IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 17, Issue 3, Ver. VII (May – Jun. 2015), PP 16-24
www.iosrjournals.org

Efficient IOT Based Sensor Data Analysis in Wireless Sensor Networks with Cloud

Raghavendra L A[1,] Dayananda Lal.N[2,] Karthik D U[3]

Abstract: *The improvement of wireless sensor network has offered move to public sensing as it is vibrant sharing model. This creative energy can be clarified under the Internet of Things (IoT) to adopt different information sources inside shrewd urban areas, such as sensors on roads, buildings, radio frequency identifier tags (RFID), cell phones and living spots. Sensor system incorporated with enormous number of nodes where every nodes need to communicate with other node at whenever state of the link changes. Link state (LS) routing protocol directly floods announcement of change in any join's status to each router in the network and Distant Vector (DS) routing uses ceaseless appropriation of current guide of whole system's topology for all switches. However both DS and LS experience the ill effects of disconnection of link when the topology is in constant flow. Proposed system utilizes Greedy Perimeter Stateless Routing Algorithm (GPSR). GPSR algorithm comprises of dual strategies in order to send packets: greedy forwarding at the point where it uses evidence around a router's next nearest within network topology and perimeter routing- is used at the point when packet achieves a locale where greedy forwarding is unimaginable. Nodes in sensor network comprise of bulk of data from different areas. Our proposed system uses cloud storage platform that is extremely helpful to perform data calculation. Advised system is about permitting clients to get data, information and knowledge from sensor data. Aimed GPSR algorithm utilizes broad simulation of mobile remote network to contrast its execution and that of the Dynamic Source Routing. Our aimed system exhibits simulation result by analyzing parameter such as packet delivery ratio (PDR), energy consumption and delay.*

Keywords: *cloud computing; Internet of Things; routing protocols; Wireless Sensor Network*.

I. Introduction

Cloud computing is a passed on system advantages over the network. Cloud computing is a circumstance for giving information resources that are passed on as organizations to the end customer over the web on interest cloud is described with archive discriminating distinguishing proof. Public[12][5], Hybrid[12][5], Community[12][5] and Private[12][5] are the major cloud deployment models and service models are PaaS[12][5], IaaS[5][12], SaaS[12][5]. Merits for going into cloud is simply because by using internet of cloud allows user to access application from anywhere at any time from differing locations. Expansion of cloud are Automatic software restore, Resilience, pay per use, reduced costs, Restoration, Distracted. CC likewise made out of the real hazards such as secrecy of data, consistency of data and systematization. There have been many of cloud storage technology among which our paper utilizes identify-based encryption (IBE) [2] for providing storage on cloud [2].

The Internet of Things (IoT) [3] is a field of study that bindings a extensive number of themes from simply specialized issues such as semantic queries, routing protocols to a blend of specialized and societal effects security, privacy, usability and social and business subjects. IOT systems may help bolster the connection in the middle of "things" and take into account more perplexing structures like Distributed computing and the improvement of Distributed applications. Succeeding improvements may prompt particular Software advancement situations to make the product to work with the equipment utilized as a part of the Internet of Things.

Dynamic source routing protocol does not locally restore a broken link even though the route maintenance mechanism [5]. In the route reconstruction stage, Stale route save information could in like manner achieve irregularities. DSR protocols bring about higher connection setup delay than in table-driven protocols. The performance degrades rapidly with increasing mobility despite the fact that the convention performs low-compactness situations and fine in static. On account of the source-routing mechanism utilized in DSR, appreciable routing overhead is involved.

Caching has come to noticeable quality as a procedure for enlarging ad-hoc routing protocols. Zone Routing Protocol (ZRP), Dynamic Source Routing (DSR) furthermore, the Ad Hoc On-Demand Distance Vector Routing and the all shun continually pushing current topology data throughout the network. Rather, routers implementing such protocols demand topological data in an on-demand design as needed through their packet advancing burden, later routers stores it forcefully. At the point when their cached topological data gets to be outdated, these routers must get more present topological data to keep steering effectively. Routing protocols' message load can be decreased in two directions by means of caching: first one, wherever the forwarding load does not requires routing protocols' message load, it invalidates from pushing topological data say out of gear routers and second one, it regularly lessens the quantity of hops among routers that contains required topological data also router that obliges it like a node that have stored new status of link that is closer than a changed link.

Proposed system utilizes GPSR Algorithm. GPSR algorithm involves of binary strategies for sending packets: greedy forwarding where it utilizes data around a router's prompt neighbors within network topology and perimeter routing**-** is used when packet achieves a locale where greedy forwarding is unimaginable [3].

