Secure Neighbour Discovery: Secure k-Nearest ROUTING AD-HOC Networking Using Diffie-Helman and HIGHEST Connectivity Algorithm

Dhanabal S[1], Prasanna Venkatesan G. K. D[2], and Amudhavalli P[3]
[1] Research Scholar, Department of Computer science Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
[2] Research Supervisor, Dean-Faculty of Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
[3] Associate professor, Department of Computer science Engineering, Karpagam Academy of Higher Education, Coimbatore, Tamil Nadu, India
Email: nkldhanapal@gmail.com, prasphd@gmail.com, amudhapadmanabhan@gmail.com

Abstract —The approach of splendid flexible contraptions and zone-based applications, and customers' movability configuration are seen to be exceedingly dependent on moving zones. Proficiency and effortlessness of irregular algorithms have made transfer of data a lucrative option for taking care of complex issues in the space of correspondence systems. Achieving efficiency with the mobility of wireless communication is tedious. To deal with this, the data are sent through the chosen nodes. The data are forwarded to a destination via the primary path from source. Remote framework organizations rely highly on a basic structure for neighborhood discovery (ND). Neighborhood Discovery (ND) is the disclosure of gadgets specifically reachable for correspondence or in physical nearness, which becomes a key necessity and building obstruct for different data transfer applications. A completely conveyed and agreeable arrangement that is powerful against free and plotting foes can be weakened just by a staggering nearness of enemies and distributed solution for (Neighbor Position Verification) NPV, which permits any hub in a portable unplanned system to confirm the situation of its correspondence neighbors without considering the prior reliable nodes. Deffie-Hellman (DH) algorithm and HCS clustering algorithm have been implemented to make safe transmission between nodes and receiving nodes or clients without any traffic or data loss. The data are passed to destination by using grid topology. Our comparison of the proposed system with existing systems demonstrates that our convention is exceptionally strong concerning communication cost, energy, average delay, accessing of data and PDR.

Index Terms—Secure ND, Network communication, DH algorithm, Clustering algorithm, HCS algorithm

I. INTRODUCTION

Over the earlier decade, remote portable correspondence advancements have developed and been broadly embraced [11]. The quantity of cellular phone now surpasses by an extended shot that of wired telephones; a large number of roaming clients routinely interface with the remote neighborhood (WLANs); and remote gadgets are typical in homes, industrial services and healing centers [2]. In the meantime, the developing portable appointed and organizing ideal models introduce another sort of system: gadgets frame multihop topologies in a self-arranging way, transferring bundles from different gadgets over various remote connections (jumps), and basically turn into the system. A few applications are empowered as of now by these advancements or expected sooner rather than afterward. Remote sensor systems are one among them that is used in various fields. Versatile specially appointed systems are utilized as a division of debacle help tasks, with "came in" base stations and compact radios, and in addition in strategic activities with a huge number of vehicles, flying machines or faculty borne remote gadgets. Static impromptu or work systems are being shaped by home PCs with housetop receiving wires. Low-versatility impromptu systems will empower (frequently delay- tolerant) correspondence in urban conditions; illustrations incorporate systems of handheld gadgets, wearable gadgets, and radio recurrence identifiers (RFIDs). The gadget portability and unpredictability of remote correspondence, regularly crosswise over radio recurrence channels, result in associations that are, much of the time, built up and torn down without earlier notice. The test here is to find neighbors that, contingent upon the upheld application, can be:

- Devices straightforwardly reachable for correspondence (i.e., correspondence neighbors)
- Devices in nearness (i.e., physical neighbors)

Regularly, it is accepted that if two hubs can impart specifically, they are inside each other's correspondence range. Vicinity and correspondence, notwithstanding, are not generally related. Conventions for neighborhood revelation (ND) fill in as major building hinders in versatile remote frameworks. Securing ND is a difficult issue, in any case. A striking illustration is that of overcoming a distinguished companion or adversary

Manuscript received June 20, 2018; revised February 21, 2019.
doi:10.12720/jcm.14.3.164-169

framework [1]. Our system demonstrates that the security of ND remains an open issue to a greater extent, in spite of different existing propositions. We finish up by recommending the formal examination of ND conventions as the subsequent stage on a guide towards promising secure neighborhood revelation.

