DLBPS: Dynamic Load Balancing Privacy Path Selection Routing in Wireless Networks

R. Jayaprakash and Radha Balasubramanian

Abstract The Adhoc Network (MANET) is a set of nodes inside a particular group which communicates one another inside the network. These are generally packet nodes that travel and subjected for variation in the routing based on the requirement of the mobility. A proper routing technique is essential for the transmission of data packet from the source to the destination. A cluster-based routing protocol is accessed on its capability to distribute transfer over the network mobile nodes, and a superior routing protocol realizes this without establishing unacceptable delay. This paper presents novel dynamic load balancing privacy path selection (DLBPS) algorithm for mobile ad hoc networks to address the issue of the packets' strength when transmitted and also on the security aspect by addressing attack prevention. The experiment is carried out as a simulation in NS2 framework. The DLBPS method performs gateway mobility load balancing in the network order to achieve higher aggregated throughput among data transfer. Meanwhile, the proposed algorithm establishes detection, privacy collector privacy manager, and privacy propagator to complete the privacy path selection. The experimental result proves that the proposed mechanism outperforms the existing HsecGR and Trust-ECC methods.

Keywords Cluster · Load balancing · Gateway · Privacy preserving · Path selection

1 Introduction

A mobile ad hoc network (MANET) is a kind of ad hoc network that consists of many nodes that are mobile and wireless in nature forming a temporary network in the absence of the support from stable "network infrastructure." In MANETs,

R. Jayaprakash (✉)
Department of Computer Science, Nallamuthu Gounder Mahalingam College & STC, Coimbatore, India
e-mail: jpinfosoft@gmail.com

R. Balasubramanian
Department of Information Technology, Sri Krishna Arts and Science College, Coimbatore, India

T. Sengodan et al. (eds.), *Advances in Electrical and Computer Technologies*,
Lecture Notes in Electrical Engineering 672,
https://doi.org/10.1007/978-981-15-5558-9_70

Table 1 Simulation parameters

Parameters	Symbol and value
Mobile nodes	MN & 5-200 in steps of 10
Simulation area	Row × Column & 1000 × 1000
Transmission range	TR & 5-200 in steps of 10
Distributed weights	D_{w1}, D_{w2}, D_{w3}, …, D_{wn} & (0.1, 0.04, 0.05, 0.2, 0.5)
Node energy	E_{node} & 100 Joules
Boosting energy	E_{boost} & 100J/bit/m^2

all nodes are capable to move and still connected using multi-hop communication. The foremost goal of this network is provisioning of efficient communication by incorporating routing functionality into mobile network nodes. A MANET network is decentralized networked system where the nodes themselves are responsible for all activities within the network such as topology discovery and packets or message delivery.

The MANET can be logically depicted in the form of clusters through assembling together group of nodes that can be managed by cluster heads. Within a particular cluster, the cluster head (CH) is interconnected to all the nodes in its cluster [1], (*Chatterjee M, SK Das, D Turgut*, **2002**). Clustering is vital technique in a MANET often utilized to structure its hierarchy and organization. The use of clusters assists to simplify the complexity in how information about cluster nodes are managed as well as approaches to resolving or reducing network blocking.

Cluster-based routing is one of the routing methods with regard to MANETs (E*phremides, Jeffery Wieselthier, Dennis Baker*, **1987**) [2] in which several clusters of mobile nodes tend to be shaped using each cluster featuring its own cluster head that accounts for routing between clusters. "Clustering of nodes saves energy along with transmission bandwidth in ad hoc networks."

2 Cluster Network Model

In the ad hoc network, the packets are sent from a source to destination using the multi-hop approach by selecting suitable nodes in the middle data which are transmitted across a peer-to-peer network in the absence of a centralized server in the available protocols. These are organized dynamically by self as in case of an ad hoc topology.

Clustering (*Bednarczyk W, P Gajewskil*, **2013**), [3] is a methodology where relatively large network is segmented into smaller groups having some characters or behavior in a similar fashion. This is done based on some protocols in order to make the difference visible in-between the available nodes in other sub networks. The nodes which are not related to each other are combined to arrive at a structure. All nodes are assigned predefine functions and constraints, namely cluster head, the gateway,

and nodes of the member of cluster. This area which is segmented is called a cluster which bears a head and acts as a co-ordinator and is selected by every cluster.