GPSR algorithm utilizes broad simulation of mobile remote network to contrast its execution and that of the Dynamic Source Routing. Proposed system exhibits simulation result by analyzing parameter such as delay, packet delivery ratio (PDR) and energy consumption.

To achieve scalability, we proposed the fast growing use of geography protocol called Greedy Perimeter Stateless Routing (GPSR) in WSN. Target of proposed system is to provide versatility under expanding quantities of nodes in the network architecture. Later on increase in the number of nodes, proposed system addresses some of main points that methods of scalability are:

- Message cost of Routing protocol: Concerns about how many routing protocol bundles does it drive?
- Application PDR: Concerns about what fraction of applications' packets is delivered successfully?
- State of each node: Concerns about how much storage does it needs at each node?

Networks that impulse on portability, number of nodes or both includes:

- Ad-hoc network: No fixed infrastructure exist in mobile network, hence support applications for temporary collaborations among temporary associates, military users and post-disaster rescuers as at a business meeting or address..
- Sensor networks: Mobile nodes are deployed in very large number of WSN and resources are available at each node. Step down in state every node in a network of a huge number of memory-poor sensors is important.

At each router, state relative to the quantity of reachable destinations is required to traditional shortest-path (DV and LS) algorithms. DSR requires often more state corresponding towards quantity of sink a node advances packets toward also at least one in case of On-demand ad-hoc routing algorithms. In order to decrease the engendering extent of other nodes' overflowed route asks for a nod forcefully stores all source routes it catches. Aimed system demonstrates engendering of topology data for just a solitary hop i.e. each node need to be known only its neighbors' and positions that geographic steering permits routers to be almost stateless. Auto-describing nature of position of each router in the WSN can be easily done in geographic routing. In the absent of any other topological data, location of the candidate next hops and position of a bundle's sink are sufficient to sort correct advancing conclusions.

Either from a GPS device or through extra modes, wireless router's position can be easily determined. Inertial sensors on vehicles and surveying for stationary wireless routers are included in practical result. Recognitions will be received by all unicast packets from widely used IEEE 802.11 wireless network; henceforth all connections in a 802.11 network must be bidirectional.

Lastly proposed system simulates a network that evaluates our GPSR routing calculation. Network topologies in which the remote nodes are generally in a plane are taken into an account. Finally, to check packet they begin with their destination's area we accept that packet originator can emphasis areas of packet sink. Thus, an area enlistment and lookup benefit that maps node locations to positions. Questions to proposed framework utilize the identical geographic routing framework as data packets. Extent of this paper is restricted to geographic routing algorithm. Our paper explains following subdivisions, i.e. address to the algorithms that consist of GPSR routing algorithm that investigate GPSR's presentation, recognize coming investigation chances recommended via GPSR, conduct in simulated mobile network, refer to and separate related work, conclude by summarizing our findings.