II. Related Work

Various secure neighbor disclosure plans have been proposed. We quickly review plots that are not for the most part appropriate to WSN, due to their extraordinary equipment prerequisites or dependence on extra infrastructure [3]. The present scheme of an impromptu system where hubs communicate with random source-destination pairs is used [14].

For the issue sending information securely, two components that (i) recognize acting up hubs and report such occasions and (ii) keep up an arrangement of measurements mirroring the past conduct of different hubs [7] have been proposed to ease the adverse impacts of parcel dropping. Every hub may pick the 'best' suitable route that generally contains the good capacity nodes; i.e., nodes that don't have history of abstaining from sending bundles along the confirmed route. Among the conclusion the previously mentioned work are a mutual medium, that has bi-directional connections, and uses source routing (i.e., the intermediate nodes that knows the details of packets are carried through the route), and there is no suspicious nodes. [7]

III. Types of Neighborhood

Devices in the existing remote and forthcoming versatile impromptu systems are different in their qualities and usefulness. To present the recent issue, we put away various unique points of interest and consider framework substances as non-specific hubs. Every hub has a one of a kind character, a handling unit and a remote handset. Hubs impart over the remote medium in view of the condition of the medium and the capacities of their handsets. [2] We don't harp on the handset attributes unless required. Predominantly, past specialized attributes of the collector (e.g., their affectability), parameters and elements that decide the capacity to impart include:

- The energy of the transmitted flag
- The separation between the transmitting and (Planned) accepting hubs
- The proportion of control over that of commotion and meddling signs
- Impairments of the remote medium (e.g., blurring or dispersing) [2].

The remote sensors are sent haphazardly in the system with a known thickness, which covers various situations going from combat zone reconnaissance to perception of risky conditions. We expect that the sensor that is sent is of a substantial scale and the sensor areas take over an irregular Poisson point process, bringing about a uniform hub organization. Every sensor node *i* decides its position (xi,yi) in a two-dimensional Euclidean coordinate framework through a (non-secure) confinement technique [6].

IV. The Proposed Methodology

In proposed system flat grid topology and three algorithms Diffie-Helman algorithm, Highest Connectivity algorithm and cluster change algorithm is implemented. In our network data from one client to another client can be transferred. The four steps for transferring are as follows.

A. Route Request

The source node *S* keeps up a Query Sequence number *Qseq* for every receiver it safely conveys with. This 32-bit succession number increments invariably, for every route request produced by S, and enables T to recognize obsolete request for route. by using HCC algorithm. The arrangement number is introduced at the foundation of the *SA* and in the face of the fact that it isn't permitted to fold over, it gives roughly a space of four billion question demands for every destination. [7]

B. Route Reply

T approves the received route packet that has been requested, by first confirming that it has started from a hub with which it has a security authority. After this, comparision between *Qseq* with *Smax* is done and the majority extreme query sequence number got from *S*, inside the lifetime of the *SA*. The demand is disposed of as obsolete or replayed if *Qseq* *Smax*. If not, *T* computes the keyed hash of the demand fields. If the outcome coordinates the SRP header MAC, the uprightness of this demand is confirmed, alongside the validness of its origin [7].

C. Intermediate Node Replies

The storing of caught routes is a serious defenselessness, since false topology data can be effectively dispersed all through a substantial constituent of the system by using Cluster change algorithm. A malignant hub can create information bundles or route answers, which are, for instance, stored by hubs orking in wanton mode.[7]

D. Link Score and Information Receive

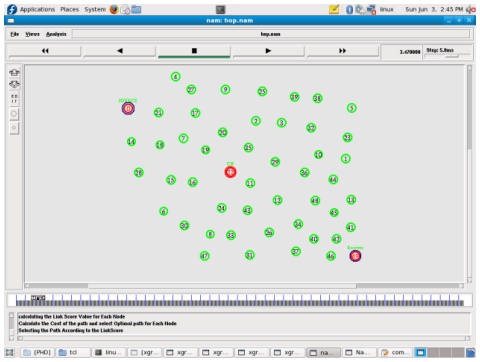

Fig. 1. Assigning the source and destination with Center Node used as flat grid topology

In Fig. 1 Node 0 is the source and Node 49 the goal. Connection Score is a review for each system figured by its flag quality, channel power and the number of systems vying for broadcast appointment. Subsequently the connection score has is ascertained for every node. After determine the connection score, the cost of the route and ideal way for Each node is selected and the Receiver node gets the information.