Cluster head (CH) is similar to other nodes, but performs the functionality as a supervisor and is responsible for functions such as cluster management and updation of routing table and is responsible to identify new routes. All the other nodes are members inside a cluster, and the node through which the intercommunication occurs is called as gateway node. The cluster head is responsible for the data transmission among the nodes inside a cluster, and outer communications if any are done through the CH through the gateway nodes.

The clustering is done in a way that all the nodes inside a cluster are subjected to transmit a HAI or hello message along with their IP address. The CH in further appends the IP address of the nodes that are members to their self-messages that are controlled. The connection is considered as broken if the member node fails to get three control messages in the process of selection of clusters. In case of broken communication, the corresponding node goes in search of a new CH. To confirm the new CH, The hello message is transmitted along with its IP address.

The objective of the research is to propose a protocol for routing which is based on the cluster technology and which is privacy preserving in a MANET environment. The main aim is to effectively partition the inside and outside broadcasting of cluster message in a secured fashion. To minimizing a load balancing of low-maintenance clustering schemes intend at providing secure cluster framework flow for cluster-based routing protocols with slight cluster preservation cost. By preventive re-clustering positions or minimizing precise control packets for clustering, the cluster configuration can be preserved well without extreme utilization of network resources for cluster preservation.

The remaining of the paper is segmented and presented as follows: Literature review is detailed in Sect. 3; in Sect. 4, we have discussed dynamic load balancing privacy path selection (DLBPS). Sections 5 and 6 discuss the performance evaluation and conclusion, respectively.

3 Literature Review

(*R. Jayaprakash*, *B. Radha*, **2018**) [4, 5] came up with the networking group in which the privacy is preserved. Here, the CH is responsible for the intercommunications inside a cluster with the aid of a battery in addition which is dominant in evaluating the members of the cluster. As the information packets are subjected to go in and out of the network, the overhead in testing the stability of the network becomes crucial. A routing protocol based on the clustering technology is proposed to achieve privacy preservation. The experiment is simulated using the NS2 tool. The complete process was based on the routing that happens in the source and on-demand process. The proposed protocol is based on the CH selection, and the same is applied in ad hoc framework by a variation by implementing a communication exchange on demand between the nodes that are mobile in a ad hoc network.

(*Gupta, A.K., Sadawarti, H., Verma, A.K*, **2011**), [6] put forth the problem when routing is considered and the research challenges in the MANET environment and got a large number of responses from the researchers round the globe. In order to address the problem associated with routing, various protocols were proposed and still researchers are working for man more such protocols to be proposed. To identify the best protocol is a tedious task as the behavior and performance of each protocol vary in different scenarios as when size and topology of the network are considered. The detailed surveys of the existing protocols are elaborated with its functions and characters. A comparative study was also made on the available methods that are very much used for arriving at a routing decision.

(*Kaur, H., Singh, H., Sharma, A*, **2016**), [7] explained the concept of MANET which are tented to have organized in a self-mannered networks through which there is no need of connections to be established for the transmission of information. These suffer from different factors in terms of scalability, topology, and higher mobility. These are also subjected to damage owing to its large mobile nature. Routing on the basis of the topology is subjected to fail because of the dynamic change in the topology itself. A new concept of routing based on the geography of the nodes was introduced. These proved to be more stable and efficient even in the case of dynamic change in the location of the nodes. Two methods, namely the hybrid routing and geographic routing, are studied in this paper

(*Sarika, S., Pravin, A., Vijayakumar, A., Selvamani, K.*, **2016**) In wired networks, [8] there are a large number of barriers when communication occurs. These pave the way for the intruders to get pass the firewalls. Hence, these have to be made to get through secured gateways for safe transmission of data. Unlike the wired networks, the wireless sensor networks are considered to be less safe as the nodes follow a dynamic topology and also the power consumed will be more. The mobility is the key factor to be taken for account as it paves the way for attackers leading to collapsing the complete network. The problems associated with the wireless mobile networks are discussed in detail.

(*Boulaiche, M., Bouallouche-Medjkoune, L*, **2017**), [9] proposed a new technique which takes into account the geographic locations and came up with a routing concept based on the location of the nodes under communications from source to destination. These also reduce the overhead of routing control and guarantee accurate delivery of the message without time delay over such networks. The basic problem with this approach is that all the nodes are considered as trusted which paves the way for malicious content which in turn disrupts the forwarding of the packet. A proposal was given for the new approach for the security against attacks possible. The nodes that lie in between are tested for its authenticity and integrity and send back the acknowledgment upon verification. This prevents the packet being dropped in middle due to attacks. Symmetric cryptography is used as an encryption standard. They proved to be efficient even if there are compromised packets in the network.