II. Architecture

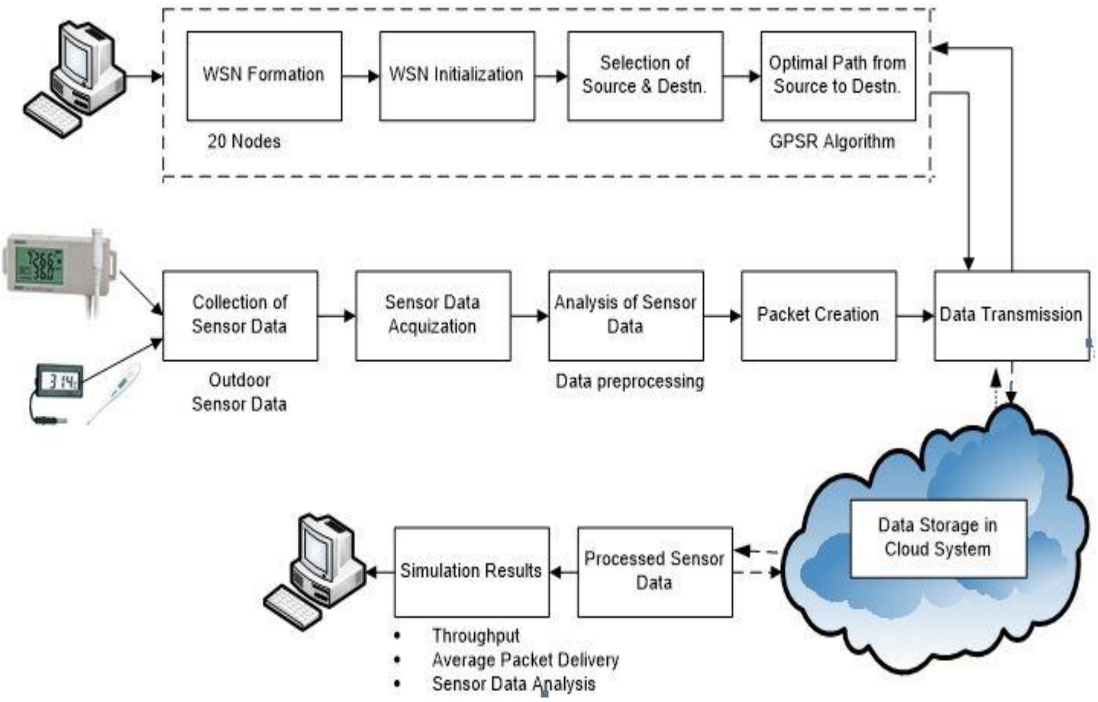


Figure1.Architecture of proposed system

As described in the figure1, the numbers of WSN nodes are defined in wireless sensor network. The nodes are created with different position in the network area size of 100*100 meter. The nodes are pointed with color and node's id. Once the network formation is done then next step is to assign the network parameters. The network parameters are ID, number of channels, energy, etc. initialized with default measures. Source and destination nodes have to be selected by the users among those MANETs nodes. This is user input selection option for source and destination nodes in the network area. Then find the distance between source and destination nodes with optimal way by using GPSR algorithm. In this Greedy Perimeter Stateless Routing Algorithm finds the route by using Greedy method and Perimeter method. Then we need to collect the outdoor sensor data from different files as a input. Next step is we need to apply data pre-processing step for the selected outdoor sensor data. Read the acquired sensor data and selection of attributes among the fields to be selected. We need to analyze what type of sensor data it is. The analysis of sensor data carried in terms low sensor data, medium sensor data and high sensor data. Before transmission of the data, according to packet structure, we need to create the packet wise data.

Lastly we show our estimated results in the form of simulation with packet delivery ratio, energy consumption and delay.

III. Algorithms And Examples

Give us a chance to clarify the Greedy Perimeter Stateless Routing calculation. It is two stages calculation for sending packets: greedy forwarding, it can be utilized effectively wherever it is conceivable and perimeter forwarding is utilized as a part of the spot where greedy forwarding can't be utilized.

3.1 Greedy Forwarding

As illustrated to within introduction beneath GPSR, each packet inside the network are labeled via their initiator with their sink's localities. Accordingly, sending node can sort a mainly ideal, greedy decision within picking a packet's subsequent hop. Particularly if a node recognizes its radio nearest node's locations, generally best decision of next hop is adjacent geologically nearest towards packet's sink [3]. Until the destination is encountered sending in this administration takes after progressively closer geographic hops.

Figure2. Shows an outline of greedy next- skip decision, where D gets a packet and that bounds for the node x. Circle indicates the radio scope of x and the bend piece with compass tantamount to the detachment in the midst of D with respect to x and y is demonstrated as a dashed contort about D. x progresses the packet to y, as the separation in the midst of D and Y is not as much as that of any of x's different contiguous and in the midst of D. Once the packet reaches the destination D, then procedure of greedy forwarding process blocks off.