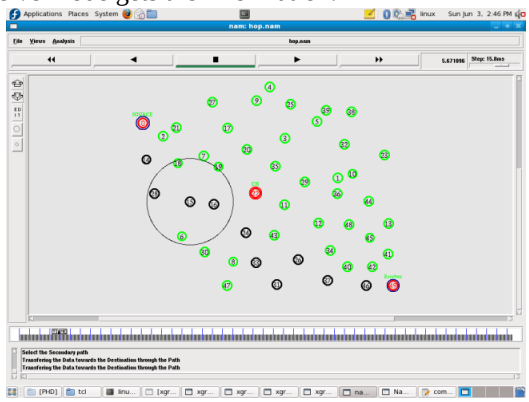

Fig. 2. Selecting the path and selecting the intermediate nodes

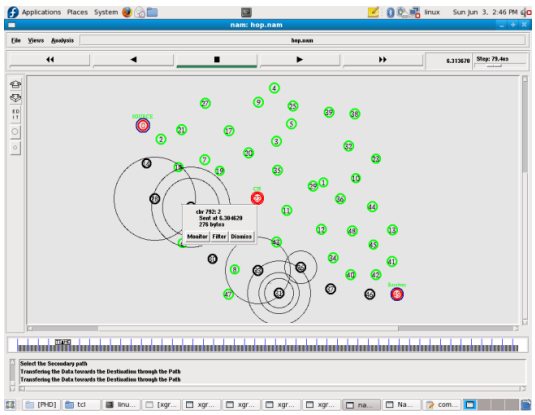

Fig. 3. Clustering and data forwarding

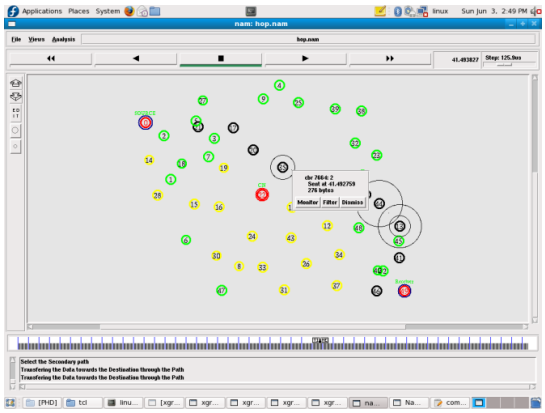

Fig. 4. Alternative route selection

V. Algorithm

A. To Find the Best Routing Path Using Deffie-Hellman (DH) Algorithm

Diffie-Hellman is a method for creating a mutual mystery between two individuals so that the mystery can't be seen by watching the correspondence. That is an imperative refinement. The data is not shared amid the key trade, instead of making a key together.

Step 1: Consider the two prime numbers a and b.

Step 2: Then a mystery number (x) is picked, which isn't uncovered. Rather a^x *mod* b is processed and the result sent back. (This is declared as X since it came from x).

Step 3: The equivalent thing is repeated, but now the secret number is y and the computed number Y. So compute a^b *mod* b and send the result (called "Y")

Step 4: Now, take the number that is sent and do exactly the same operation with *it*. So that's Y^a *mod* b.

Step 5: Do the same operation with the result, so: X^b *mod* b.

Formula:

$$(a^x \bmod b)^y \bmod b = a^{xy} \bmod b$$

$$(a^y \bmod b)^x \bmod b = a^{yx} \bmod b$$

B. To Generate Energy Level by Using Highly Connected Subgraphs (HCS) Algorithm

The HCS (Highly Connected Subgraphs) clustering algorithm is a calculation in light of graph network for Cluster examination, by first speaking to the related information in a similarity graph, and a while later discovering all the very associated sub graphs as clusters.

