9265

Daflapurkar Pradnya M, Meera G, Bhagwan P (2017) Tree based distributed clustering routing scheme for energy efficiency in wireless sensor networks. In:*2017 IEEE International Conference on Power, Control, Signals and Instrumentation Engineering (ICPCSI)*, pages 2450–2456. IEEE

Shah Rahul C, Rabaey Jan M (2002) Energy aware routing for low energy ad hoc sensor networks. In:*Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE*, volume 1, pages 350–355. IEEE,

Curt S, Srivastava Mani B (2001) Energy efficient routing in wireless sensor networks. In *Military communications conference, 2001. MILCOM 2001. Communications for network-centric operations: Creating the information force. IEEE*, volume 1, pages 357–361. IEEE

Amir YK, Yaakob BR (2018) An energy efficient and load balancing clustering scheme for wireless sensor network based on distributed approach. J Phys Conf Ser 1019:012007

Li Xinlu, Keegan Brian, Mtenzi Fredrick, Weise Thomas, Tan Ming (2019) Energy-efficient load balancing ant based routing algorithm for wireless sensor networks. IEEE Access 7:113182–113196

Adil Muhammad, Khan Rahim, Almaiah Mohammed Amin, Binsawad Muhammad, Ali Jehad, Saaidah Adeeb Al, Ta Qui Thanh Hoai (2020) An efficient load balancing scheme of energy gauge nodes to maximize the lifespan of constraint oriented networks. IEEE Access 8:148510–148527

Yousra BA, Abdelmalik B, Mohamed K, Anis K, Zhiwu L, Ting Q (2019) On feasibility of multichannel reconfigurable wireless sensor networks under real-time and energy constraints. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*

Rajaram V, Kumaratharan N (2020) Multi-hop optimized routing algorithm and load balanced fuzzy clustering in wireless sensor networks. *Journal of Ambient Intelligence and Humanized Computing*, pages 1–9

Rajpoot Prince, Dwivedi Pragya (2020) Optimized and load balanced clustering for wireless sensor networks to increase the lifetime of wsn using madm approaches. Wireless Netw 26(1):215–251