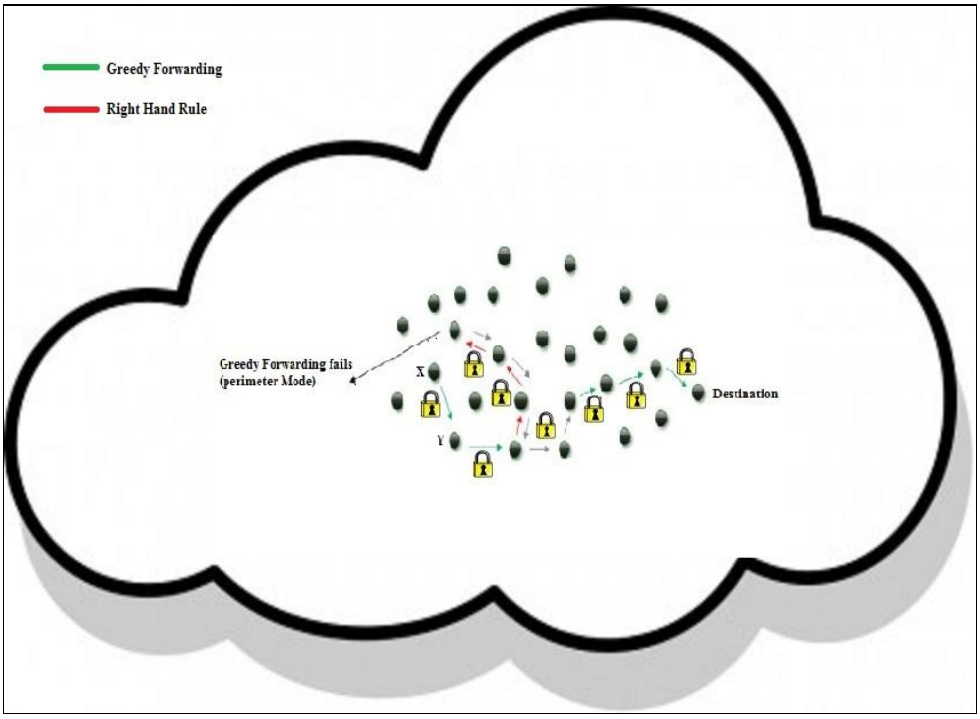


Fig2. Greedy forwarding: y is a closest adjacent of x to destination D.

A basic beaconing calculation furnishes all nodes with their neighbors' positions: from time to time to broadcast a MAC address, each node transmits a beacon that contains just its own specific identifier like position and the IP address. So as to avoid synchronization of neighbors' reference points amongst guides then we jitter every reference point's transmission by 50% of the interval B such that interim is B is considered as the mean between beacon transmission and consistently conveyed in [0:5B;1:5B]

GPSR router expects that neighbor has fizzled or gone out-of-degree upon not accepting a beacon point from a neighbor for a more than time out interim T. And later from its table it eradicates the adjacent. The 802.11 MAC layer likewise gives direct evidences of connection level re- transmission disappointments to neighbors; we decipher these signs identical. Three times of the most extreme value T = 4:5B jittered beacon point interim have been employed in this body of work.

Greedy forwarding incredible preference is its dependence just on information of the prompt sending node that is adjacent. The obliged state is irrelevant and subjects to the thickness of nodes not the aggregate number of destinations in the wireless sensor network. The measure of neighbors inside a node's radio range must be generously not exactly the aggregate number of nodes in the network wherever multi-hop routing is gainful.

Position of node partners using a neighbor gets to be fewer up-to-date among beacons as that neighbor displaces. Accuracy of the arrangement of neighbors likewise diminishes; new neighbors might enter radio range also old neighbors could leave. In this way, the right decision of beaconing between times to retain node's neighbor tables current rely upon rate of portability within network also scope of node's radios. We show the effect of this between time on GPSR's execution in reenactment results. We observe that keeping current topological state for an one-bounce go around a switch is the base expected to do any directing; without learning a topology no helpful forwarding choice can be made using one or more hops away.

Such beaconing system does speak to proactive routing protocol traffic, maintained a strategic distance from by DSR and AODV. Expense of beaconing can be minimize in such a way that GPSR piggybacks neighborhood sending hub's position on all data bundle it support, also conveys all node’s system port within unchecked way, point of fact that each station gets a copy of all bundles for all stations inside radio reach. At a little cost in bytes i.e. twelve bytes each parcel, this arrangement allows all parcels to help as signs. Definitely when any node sends a parcel that contains data, later inundated signal time is then reset. Such sort of forward movement reduces signal traffic within locale of system adequately sending information bundle. In a point of fact, we could make GPSR's beacon component completely receptive through using nodes request beacon with a show "neighbor requests" just when they contains information traffic towards advance. It is always not necessary to make this stride, in any case, as the one-hop beacon burden or a load does not really impact on our simulated network.

The force of eager forwarding to route utilizing just neighbor node's positions accompanies one chaperon downside: some topologies exist within which main course towards a sink obliges a bundle travel momentarily more distant within geometric separation by sink. A straightforward sample of such a topology is demonstrated in Figure 2. Following figure clearly shows that amongst B's neighbors V, P and H, B is closer to H. Once again, the dashed arc about H has a range equivalent to the separation in the middle of x and H. However two ways, (B !P! G!H) and (B! M!N!H), exist to H, B won't decide to forward to w or y utilizing greedy forwarding. B is a nearby greatest in its closeness to H. Some other component must be utilized to forward packets in these circumstances.

3.2 The Right-Hand Rule:

Edges Motivated by Figure3, we observe that union of B's indirect radio degree also circle about H of extent jBHj that is; of length of line bit BH is unfilled of neighbors. We show this district clearly within Figure 3. From node B's perspective, we term shaded area without node a void. B tries to forward a bundle towards sink H past edge of this void. Instinctually, B tries towards course around void; if an approach towards H exists from B, it does avoid nodes arranged inside void else B would have sent to them rapaciously.

