RELIABLE AND ROBUST HYBRID VDVH AND MODIFIED RGR FOR MANET

[1]ANURAGH VIJJAPU, [2] Dr. AMARAVATHI PENTAGANTI
[1]Ph. D Scholar, Department of CSE, NIILM University, Kaithal, Haryana.
[2]Professor, Department of CSE, NIILM University, Kaithal, Haryana.

ABSTRACT: In order to improve the routing performance in the face of fast changing network topology, This paper proposes a novel Robust Geographic Routing (RGR) protocol which takes advantage of the broadcast nature of wireless medium by employing opportunistic routing like forwarding strategy. At the same time, a Virtual Destination based Void Handling (VDVH) scheme is also proposed to work together with RGR. Simulation results show that RGR achieves excellent performance even under high node mobility and the new void handling scheme also works well and further enhances the performance of RGR.

Keywords: Wireless Sensor Network, Virtual Destination based Void Handling, Robust Geographic Routing,

Introduction: Feasible executing and aggregating association are offered on one hand and On the other hand, it might try to increase unapproved data for its own special points of interest. Past the cloud, the entire structure incorporates one CA, different proprietors and clients, wherein CA is accepted to be absolutely trust, while clients can be hazardous (Yan et al. 2016). CA is liable for key course and time token spreading. We recognize that a perilous client may attempt to unscramble the figure substance to pick up UN attested information certainly, combining plotting with various clients. The proposed TAFC can understand a fine-grained and facilitated release find a workable pace: Only a client with fulfilled property set can find a good pace after the allot time. The proposed game plan is depicted to be undermined if both of the going with two sorts of clients can satisfactorily interpret the figure content: 1) A client whose trademark set doesn't fulfill the get the chance to approach of relating figure content; 1) A customer who endeavors to get to the data before the predefined release time, paying little heed to whether he/she has satisfied trademark set. Passed on gathering affiliation has fundamental focal spotlights on both satisfying data sharing (Kren et al. 2017) and cost rot. Taking everything into account, this new perspective of data taking care of perceives new burdens about data protection security. Data is no longer in data owners trusted in space, and he/she can't trust in the cloud server to organize certify data find a good pace. Right now, guaranteed get to control issue has changed into a risky issue in streamed limit. There have been different courses of action with security sparing data participating in cloud subject to various cryptographic neighborhood individuals, in which the plans reliant on Cipher text policy ABE attract expansive contemplations, since they can guarantee data owner fine-grained and adaptable access control of his/her own Data. Regardless, these plans pick customer's direction advantage simply subject to his/her trademark Attributes with no other focal edges, for instance, the time factor. Believe it or not, the time thinks about when vulnerability recognizes a basic activity in controlling time fragile data (Bourne et al. 2017) (for instance to spread a latest electronic magazine, to reveal a connection's future field-endeavored methodology).

For the point of confinement of organized discharge, there is no utilization of an ensured area among and the data owner. Along these lines, the additional overhead is light weight . Cloud Service Provide By utilizing Drop Box The progression of conveyed figuring convinces attempts likewise, relationship to re-proper their data to outcast cloud authority centers(Ali et al. 2017) (CSPs), which will improve the limit requirement of advantage oblige close by devices. Beginning late, some business cloud limit associations, for example, the basic putting away association on-line information bolster associations of Amazon, Drop box Mazy, Bitcasa, and Memopal, are working for cloud application. There are some outcomes which may be invalid in some cases like disappointment or server equipment. To overcome security challenge of the present circulated stockpiling organizations, direct replication what's more, shows like Rabin's data dispersing plan are far from practical application. The formers are not practical because a progressing IDC(Karame et al. 2017) report prescribes that data age is outpacing limit availability. The later shows guarantee the accessibility of information right when a larger piece of stores, for example, k-out-of-n of normal information, is given. Regardless, they don't give insistences about the receptiveness of each vault, which will restrain the attestation that the shows can accommodate depending parties. For giving the dependability and accessibility of remote cloud store, two or three plans and their assortments have been proposed. In these courses of action, when an arrangement Underpins data modification we call it dynamic arrangement, for the most part static one (or limited special arrangement, if an arrangement could just beneficially reinforce some foreordained Action, for instance, attaches). In any case, the dynamic plans above focus on the circumstances where there is a data owner besides; the data can be easily changed by the data owner. Starting late, the improvement of conveyed figuring upheld a couple of uses. In these thing improvement (Ferreira et al. 2019) conditions, It will make monstrous correspondence and estimation overhead (Liu et al. 2016). To additionally redesign the past arrangement and care bunch customer disavowal, organized an arrangement reliant on go-between re-marks.