(*Kaur, M., Kaur, S*, **2016**), [10] discussed routing protocols methods which are employed to send and obtain information from origin to vacation spot correctly. Clustering structured routing protocol methods are the methods through which course plotting will certainly be done by means of grouping. Clustering is often a practice

where a big network is divided right small groups as well as communities. The leading purpose of clustering is usually to boost routing protocols in the network stratum through reducing the size of the particular routing protocol platforms as well as lessens improve over head through updating the particular routing protocols platforms soon after topological alterations take place. This kind of report is evaluated as well as applied for the particular functionality associated with current cluster structured routing protocols method that the election associated with cluster is dependent on the particular minimum Ids associated with node in cluster. The authors evaluated the particular functionality associated with CBRP method and presented each of our outcomes.

(*Rajasekar, S., Subramani, A.,* **2016**), [11] briefed that a MANET has a great number of nodes that are subjected to move in a dynamical manner. In such networks, the devices used for computation will require a large and costly infrastructure. In these networks, the nodes are subjected to move dynamically from one place to other and try to get synchronized with other nodes that are nearer. The topology can also change due to the mobility aspect. The main limitation of the MANET is the energy that will be available for each node for successful transmission and the lifetime of a node. Hence, the energy efficiency is a vital factor and was discussed elaborately.

4 Dynamic Load Balancing Privacy Path Selection

It is a vital process that aims to control the traffic in a complete network and also assures of distributing the traffic evenly over the network. The load will not be evenly distributed if there are user demands that are uneven and are more common in case of a MANET. The nodes present inside a network get more congestion and naturally vulnerable as a consequence owing to the fact of their location and the role assigned to them. The congestion will normally be more at the center rather in the end due to the fact that major of the nodes travel through the center part else would be put in a position to have contented with the relatively large number of neighboring nodes in the medium. The gateway nodes are subjected to more congestion since the traversal has to be done through the intermediate traffic domain. The congestion has to be avoided in such cases to maintain the connectivity in the network and the services they provide. Figure 2 depicts the dynamic load balancing privacy path selection (DLBPS) approach.

4.1 Network and Mobility Model

In process of network formation [4, 5] is ranked by forming graph and was already presented in the previous work (*R. Jayaprakash*, *B. Radha*, **2018**). In the mobility model, V_{max} and T_{pause} denote the two important key metrics that depict the node's behavior. If the V_{max} is minimum and the pause time T_{pause} is long, there exists a

strong topology which will be more stable. Contrarily, if the speed of the node is more, (i.e., V_{max} is more) and time of pause is T_{pause} is less, there will be high dynamicity among the nodes. By changing the values of these metrics, different scenarios for mobility can be achieved for variety of node's speed. The metric of mobility is to calculate in a quantified notation of the node's notation speed. This relative measure of speed between the node i and j at a given time t is

$$\text{Speed(i, j, t)} = \left| V_i(t) - \frac{V_j(t)}{M} \right| \tag{1}$$

The metric of the mobility is then calculated with reference to the speed in a relative manner which is taken as a mean of all the speeds in all the pairs of nodes in the entire time. The function is denoted with a formal notation as

$$M = \frac{1}{|i,\ j|} \sum_{i=1}^{N} \sum_{j=i+1}^{N} \frac{1}{T} \int_0^T \text{Speed}(i,\ j,\ t)\mathrm{d}t \tag{2}$$

where$|i,\ j|$ is the count of pairs of node that are distinct n is the overall count of the node in entire field of simulation. (i.e., the complete ad hoc network) and T is the time of simulation.

4.2 Gateway Mobility Load Balancing

This is a task of even distribution of interdomain traffic in an orderly manner and also efficiently in between the gateways and the primary objective being to increase the throughput as depicted in Fig. 1. The primary precondition is that it should have more than one gateway that are placed in the network which ensures the connection to the gateways present outside the network for transmission. This can also be the Internet. All the interdomain traffic are subjected to go through the nodes that are the gateways. They become more congested, and hence, many gateways need to be deployed in the network which enables the complete capacity of the network increased and the probability of congestion decreases.