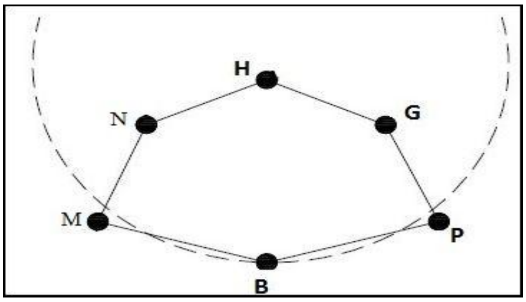
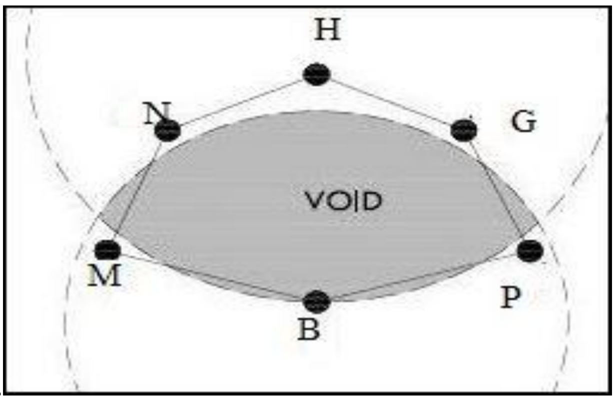


Figure3. Failure of Greedy forwarding: B is a neighborhood greatest in its geographic closeness to H; V and P are more distant from H.

3.2 The Right-Hand Rule:

Edges Motivated by Figure3, we take note of that the convergence of B's roundabout radio extent and the circle about H of range jBHj that is; of the length of line portion BH is unfilled of neighbors. We demonstrate this locale obviously in Figure 3. From node B's viewpoint, we term the shaded locale without nodes a void. B tries to forward a packet to destination H past the edge of this void. Instinctively, B tries to course around the void; if a way to H exists from B, it does exclude nodes situated inside the void or B would have sent to them covetously



.

Figure 4: Void range of node B with respect to destination H.

The farseeing experienced right-hand standard for crossing a chart is portrayed in Figure5. This principle expresses that when landing at node J from node B, the following edge navigated is the following one successively counter right-handed with respect to J from boundary (J;B). It is realized that the right-hand guideline crosses the inside of a shut polygonal locale in clock- wise edge request for this situation, the triangle limited by the boundary between nodes K, J, and K, in the request i.e. B ! J ! K ! B. Road map navigates an outside area, for this situation, the locale outside the same triangle, in counterclockwise edge request.

We try to adventure these cycle-navigating properties to route around voids. In Figure 4, navigating the cycle (B! M!N!H!G!P!B) using the right hand tenet adds up to exploring around the envisioned void, specifically to such nodes which are closer to the destination than B. This achieves an arrangement of edges crossed by the right-hand govern a perimeter. In prior work, the demonstration of mapping perimeters by sending packets on voyages through them has been done by utilizing the right-hand standard. The state amassed in these packets is reserved by nodes, which recuperate from neighborhood maxima in greedy forwarding by directing to a node on a stored border closer to the

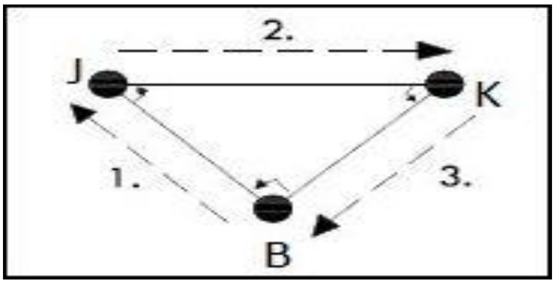


Figure 5: The clock-wise rule or Right Hand Rule/interior of the triangle. J sends a packet that is received by B to its first neighbor in a counter clock-wise about itself, K.

Sending via guiding towards node on a put away outskirt closer towards sink. This technique obliges a heuristic, no-convergence heuristic, towards drive right-hand standard towards find edges that encase voids within regions where edges of diagram cross. This heuristic improves reachability comes about as a rule, yet leaves a certified danger: estimation does not for most part find courses when they exist. No-crossing point heuristic erratically uproots whichever border it encounters second within a few convergence edge. Edge it uproots, on the other hand, may segment the network. In the event that it does, the calculation won't find courses that cross this segment.

3.3 Combining Greedy and Planar Perimeters

We now introduce the full Greedy Perimeter Stateless Routing algorithm, which joins ravenous sending (Section 2.1) on the full system diagram with border forwarding on the planarzed network diagram where eager sending is unrealistic. Survey that all nodes keep up a neighbor table and which stores the areas and territories of their single hop radio neighbors. The following table gives all state needed to GPSR's sending choices, past the state in the packets themselves.