Chosen-Cipher text-Attack (CCA) Security Model: A secure one-time signature plot (G, register, and verify) supports the protected scheme. The special label is used to keep the figure material respectable. We can overhaul our CPA Secure deniable Cypher text policy- attribute dependent encryption strategy to be a secure deniable CCA cellular cipher with a comparative (Lang et al. 2018). We change the Following computations for this redesign

SetUpcca(1n) →(PP cca,MSK) for processing these algorithm we used Hash function H2 : {0,1}*→Gp3it randomly picks b€ZN these process attaches (g1,g3)bH2 to the public parameter is linked with the proposed algorithm PP cca .

Wireless Sensor Network: Internet of Things (IoT) envisions interoperability of heterogeneous devices to support diverse applications, and the Wireless Sensor Network (WSN) technology is an important building block of IoT sphere. Consideration of heterogeneity (e.g., energy, link and computational heterogeneities) [1] can improve the performance of WSN routing algorithms in terms of network lifetime, stability, reliability, network delay, etc. The energy heterogeneity in WSN routing is pursued widely; however, the link and computation

heterogeneities, which are generally used along with the energy heterogeneity, are relatively less explored areas. In the early work in WSN routing algorithms for energy heterogeneous scenarios, Stable Election Protocol (SEP) [2] considers two-level energy heterogeneity in Low-Energy Adaptive Clustering Hierarchy (LEACH) [3] like cluster-head (CH) role rotation environment. SEP proposes weighted election probabilities based on the initial energies of the nodes to give energy-rich nodes more chances of becoming CHs. The Distributed Energy-Efficient Clustering (DEEC) [4] considers multi-level energy heterogeneous WSN and prefers nodes with higher initial energy and residual energy for CH role The heterogeneity in terms of disparities in data generation rate (traffic) is considered under computation heterogeneity [5]. Sharma et al. [6] analyzed the effect of traffic heterogeneity in homogeneous WSN routing (LEACH) algorithm. Energy Dissipation Forecast and Clustering Management (EDFCM) [5] considers traffic heterogeneity along with energy heterogeneity in a very specific two-level WSN. Further, EDFCM considers additional nodes (management nodes) to control the number of clusters, which makes its natural distributed localized decision-making behavior questionable. The consideration of traffic heterogeneity along with energy heterogeneity is crucial for modeling realistic WSNs with application heterogeneity and event-driven scenarios. This letter considers both, energy and traffic heterogeneities, with multiple random levels. An energy model is presented for the multi-heterogeneity scenario, where consideration of multi-level traffic heterogeneity is a novel concept. A novel routing algorithm named Traffic and Energy Aware Routing (TEAR) is presented, which considers node's traffic requirements along with its energy levels while making CH selection. TEAR shows improvements in terms of stability period (reliable lifespan of the WSN before the death of its first node) over existing algorithms (LEACH, SEP and DEEC) under the scenario. The rest of this letter is arranged as follows. Section II presents the system model, which includes the energy model for the multi-heterogeneous scenario. In Section III, the proposed routing algorithm is described. The simulation results have been disc Effective monitoring of network performance is essential for network operators in building reliable communication networks that are robust to service disruptions. In order to achieve this goal, the monitoring infrastructure must be able to detect network misbehaviors (e.g., unusually high loss/latency, un reach ability) and localize the sources of the anomaly (e.g.,malfunction of certain routers) in an accurate and timely manner. Knowledge of where problematic network elements reside Research was sponsored by the U.S. Army Research Laboratory and the U.K. Ministry of Defence and was accomplished under Agreement Number W911NF-06-3-0001. The views and conclusions contained in this document are those of the authors and should not be interpreted as representing the official policies, either expressed or implied, of the U.S. Army Research Laboratory, the U.S. Government, the U.K. Ministry of Defence or the U.K. Government. The U.S. and U.K. Governments are authorized to reproduce and distribute reprints for Government purposes notwithstanding any copyright notation hereon. in the network is particularly useful for fast service recovery, e.g., the network operator can migrate affected services and/or reroute traffic. However, localizing network elements that cause a service disruption can be challenging. The straightforward approach of directly monitoring the health of individual elements is not always feasible due to traffic overhead, access control, or lack of protocol support at internal nodes. Moreover, built-in monitoring agents running on network elements cannot detect problems