The more edges exist for a given amount of vertices, the more comparable such an arrangement of vertices is among one another in the similarity graph. In another word, on the off chance that we attempt to detach a similarity graph by evacuating edges, the more edges we have to expel before the graph ends up disengaged, the more comparative the vertices in this graph. Minimum cut is a base arrangement of edges without which the diagram will wind up detached.

On chart hypothesis, a least cut of a diagram (graph) is a cut that is insignificant in some sense.

HCS algorithm discovers all the sub graphs with x vertices to such an extent that the base cut of those sub graphs contains more than x/2 edges, and distinguishes them as groups. Such a sub graph is known as a Highly Connected Subgraph (HCS).

By considering the similarity graph R(S,T), HCS grouping calculation will check on the off chance that it is now exceedingly associated, if yes, returns R, generally utilizes the base slice of R to segment R into two sub graphs H and H', and recursively run HCS bunching calculation on H and H'.

Pseudo code

```
function HCS(R(S,T))
  if R is highly connected then return (R)
else
    (H1,H3,C) ←MINIMUMCUT(R)
    HCS(H1)
   HCS(H2)
```

End if
End

C. To Perform Energy Level and Packet Delivery Using Clustering Algorithm

Step 1: The total distance enclosed by a node during final n seconds is

$$Dt = \sum_{i=t-n}^{i=t} Dist_i$$ where $i=t$ is the present time

Compute the normal speed of a node as $Sv=Dt/n$.

Step 2: Register Mobility factor $\Delta M=\delta-Sv$. That is themeans by which far is the normal speed of the hub from the greatest allowable speed δ of the system.

Step 3: Compute accessible battery control as Pav = Pav - Pcons where

Pav = Available battery energy of the hub (Initially it is the most extreme battery control). Pcons = Battery control devoured by the hub.

Step 4: Compute the heaviness of hub as wv = x1 ΔM+ x2 Pav

Where x1 and x2 are the weight factors, once the weights of the hubs are ascertained then the calculation works.

Algorithm Steps

For (every v €V)
If wv>wi where i €*T (v) // T(v)* is the neighbor set of v
Then Set source= v
For (every x €Vuncoverd)
If dist (source, x) <= destination range
Then
Set source x = destination
End for
End for

VI. Simulation Results and Discussion

The output of our system has implemented in the Network Simulator tool under the version (Ns2.35) for saving energy level and secure transmission of the information starting from sender to receiver.

TABLE I: CORRELATIONS WITH EXISTING AND PROPOSED

Methodology	Communication cost		Energy		Avg Delay		Data Access		PDR (packet delivery ratio)	
	High	Low	High	Low	High	Low	High	Low	High	Low
Existing (Message Exchange Protocol)	5	4	100	90	11	10	600	500	0.7	0.3
Proposed (DH and HCC algorithm and cluster change algorithm)	0.5	0.4	38	18	1	0	900	810	1.3	0.5

Correlation of existing framework and proposed framework is classified as far as it focuses on considering communication cost, Average delay, Energy, Data access and Packet Delivery Ratio (PDR). By this, it can be seen that the proposed framework is superior in all terms. Correspondence cost, Energy utilized and the delay in the framework have been lessened. Information can be sent effectively with this benefits of the proposed system.

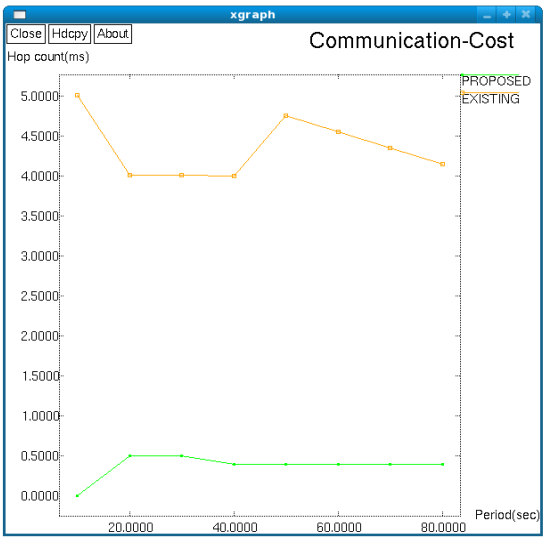

Fig. 5. Comparison with communication cost. [x axis=Hop Count(ms) and Y axis=Period(seconds)]

In Fig. 5 to Fig. 9, the comparison of existing and proposed diagrams in light of communication cost and energy, delay and information availability is shown. All of the comparision graph is generated by using the Ns2

Scripting language for comparing the existing and proposed system in terms of Fig. 5 to Fig. 9.