Field	Function
H	Destination Location
Lp	Location Packet Entered Perimeter Mode
Lf	Point on xV Packet Entered Current Face
e0	First Edge Traversed on Current Face
M	Packet Mode: Greedy or Perimeter

Table 1: GPSR packet header fields used in perimeter mode forwarding.

The packet header fields GPSR uses in perimeter-mode forwarding are shown in Table 1. GPSR packet headers include a flag field showing whether the packet is in covetous mode or edge mode. All information bundles are checked at first at their originators as eager mode. Bundle sources likewise incorporate the geographic area of the destination in bundles. Only a packet’s source sets the location destination field; it is departed unaltered as the packet is sent through the network. In the wake of getting an unquenchable mode packet for sending, a node chases its neighbor

Table down the neighbor geologically closest to the packet's destination. In case this neighbor is closer to the destination, the node propels the packet to that neighbor. Right when no neighbor is closer, the node demonstrates the packet into edge mode.

GPSR progresses border mode parcels using a fundamental planar diagram traversal. Essentially, when a parcel enters edge mode at node B bound for node H, GPSR propels it on intelligently closer faces of planar chart, each of which is crossed via line BH. A planar graph has two sorts of faces. Inside faces are close polygonal regions restricted via graph's edges. Outside face is one unbounded face outside outer furthest reaches of outline. On every face, traversal uses right-hand rule to accomplish an edge that crosses line BH. At that edge, traversal moves to contiguousness face crossed via BH. See Figure 6 for delineation. Note that in figure, each face explored is infiltrated by BH the first two and last faces are inside goes up against, while third is outside.

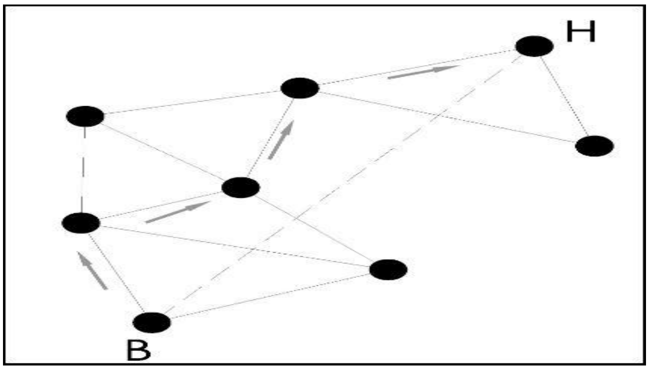


Figure 6: Perimeter Forwarding Example. H indicates destination; packet enters perimeter mode which are generated from node B; solid arrows indicates forwarding hops; dashed line indicates BH.

At the point when a packet enters border mode, GPSR records in the packet the area Lp, the site where insatiable sending fizzled. This area is utilized at resulting hops to figure out if the packet can be come back to a greedy mode. Every time GPSR advances a packet onto another face, it records in Lf the point on BH imparted between the past and new faces. Note that Lf require not be situated at a node; BH typically converges edges, as in Figure 6. At last, GPSR records e0, the first edge (sender and collector addresses) packet a crosses on another face, in the packet.

After getting an edge mode packet for sending, GPSR first thinks about the area Lp in a perimeter mode packet with the sending node's area. GPSR gives back a packet to covetous mode if the separation from the sending node to H is not as much as that from Lp to H. Perimeter sending is just planned to recuperate from a neighborhood most extreme; once the packet achieves an area closer than where avaricious sending beforehand fizzled for that packet, the packet can proceed with eager advancement toward the destination without prior of coming back to the earlier nearby maximum.

At the point when a packet enters edge mode at B, GPSR advances it along the face crossed by the line BH. B advances the packet to the first edge counterclockwise about B from the line BH. This discourages mines the first confront over which to forward the packet. From that point, GPSR advances the packet around that face utilizing the right-hand guideline. There are two cases to consider: either B or H is joined by the picture.

When B and H are connected by the graph, traversing the face bordering B in either direction (we use the previously described right- hand rule) must lead to a point y at which BH intersects the far side of the face. This is the case whether the traversed face is interior or exterior. At P, the distance between the packet and its destination has been reduced using GPSR in comparison with the packet’s start in perimeter mode at B.