The redundancy is also reduced which paves the way for increase in robustness. If any of the gateways experiences a failure, the others that are in stand-by will take care of the network. The policy of fairness is also achieved as with single gateway, different nodes enjoy different capacities that are based on the gateway's proximity. The mean distance to reach the gateway will be same in case if many gateways are deployed. Even though this technique proves to be more efficient than others, it also suffers some drawbacks. The traditional methods lack a concrete method to overcome these issues. When a short path is arrived, there are more possibilities that a gateway will be overloaded leading to collapse in the entire network. Hence, appropriate load balancing techniques are to be deployed for removing the potential risk involved and

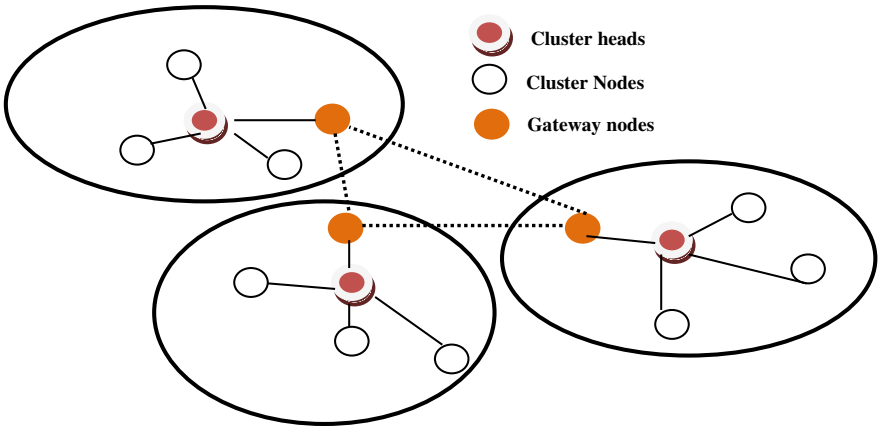

Fig. 1 Cluster network model

to ensure that there is no degrade in the aspect of performance. Cluster-based privacy preserving routing selection (CBPPRS) [4] is already elaborated in the previous work (*R. Jayaprakash*, *B. Radha*, **2018**). Here, a DEFINED-VALUE concept is used between the CHs and the nodes such that all the nodes in the given time of a network are within h hops of a CH.

4.3 LBCPR: Load Balancing Cluster-Based Privacy Routing

The LBCPR was already presented by both authors (*R. Jayaprakash*, *B. Radha*, **2018**) [4, 5] for load imbalance in the network and the partiality or favoritisms in picking up centrally located nodes for data transfer. The proposed novel cluster based routing metric, load and a minimization principle are to make a decision on a path that occupies mobile nodes with fewer load weight on them. In LBCPR, new metric called *load* will tell us the estimated load a mobile node (*mn*) is focused to in a network, and its value will specify the quantify of current load. In this model, link searching and send respond algorithms performs cluster load field accurately.

4.4 Dynamic Load Balancing Privacy Path Selection (DLBPS)

The DLBPS searching is achieved by k-path measure in the MANET, and this can be either in one direction or two directions. Hence, the host must be known its neighbor and the related information. The data packets are transmitted on a regular interval of time by sensing the neighbors. These are transmitted only a hop away and are not