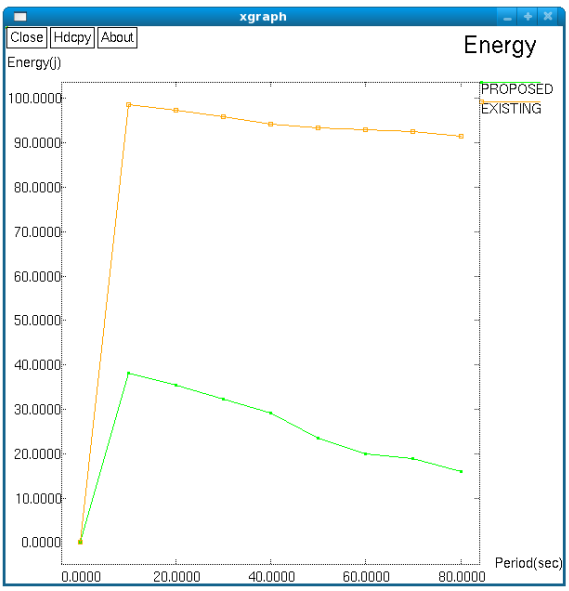

Fig. 6. Comparison with Energy Level. [x axis=Energy (j) and Y axis=Period(seconds)]

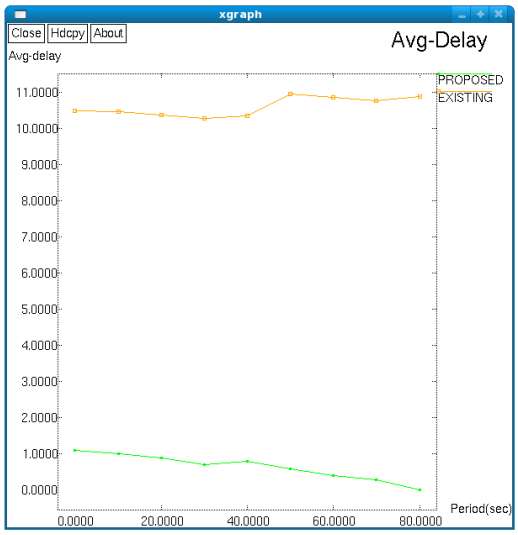

Fig. 7. Comparison with Avg-Delay for the existing and proposed system. [x axis=Average delay and Y axis=Period(seconds)]

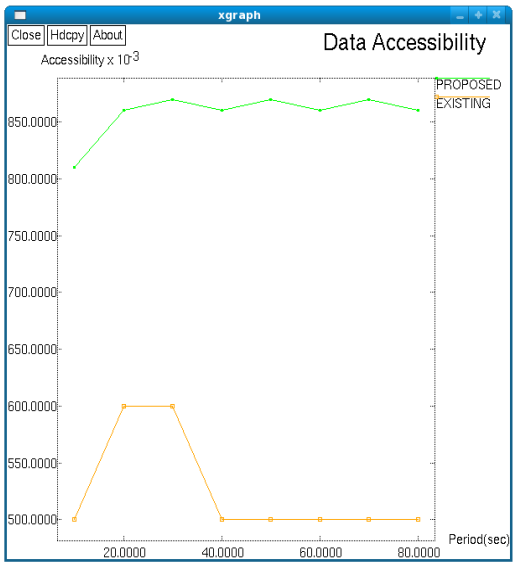

Fig. 8. Comapre with Data Accessibility. [x axis=Accessability x 10^{-3} and Y axis=Period(seconds)]