caused by misconfigured/unanticipated interactions between network layers, where end-to-end communication is disrupted but individual network elements along the path remain functional (a.k.a. silent failures) [1]. These limitations call for a different approach that can diagnose the health of network elements from the health of end-to-end communications perceived between measurement points. One such approach, generally known as network tomography [2], focuses on inferring internal network characteristics based on end-to-end performance measurements from a subset of nodes with monitoring capabilities, referred to as monitors. Unlike direct measurement, network tomography only relies on end-to-end performance (e.g., path connectivity) experienced by data packets, thus addressing issues such as overhead, lack of protocol support, and silent failures. In cases where the network characteristic of interest is binary (e.g.,normal or failed), this approach is known as Boolean networktomography [3].In this paper, we study an application of Boolean network tomography to localize node failures from measurements of path states1. Under the assumption that a measurement path isnormal if and only if all nodes on this path behave normally, we formulate the problem as a system of Boolean equations, where the unknown variables are the binary node states, and the known constants are the observed states of measurement paths. The goal of Boolean network tomography is essentially to solve this system of Boolean equations.Because the observations are coarse-grained (path normal/failed), it is usually impossible to uniquely identify node states from path measurements. For example, if two nodes always appear together in measurement paths, then upon observing failures of all these paths, we can at most deduce that one of these nodes (or both) has failed but This model can also capture link failures by transforming the topology into a logical topology with each link represented by a virtual node connected to the nodes incident to the link. This model can also capture link failures by transforming the topology into a logical topology with each link represented by a virtual node connected to the nodes incident to the link. cannot determine which one. Because there are often multiple explanations for given path failures, existing work mostly focuses on finding the minimum set of failed nodes that most probably involves failed nodes. Such an approach, however, does not guarantee that nodes in this minimum set havefailed or that nodes outside the set have not. Generally, to distinguish between two possible failure sets, there must exist a measurement path that traverses one and only one of these two sets. There is, however, a lack of understanding of what this requires in terms of observable network properties such as topology, monitor placement, and measurement routing. On the other hand, even if there exists ambiguity in failure localization across the entire network, it is still possible to uniquely localize node failures in a specific sub-network (e.g., sub-network with a large fraction of monitors). To determine such unique failure localization in sub-networks, we need to understand how it is related to network properties. In this paper, we consider three closely related problems: Let S denote a set of nodes of interest (i.e., there can be ambiguity in determining the states of nodes outside S; however, the states of nodes in S must be uniquely determinable). (1) If the number of simultaneous node failures is bounded by k, then under what conditions can one uniquely localize failed nodes in S from path measurements available in the entire network? (2) What is the maximum number of simultaneous node failures (i.e., the largest value of k) such that any failures within S can be uniquely localized? (3) What is the largest node set within which failures can be uniquely localized, if the total number of failures is bounded by

k? Answers to questions (2) and (3) together quantify a network's capability to localize failures from end-to-end measurements: question (2) characterizes the scale of failures and question (3) the scope of localization. Clearly, answers to the above questions depend on which paths are measurable, which in turn depends on network topology, placement of monitors, and the routing mechanism of probes. We will study all these problems in the context of the following classes of probing mechanisms: (i) Controllable Arbitrary-path Probing (CAP), where any measurement path can be set up by monitors, (ii) Controllable Simple-path Probing (CSP), where any measurement path can be set up, provided it is cycle-free, and (iii) Uncontrollable Probing (UP), where measurement paths are determined by the default routing protocol.