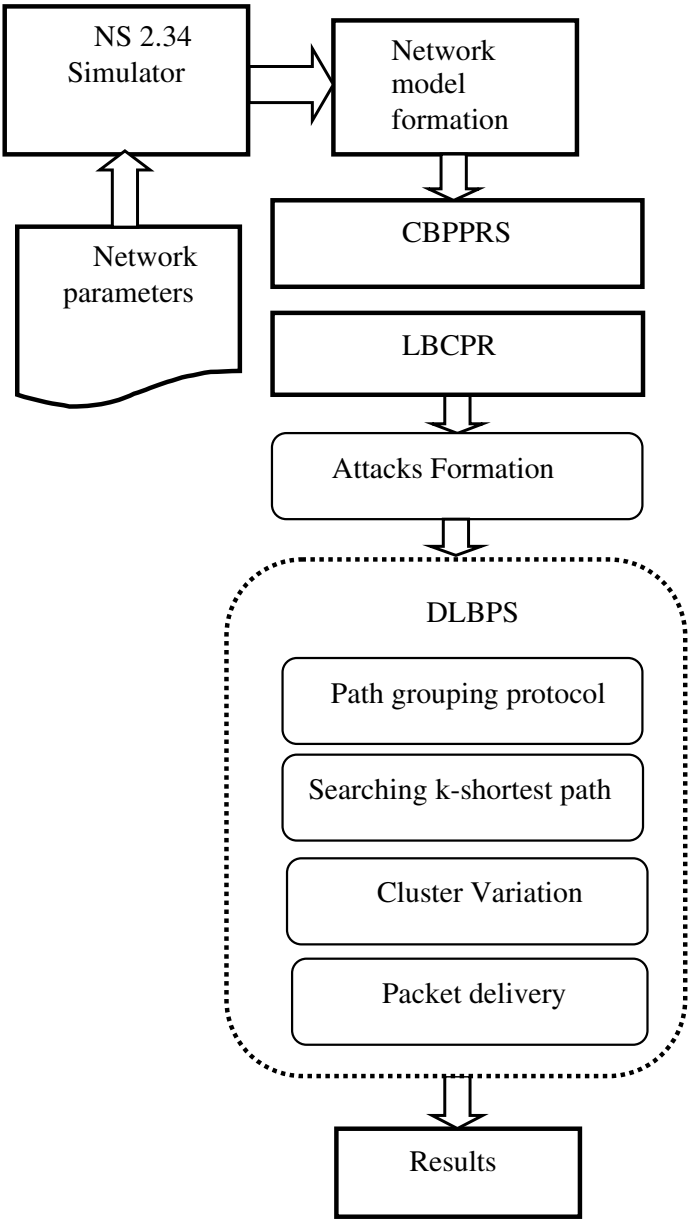

Fig. 2 Dynamic load balancing privacy path selection flow

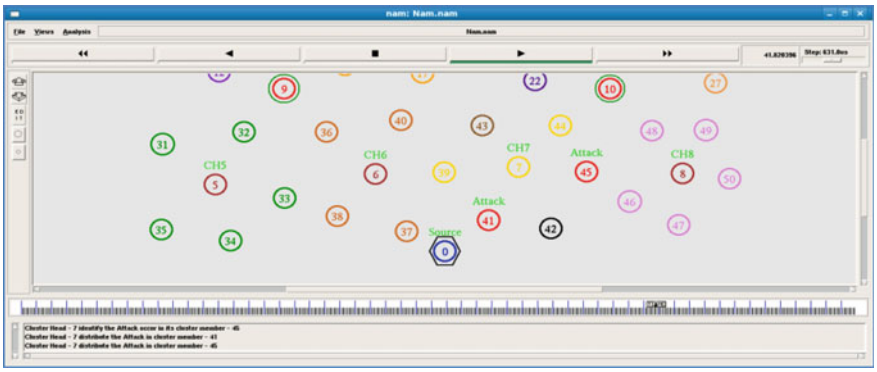

Fig. 3 Attacks formation

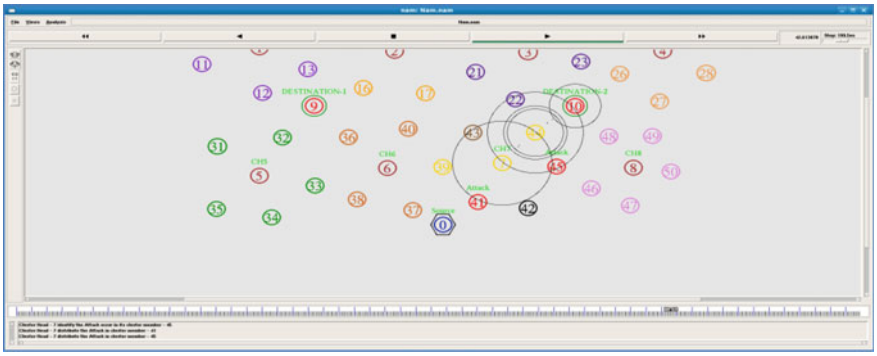

Fig. 4 DLBPS result

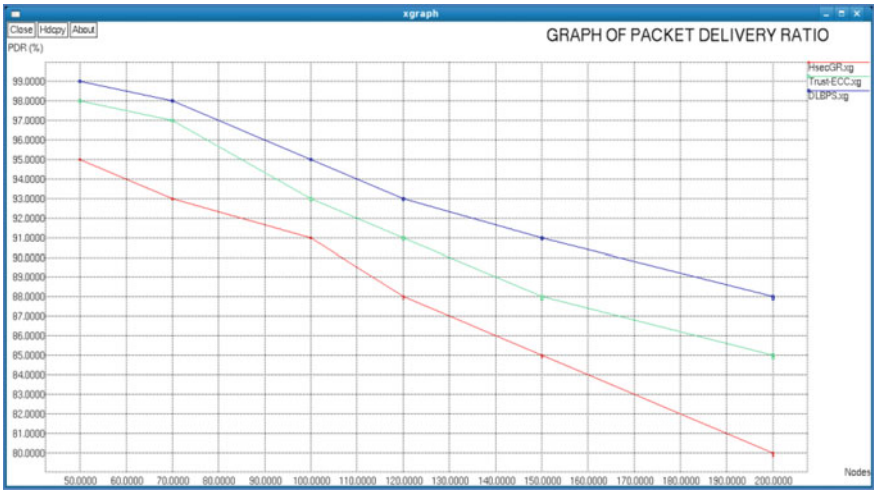

Fig. 5 Graph of packet delivery ratio

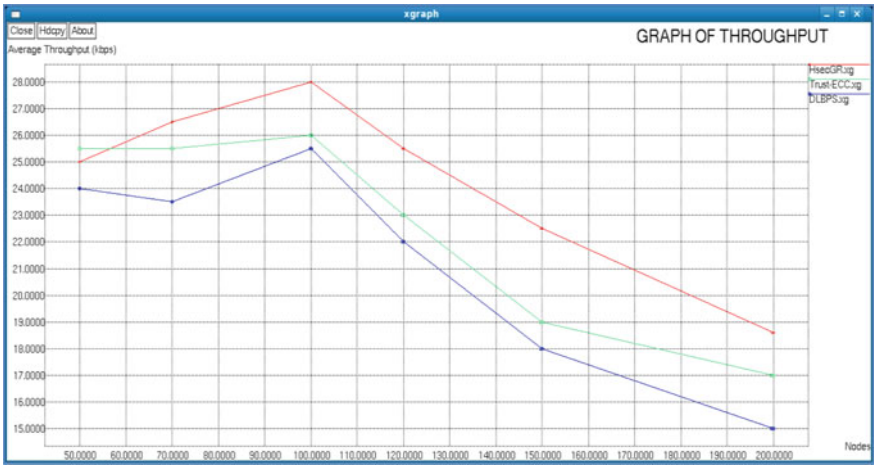

Fig. 6 Graph of average throughput

pushed further. When the host 1 gets the Hello message from Host II, The status of the second host is set to be asymmetric in the routing table.

DLBPS algorithm also helps in predicting the attacks that are distributed in an MANET. The scheme of investing the scheme's path of a protocol will examine all the nodes in the available network, and when any unusual behavior is found, the invocation of a distributed algorithm is done to confirm that the node is out of any malicious content. This method works along with other security metrics which are available in every node inside a network. The computations are given in terms of: (i) detection, (ii) privacy collector, (iii) privacy manager, and (iv) privacy propagator.

Algorithm 1: ***Dynamic Load Balancing Privacy Path Selection (DLBPS)***

Intialize *CH*← 0; *LBCPR*← 0; *DLBPS*← 0;

Process