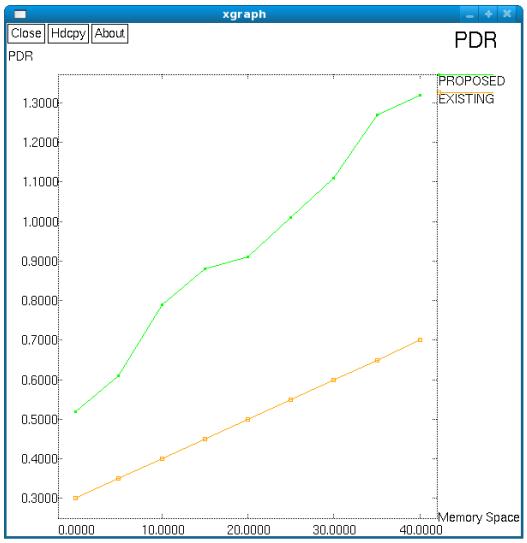

Fig. 9. Comparison with PDR. [x axis=Packet Delivery Ratio and Y axis=Memory Space]

This comparison chart explains how the present system has overcome as non secure data transimission in network. The proposed scheme is highly secure with the data transfer to one another with the use of the algorithm.

VII. Conclusion and Scope for Further Enhancement

Our System is vitality-effective and topology- versatile, disseminating grouping calculation that guarantees better bunch steadiness and upgrades the system lifetime.

The proposed system is an effective, secure navigation convention for portable, particularly selected network systems that ensure the disclosure of right availability data over an obscure system. In this model the data transfer has been done efficiently and securely with the use of Network Discovery.

As far as the future work is considered, it seems ahead to consider in extra information the behavior of the proposed conventions, eminently by methods for reproductions, in various versatility situations. We will likewise demonstrate that this scheme can be valuable in more traditional, one-jump remote systems, if the base stations (or the entrance focuses) is not totally trusted.

References

[1] L. Lazos and R. Poovendran, "HiRLoc: High-Resolution robust localization for wireless sensor networks," *IEEE J. Selected Areas in Comm.*, vol. 24, no. 2, pp. 233-246, Feb. 2006.

[2] P. Papadimitratos, M. Poturalski, P. Schaller, P. Lafourcade, D. Basin, S. Capkun, and J. P. Hubaux, "Secure neighborhood discovery: A fundamental element for mobile ad hoc networks," *IEEE Comm. Magazine*, vol. 46, no. 2, pp. 132-139, Feb. 2008.

[3] R. Shokri, M. Poturalski, G. Ravot, P. Papadimitratos, and J. P. Hubaux, "A practical secure neighbor verification protocol for wireless sensor networks," in *Proc. Second ACM Conf. Wireless Network Security (WiSec)*, Mar. 2009.

[4] M. Poturalksi, P. Papadimitratos, and J. P. Hubaux, "Towards provable secure neighbor discovery in wireless networks," in *Proc. Workshop Formal Methods in Security Eng.*, Oct. 2008.

[5] S. Capkun and J. P. Hubaux, "Secure positioning in wireless networks," *IEEE J. Selected Areas in Comm.*, vol. 24, no. 2, pp. 221-232, Feb. 2006.

[6] E. Ekici, S. Vural, J. McNair, and D. Al-Abri, "Secure probabilistic location verification in randomly deployed wireless sensor networks," *Elsevier Ad Hoc Networks*, vol. 6, no. 2, pp. 195-209, 2008

[7] P. Papadimitratos and Z. J. Haas, "Secure routing for mobile ad hoc networks," in *Proc. SCS Commun. Networks and Distrib. Sys. Modeling and Simulation Conf.*, 2002.

[8] S. Capkun, L. Butty án, and J. P. Hubaux, "Sector: Secure tracking of node encounters in multihop wireless