While forwarding around a face, GPSR determines whether the edge to the chosen next hop n intersects BH. GPSR has the in- formation required to make this determination, as Lp and H are recorded in the packet, and a position of each node stored in GPSR as well as its neighbors node's position. If a node borders the edge where this intersection point P lays, GPSR sets the packet’s Lf to P. At this point, the packet is forwarded along the next face bordering point P that is intersected by BH. The node forwards the packet along the first edge of this next face by the right-hand rule, the next edge counterclockwise about itself from n. This first edge on the new face is recorded in the packet’s e0 field.

This methodology rehashes at progressively closer faces to H. At every face, the packet advances by the right-hand standard until coming to the edge that meets with BH at a point y closer than the parcel's Lf field to H. At long last, the face containing H is come to, and the right-hand- guideline prompts H along that face.

At the point when H is not reachable i.e., it is detached from the chart two cases exist: the separated node lies either inside an inside face, or outside the outside face. GPSR will forward perimeter mode packet until the packet achieves the comparing face. After coming to this inside or outside face, the packet will visit unsuccessfully around the whole of the face, without finding an edge converging BH at a point closer to H than Lf. At the point when the packet crosses the first edge it tackled this face for the second time, GPSR perceives the reiteration of sending on the edge e0 put away in the packet, and accurately drops the packet, as the destination is inaccessible; the border mode chart traversal to a reachable destination never sends a packet over the same connection in the same bearing twice.

Note that GPSR will voraciously forward a bundle for conceivably numerous jumps, before parcel circles on an outside or inside face also is perceived as undeliverable. In event that greater part of inaccessible destinations lies past limit of a solitary face, undelivered parcels may assemble at that face of the system chart. This conduct is an immediate result of GPSR's shirking of transitive directing convention traffic over numerous jumps from a destination to a sending switch which is closest towards sink. Diverse methods for scaling directing have comparative impacts, nonetheless: chain of command used towards scale steering on wired systems darkens intra-area join disappointments from spine within light of a legitimate concern for scaling or surmounting. Thusly, between space coordinating system will push a parcels an uncommon detachment, with potential result that group will be dropped inside sink AS

Sometime recently the end-to-end contention, the most intelligent spot for directing inaccessibility to be resolved, and the heap on the network from undelivered packet to be diminished, is at the sending end-framework. Components from inside the system, as ICMP Unreachable, are difficult to decipher at senders; it is difficult to know on what time scale they demonstrate inaccessibility, for instance. Applications running over a GPSR-directed system, or whatever other network, should to offer an acclimating burden; senders should to cut their transmission rate non attendant criticism from beneficiaries.

IV. Simulation Results

Our proposed system simulates the sensor node parameters and shows that advised system has greater performance over the existing system in terms of packet delivery ratio, delay and energy consumption.

4.1 Packet Delivery Ratio (PDR): The proportion of the quantity of conveyed information packet to the destination. This outlines the level of conveyed information to the destination**.** Refer figure 7.

4.2 End-to-end Delay: The normal time taken by an information packet to touch base in the destination. It likewise incorporates the deferral brought on by course revelation procedure and the line in information packet transmission. Just the information packet that effectively conveyed to destinations that checked. Refer figure 8.

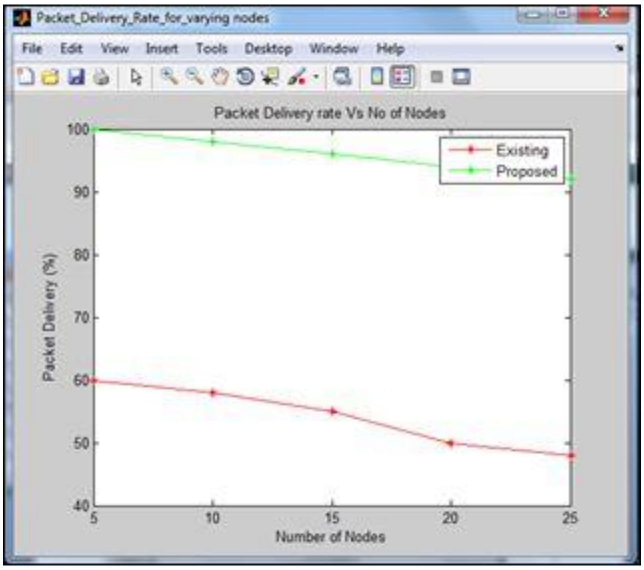


Figure 7: Packet Delivery Ratio.