VIRTUAL DESTINATION BASED TECHNIQUE: Virtual Destination based Technique Exploit of Virtual destinations in void-handling Techniques is a new approach has been introducing in this research. According to this proposed algorithm advantages of greedy forwarding can be exploited to direct data packets even in dealing with voids by specifying one or more temporary destination, whereas during the other void handling techniques the advantage of greedy forwarding cannot be achieved. POR algorithm is an effective and efficient technique in this group. a novel Robust Geographic Routing protocol (RGR) is proposed, in which several sub-optimal forwarders cache the packet that has been received using MAC interception. If the best forwarder does not forward the packet in certain time slots, sub-optimal candidates will take turn to forward the packet according to a locally formed order. In this way, as long as one of the candidates succeeds in receiving the packet, the data transmission will not be interrupted, leading to RGR's excellent robustness. Here we do not use the unexpectedly far links as in opportunistic routing since our focus is not on the throughput improvement. On the other hand, a Virtual Destination based Void Handling (VDVH) scheme is also proposed to work together with RGR. In VDVH, the packet is forwarded towards a virtual destination which has a certain degree of offset compared to the real destination. However to the usage of virtual destination, the advantage of greedy forwarding (e.g. large progress per hop) and opportunistic forwarding can still be achieved while handling communication voids. receiver based routing decision, all neighbor nodes located in the forwarding area [8] will calculate their own priority, except for the last hop (if the destination is found within the one hop neighborhood, a one-hop label in the packet header will be set positive thus suppressing all other nodes' forwarding as the destination will not relay the packet). A node located in the forwarding area, satisfies the following two conditions: i) it makes positive progress towards the destination; ii) it is in the transmission range of the next hop node which is selected by the previous hop. The forwarding area is illustrated in Fig. 1(a) where Node S is the sender and Node A is the selected next hop by Node S. Node A

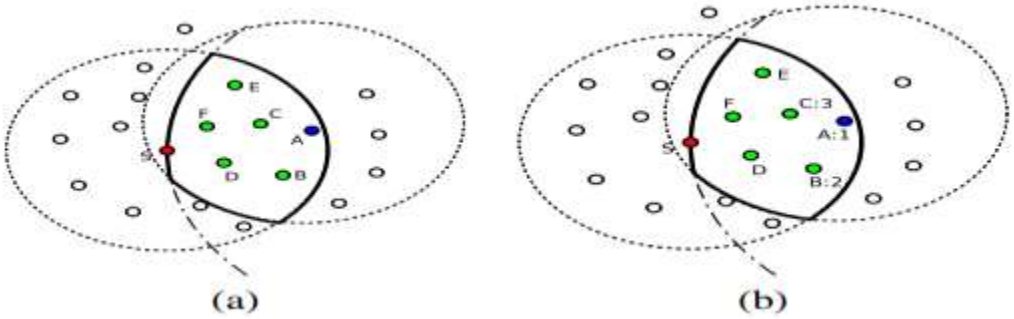


Fig.1 (a) The forwarding area of RGR (Node A is the best forwarder selected by previous hop Node S). (b) The priority from Node C's perspective

gets the first priority to forward the packet without any doubt while Nodes B – F have to determine their own priority. Algorithm 1 shows the receiver based priority decision in which R is a node's transmission range, and NA, NP , NN , ND mean current node, the previous hop, the next hop and the destination, respectively. For instance in Fig. 1(b), Node C will find its priority (at 3) is lower than Nodes A (at 1) and B (at 2). To reduce buffer consumption and potential duplicate relay, a maximum priority is defined. If a node's priority exceeds that value (5 in our simulation), it will discard the received packet and give up participating in the relay.

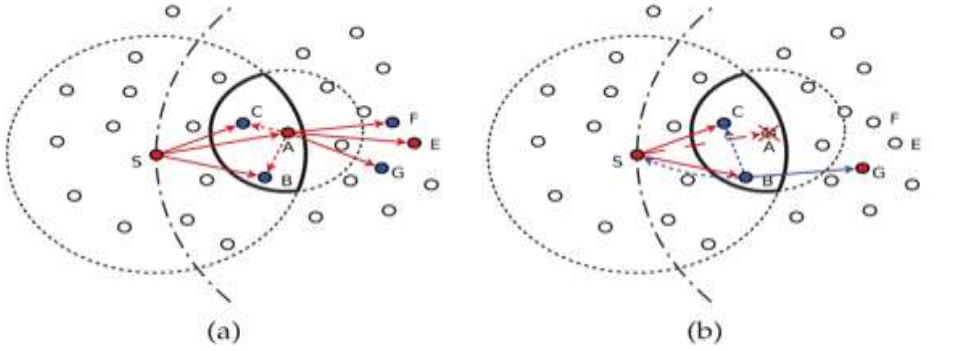
Algorithm GetPriority

```
ListA : List of all neighbors of N_A
if N_A == N_N then
  priority ← 1
else if dist(N_A, N_D) ≥ dist(N_P, N_D) then
  priority ← 0
else if find(ListA, N_N) == false then
  priority ← 0
else
  priority ← 2
  for i ← 1 to length(ListA) do
    if ListA[i]! = N_N && dist(ListA[i], N_P) ≤
    R && dist(N_A, N_D) − dist(ListA[i], N_D) > Δd
    then
      priority++
    end if
  end for
  if priority > MAX_PRIORITY then
    priority ← 0
  end if
end if
return priority
```