networks," in. *ACM Wksp. Security of Ad Hoc and Sensor Networks*, ACM Press, 2003, pp. 21–32.
[9] D. Ciullo, V. Martina, M. Garetto, and E. Leonardi, "Impact of correlated mobility on delay-throughput performance in mobile ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1745–1758, Dec. 2011.
[10] M. J. Neely and E. Modiano, "Capacity and delay tradeoffs for ad hoc mobile networks," *IEEE Trans. Inf. Theory*, vol. 51, no. 6, pp. 1917–1937, Jun. 2005.
[11] M. Garetto and E. Leonardi, "Restricted mobility improves delaythroughput tradeoffs in mobile ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 56, no. 10, pp. 5016–5029, Oct. 2010.
[12] S. Capkun, M. Hamdi, and J. Hubaux, "GPS-free positioning in mobile ad-hoc networks," in *Proc. HICCSS*, Maui, Hawaii, Jan. 2001, pp. 3481–3490.
[13] G. ´Acs, L. Butty´an, and I. Vajda, "Provably secure on-demand source routing in mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 5, no. 11, pp. 1533–1546, 2006.
[14] M. Grossglauser and D. N. C. Tse, "Mobility increases the capacity of ad hoc wireless networks," *IEEE/ACM Trans. Netw.*, vol. 10, no. 4, pp. 477–486, Aug. 2002.
[15] D. Ciullo, V. Martina, M. Garetto, and E. Leonardi, "Impact of correlated mobility on delay-throughput performance in mobile ad hoc networks," *IEEE/ACM Trans. Netw.*, vol. 19, no. 6, pp. 1745–1758, Dec. 2011.
[16] L. Ying, S. Yang, and R. Srikant, "Optimal delay-throughput trade-offs in mobile ad hoc networks," *IEEE Trans. Inf. Theory*, vol. 54, no. 9, pp. 4119–4143, Sep. 2008.
[17] X. Lin and N. B. Shroff, "The fundamental capacity-delay tradeoff in large mobile ad hoc networks," in *Proc. MedHoc'04*, 2004.
[18] G. Sharma, R. R. Mazumdar, and N. B. Shroff, "Delay and capacity trade-offs in mobile ad hoc networks: A global perspective," in *Proc. IEEE INFOCOM '06*, 2006.
[19] X. Hong, M. Gerla, G. Pei, and C. Chiang, "A group mobility model for ad hoc wireless networks," in *Proc. ACM MSWiM '99*, 1999.
[20] A. Savvides, C. Han, and M. Srivastava, "Dynamic fine-grained localization in ad-hoc networks of sensors," in *Proc. MOBICOM*, Rome, Italy, Jul. 2001, pp. 166–179.
[21] S. Chinara and S. K. Rath, "TACA: A topology adaptive clustering algorithm for mobile ad hoc network," in *National Institute of Technology*, Rourkela, Orissa, India, January 2009
[22] M. Kumaresan and G. K. D. P. Venkatesan, "Enabling high performance computing in cloud computing environments," in *IEEE Xplore*, ICEICEECE-2017.
[23] K. K. Sampth and V. G. K. D. Prasanna "Certain investigation in DNS stub network performance by using accelerator system," *Asian Journal of Research in Social Sciences and Sciences and Humanities*, vol. 7, no. 2, 2017.

S. Dhanabal is an Associate professor in Department of Computer Science and Engineering, PGP College of Engineering and Technology, Namakkal. He recived aM.E degree specializing in computer science and engineering from Sathyabama University ,Chennai in 2006. Now he purusing a PhD in Karpagam academy of higher Education, Coimbatore. He has over 12 years of teaching experience. His area of interest includes networking, data structures and mobile computing.

Dr. G. K. D. Prasanna Venkatesan is an a Dean- Faculty of Engineering in Karpagam Academy of Higher Education, Coimbatore. He received a Ph.D. information and communication from Anna University, Chennai in 2009. He is expertise in physical layer design of beyond 4G Technologies. He has published more than 120 Research journals, conferences and Six Patents. He produced 10 doctorates under his supervision. His area of research includes 5G, Network algorithm development for RF, Testing of high speed wireless communication, Machine Learning, Artificial intelligences(AI), Design of Antenna, etc.,

Dr. P. Amudhavalli is an Associate Professor in Department of Computer Science and Engineering, Karpagam Academy of Higher Education, Coimbatore. She received a MCA degree in from University of Madras in 2003 and M.E.in Information and Communication from Anna University Chennai in 2008. She finished her doctoral degree in Computer Science and Engineering specializing in Cloud Computing. She has over 12 years of teaching experience. She has published more than 14 papers in international journals and conferences. Her area of interest includes Cloud Computing, Big Data, Image processing and Soft computing.