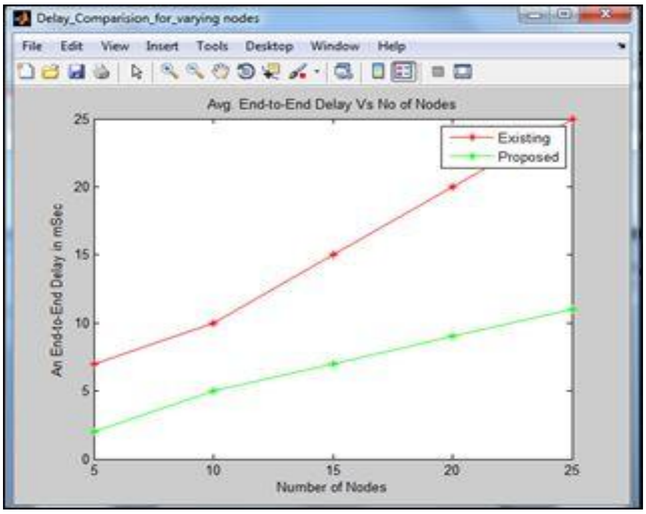


Figure 8: Packet Delivery Ratio.

4.3 Energy Consumption: The amount of energy consumed by all the nodes which falls in the established route while transmitting a packet from source and destination is termed as energy consumption. Refer figure 9.

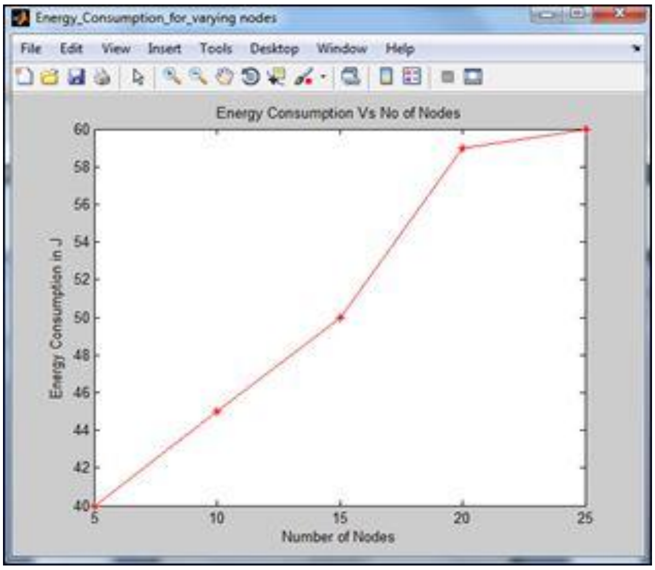


Figure 9: Energy Consumption.

References

[1]. Ashraf E, Al- Fagih (member, IEEE) Fadi M. Al-Turaman (member, IEEE), Waleed M, Alsalih and Hossam S, Hassanein (senior member IEEE): A priced public sensing for heterogeneous IOT Architecture.

[2]. Sivashakthi, Dr. N Prabakaran (2013): A Survey on Storage Techniques in Cloud Computing, Volume 3, Issue 12.

[3]. Kumaraswamy Krishnakumar, Ling wan: University of Melbourne: .A Framework for IoT Sensor Data Analytics and Visualization in Cloud Computing Environments.

[4]. Brad Karp Harvard University / ACIRI, H. T. Kung Harvard University: GPSR: Greedy Perimeter Stateless Routing for Wireless Networks.

[5]. JOHNSON, D. B.AND MALTZ, D. B: Dynamic source routing in ad hoc wireless networks. In Mobile Computing, T. Imielinski and H. Korth, Eds. Kluwer Academic Publishers, 1996, ch. 5, pp. 153–181.

[6]. Pradeep Kumar Tiwari, Dr. Bharat Mishra: Cloud Computing Security Issues, Challenges and Solution (ISSN 2250-2459, Volume 2, Issue 8, August 2012).

[7]. T. Grance and P. Mell, ―The NIST definition of cloud computing NIST U.S. Dept. Commerce, Special Pub., 2011, pp. 145–800.

[8]. C. Perkins, Ad Hoc Networks, Addison-Wesley, Reading, MA, 2000.

[9]. Mohammed ERRITALI, Oussama Mohamed Reda, Bouabid El Ouahidi: "Greedy Perimeter Stateless Routing" for its integration into the " Java Network Simulator'' Volume 2, Issue 2, February 2012.

[10]. Olatunde Abiona1, Adeniran Oluwaranti2, Ayodeji Oluwatope2, Surura Bello2, Clement Onime3, Mistura Sanni2, Lawrence Kehinde4 :"Wireless Network Security"

[11]. H. Yang, F. Ricciato, L. Songwu and L. Zhang, "Securing a wireless world," The Proceedings of IEEE, Vol. 94, No. 2, 2006, pp. 442-454.

[12]. http://www.thbs.com/downloads/Cloud-Computing-Overview.pdf: Indian international journal of computer science.