In above Algorithm, current node will increase its priority not only if one of its neighbor's progress is larger, but also the difference should exceed a certain threshold Δd. In real networks, it is almost impossible for a node to get the accurate location of every neighbor all the time. Such asynchronization in location would lead to confusion in determining the forwarding priority. For instance, two nodes may both think they have higher or lower priority than the other when their distance to the destination is very near, thus leading to collision caused by simultaneous forwarding or simultaneous waiting resulting in unnecessary delay. In order to make RGR robust to such inaccuracy in nodes' location, the threshold Δd is introduced. As illustrated in Figure, both Nodes

C and E are of the same priority since their location difference is within threshold Δd. In addition, to reduce the collision caused by possible simultaneous transmissions, some jitter is added before suboptimal forwarders start relaying the packet

Below architecture diagram represents mainly flow of requests between clients and server/monitoring nodes. In this scenario overall system is designed in two tires separately. For two layers called presentation layer using java swings, business logic layers using java sources This project was developed using 2-tire architecture without the need for repository. In this scenario nodes are validated by a server in order to join network.



(a) The operation of POR in normal situation.
(b) The operation of POR when the next hop fails to receive the packet.

Fig2: Operation of POR

VIRTUAL DESTINATION BASED VOID HANDLING: In order to enhance the robustness of RGR in the network where nodes are not uniformly distributed and large holes may exist, a complementary void handling mechanism based on virtual destination is proposed.

Trigger Node:

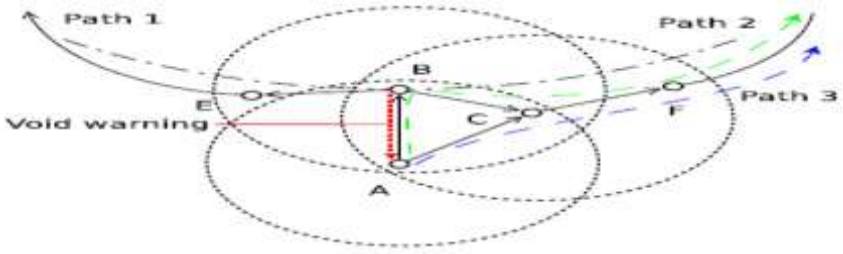


Fig.3 Potential paths around the void

The first question is at which node should packet forwarding switch from greedy mode to void handling mode. In many existing geographic routing protocols, the mode change happens at the void node, e.g. Node B in Fig. . Then Path 1 (AB- E-・ ・ ・) and (or) Path 2 (A-B-C-F-・ ・ ・) (in some cases only Path 1 is available if Node C is outside Node B's transmission range) can be used to route around the communication hole. From Fig.

4, it is obvious that Path 3 (A-C-F-・ ・ ・) is better than Path 2. If the mode switch is done at Node A, Path 3 will be tried instead of Path 2 while Path 1 still gets the chance to be used. A message called void warning, which is actually the data packet returned from Node B to Node A with some flag set in the packet header, is introduced to trigger the void handling mode. As soon as the void warning is received, Node A (referred as trigger node) will switch the packet delivery from greedy mode to void handling mode and re-choose better next hops to forward the packet. Of course if the void node happens to be the source node, packet forwarding mode will be set as void handling at that node without other choice (i.e. in this case the source node is the trigger node).

Virtual Destination To handle communication voids, almost all existing mechanisms try to find a route around. During the void handling process, the advantage of greedy forwarding cannot be achieved as the path that is used to go around the obstacle is usually not optimal (e.g. with much more hops compared with the possible optimal path). More importantly, the robustness of multicast-style routing cannot be exploited. In order to enable opportunistic forwarding in void handling, which means even in dealing with voids, we can still transmit the packet in an opportunistic routing like fashion, virtual destination is introduced, as the temporary target that the packets are forwarded to.

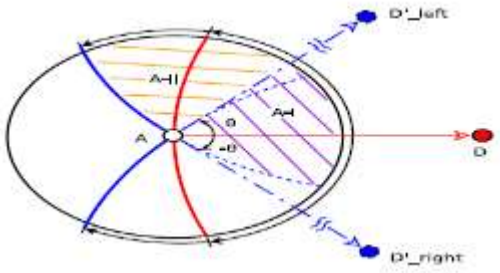


Fig.4 Potential forwarding area is extended with virtual destination

Virtual destinations are located at the circumference with the trigger node as center, but the radius of the circle is set as a value that is large enough (e.g. the network diameter). They are used to guide the direction of packet delivery during void handling. Compared with the real destination, virtual destination has a certain degree of offset}θ (π/4 in our simulation) in Figure. With the help of virtual destination, the potential forwarding area is significantly extended. Strictly speaking, our mechanism cannot handle all kinds of communication voids, since not all the neighbors of the current node are covered. However, for most situations it is effective.For those communication holes with very strange shape, a reposition scheme has been proposed [9] to smooth the edge of the hole. So with the work that has been done in [9], VDVH still has the potential to deal with all communication voids.

Path Acknowledgement and Reverse Suppression: In VDVH, if a trigger node finds that there are forwarding candidates in both directions, the data flow will be split into two where the two directions will be tried

simultaneously for a possible route around the communication void. In order to reduce unnecessary duplication, two control messages are introduced, namely, path acknowledgement and reverse suppression. If a forwarding candidate receives a packet that is being delivered or has been delivered in void handling mode, it will record a reverse entry. Once the packet reaches the destination, a path acknowledgement will be replied to inform the trigger node along the reverse path. Then the trigger node will give up trying the other direction. For the same flow, the path acknowledgement will be periodically replied (not on perpacket base, otherwise too many control messages). If there is another trigger node upstream, the path acknowledgement will be further delivered to that node, and so on. On the other hand, if a packet that is forwarded in void handling mode reaches a certain place and it cannot go any further or the number of hops traversed exceeds a certain threshold but it is still being delivered in void handling mode, the packet will be returned back to the trigger node with some flag set in the packet header indicating that it is a reverse suppression message. Once the trigger node receives the packet, it will stop trying that direction. The packet will be discarded if the other direction is still working, otherwise it will be buffered for future forwarding opportunity.

MANET Setup: The goal of our simulation experiments is to assess the impact of different aspects of realistic mobility scenarios on the ability of the MANET routing protocols to successfully deliver data packets. We base our performance comparison on the packet delivery ratio achieved by all the systems even in case of node mobility.

Neighbor Table Generation : A node constructs its neighbor table without extra signaling. When receiving a beacon from a neighbor, a node records the node ID, position and flag contained in the message in its neighbor table. To avoid routing failure due to outdated topology information, an entry will be removed if not refreshed within a period Timeout NT or the corresponding neighbor is detected unreachable.

Forwarding Nodes Selection(for N=0,1,2)(Candidate Selection Algorithm)

When a data packet is sent out, some of the neighbor nodes that have overheard the transmission will serve as forwarding candidates, and take turn to forward the packet if it is not relayed by the specific best forwarder within a certain period of time. By utilizing such in-the-air backup, communication is maintained without being interrupted. The additional latency incurred by local route recovery is greatly reduced and the duplicate relaying caused by packet reroute is also decreased.

Node Mobility Updates using VDVH: In VDVH, if a trigger node finds that there are forwarding candidates in both directions, the data flow will be split into two where the two directions will be tried simultaneously for a possible route around the communication void. In order to reduce unnecessary duplication, two control messages are introduced, namely, path acknowledgment and reverse suppression. Also if a node mobile all the neighbors are initiated with updates about the new possible location specifics thus always maintaining an updated neighbor table.

Input Configurations (Number of Nodes, Locations, Battery power, Existing or Proposed, Source , Destination, Message)The user interface construction that seeks input parameters required for simulation setup. The input parameters might range from Number of Nodes, Locations, Battery power, Existing or Proposed, Source ,

Destination, Message, Console Messages and Log messages before and after transmissions etc. Results based on(Arrival Rate, End to End Delay, Collisions, Communication Over Head, Energy Consumption) The console log to validate the authenticity of the transmission operations performed for both existing(DSDV) and proposed(POR) systems. Even though time factor is not displayed it can be intuitively felt by the simulation user for both existing and proposed systems.

RESULTS:

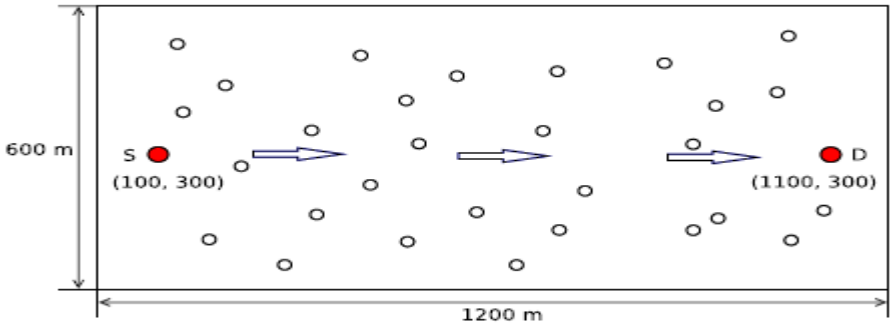


Fig. Network topology: uniformly distributed

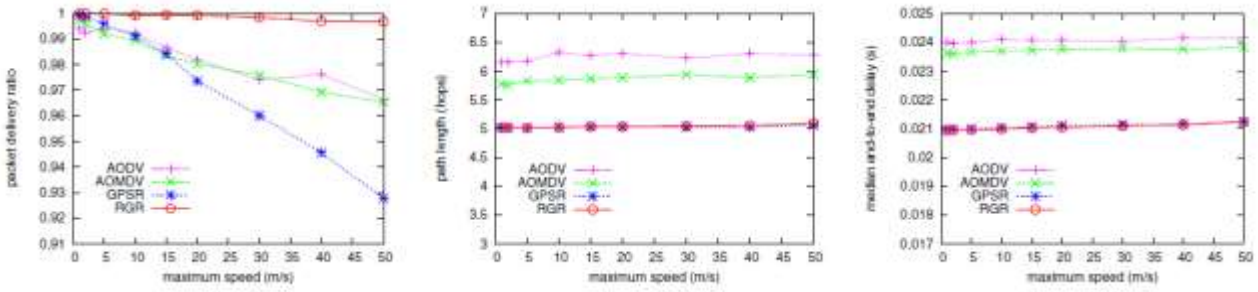


Fig. a) Packet delivery ratio b)Path length c) Median end-to-end delay

```
mysql> select * from request;
+----+-----------+----------+-------------+-----------+------------+
| id | user      | owner    | fname       | secretkey | contentkey |
+----+-----------+----------+-------------+-----------+------------+
|  1 | Rajesh    | Sukumar  | Dengue.txt  | Permitted | Permitted  |
|  2 | tmksmanju | Manjunath| Malaria.txt | Permitted | Permitted  |
|  3 | tmksmanju | Sukumar  | Dengue.txt  | Permitted | Permitted  |
+----+-----------+----------+-------------+-----------+------------+
3 rows in set (0.00 sec)
```

Fig: The select Query on request table

Download File:-

The user can download the file by passing attribute like File Name after that user should have to click on request keys button the remaining attributes automatically appends on the text boxes after clicked on download button user can get the data. The data is automatically decrypted from the server side which is initially in a plain text.

If any key miss match found while downloading data its treated as the attacker, attacked on your secure data it's not downloads any case so the process of getting fake and genuine users done .

The above screen key miss match found we removed few characters from the appended keys then our system treated as Key management.

Master secret key response:-

The generated key from cloud server, stored on the database while user searching files and matches found the Master secret keys are displayed on the web page

The generated keys along with the filenames are shown in below table.

```
mysql> select secretkey,fname,contentkey from ownerfiles;
+-------------+-------------+--------------------+
| secretkey   | fname       | contentkey         |
+-------------+-------------+--------------------+
| [B@d7b7d9   | Dengue.txt  | s119x0vf0k3q3p2k   |
| [B@11415c8  | Cancer.txt  | q189t4u13u0o4o81   |
| No          | Maleria     | Requested          |
+-------------+-------------+--------------------+
3 rows in set (0.00 sec)
```

Fig: Displayed keys along with Keys

Conclusion: This process presents a robust geographic routing protocol and a novel virtual destination based void handling scheme that can work well with opportunistic forwarding. The simulation results justify RGR's robustness to node mobility and VDVH's effectiveness and efficiency. To evaluate the performance of RGR, It

simulate the algorithm with AODV, AOMDV and GPSR. The mobile nodes are equipped with 802.11 Wave LAN radios, with a nominal range of 250 m. Many momre network topologies have been simulated: i) nodes are uniformly distributed in a rectangle with random way point mobility model; ii) nodes are manually arranged to form a communication hole. Packet delivery ratio, average path length and median end-to-end delay are taken as the performance metrics.

Bibliography:-

1. Singh, R.S., Prasad, A., Moven, R.M., Sarma, H.K.D. (2017) 'Denial of service attack in wireless data network: A survey', in 2017 Devices for Integrated Circuit (DevIC), IEEE, 354–359.
2. Wan, Z., Liu, J., Deng, R.H. (2011) 'HASBE: A hierarchical attribute- based solution for flexible and scalable access control in cloud computing', IEEE transactions on information forensics and security, 7(2), 743–754.
3. Wang, C., Ren, K., Wang, J. (2011) 'Secure and practical outsourcing of linear programming in cloud computing', in 2011 Proceedings Ieee Infocom, IEEE, 820–828.
4. Wang, C., Zhang, B., Ren, K., Roveda, J.M. (2013) 'Privacy-assured outsourcing of image reconstruction service in cloud', IEEE Transactions on Emerging Topics in Computing, 1(1), 166–177.
5. Wang, Y., Wu, Q., Qin, B., Shi, W., Deng, R.H., Hu, J. (2016) 'Identity- based data outsourcing with comprehensive auditing in clouds', IEEE transactions on information forensics and security, 12(4), 940–952.
6. Wu, Y., Wei, Z., Deng, R.H. (2013) 'Attribute-based access to scalable media in cloud-assisted content sharing networks', IEEE Transactions on Multimedia, 15(4), 778–788.
7. Xue, K., Hong, P. (2014) 'A dynamic secure group sharing framework in public cloud computing', IEEE Transactions on Cloud Computing, 2(4), 459–470.
8. Xue, K., Li, S., Hong, J., Xue, Y., Yu, N., Hong, P. (2017) 'Two-Cloud Secure Database for Numeric-Related SQL Range Queries With Privacy Preserving', IEEE Transactions on Information Forensics and Security, 12(7), 1596–1608.
9. Xue, Y., Hong, J., Li, W., Xue, K., Hong, P. (2016a) 'LABAC: A location-aware attribute-based access control scheme for cloud storage', in 2016 IEEE Global Communications Conference (GLOBECOM), IEEE, 1–6.
10. Xue, Y., Hong, J., Li, W., Xue, K., Hong, P. (2016b) 'LABAC: A Location-Aware Attribute-Based Access Control Scheme for Cloud Storage', in 2016 IEEE Global Communications Conference (GLOBECOM), Presented at the 2016 IEEE Global Communications Conference (GLOBECOM), 1–6.
11. Yan, H., Li, J., Han, J., Zhang, Y. (2016) 'A novel efficient remote data possession checking protocol in cloud storage', IEEE Transactions on Information Forensics and Security, 12(1), 78–88.
12. Yan, H., Li, J., Han, J., Zhang, Y. (2017) 'A Novel Efficient Remote Data Possession Checking Protocol in Cloud Storage', IEEE Transactions on Information Forensics and Security, 12(1), 78–88.

13. Yang, K., Jia, X., Ren, K., Zhang, B., Xie, R. (2013) 'DAC-MACS: Effective data access control for multiauthority cloud storage systems', IEEE Transactions on Information Forensics and Security, 8(11), 1790–1801.
14. Yang, Y., Chen, X., Chen, H., Du, X. (2018) 'Improving privacy and security in decentralizing multi-authority attribute-based encryption in cloud computing', IEEE Access, 6, 18009–18021.
15. Yuan, H., Bi, J., Zhou, M. (2018) 'Temporal Task Scheduling of Multiple Delay-Constrained Applications in Green Hybrid Cloud', IEEE Transactions on Services Computing, 1–1.
16. Yuan, K., Liu, Z., Jia, C., Yang, J., Lv, S. (2013) 'Public key timed- release searchable encryption', in 2013 Fourth International Conference on Emerging Intelligent Data and Web Technologies, IEEE, 241–248.
17. Zhou, Z., Zhang, H., Zhang, Q., Xu, Y., Li, P. (2014) 'Privacy-preserving granular data retrieval indexes for outsourced cloud data', in 2014 IEEE Global Communications Conference, Presented at the 2014 IEEE Global Communications Conference, 601–606.
18. Zhu, Y., Hu, H., Ahn, G.-J., Yu, M. (2012) 'Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage', IEEE Transactions on Parallel and Distributed Systems, 23(12), 2231–2244.