Step 1: The node has to travel from source to destination through a protocol which starts the identification of the route.. During the identification process, source node transmits RREQ packets through the nodes which are available nearer.

Step 2: Searching neighbor cluster list present source to destination.

Step 3: Check gateway mobility balancing (*gmb*)

Step 4: if *gmb* ≠ *CH* ***then***
CH = *CH* + 1
end if

Step 5: if *gmb_count> nodecount_thresh* ***then***
//Target and all previous nodes are declared.
forward (*attack link*);
break;
end if

Step 6: select privacy cluster path for packet delivery

5 Performance Evaluation

The proposed system considers 50 to 200 nodes *Dynamic Load Balancing Privacy Path Selection (DLBPS)* in mobile ad hoc network, with nodes and is implemented on a random basis in a area of 1000 m × 1000 m.. The parameters considered for simulation are as mentioned below. Packet delivery ratio (PDR) is described as the fraction between the number of packets sent and received in destination. The proposed method ensures more PDR ratio when compared with existing HsecGR [9] (*Boulaiche, M., Bouallouche-Medjkoune, L*, **2017**) and Trust-ECC (*S. Syed Jamaesha and S. Bhavanim*, **2018**) methods [12].

The throughput comparison is shown in Fig. 7 where the blue line indicate the performance of the proposed algorithm and the red and green lines of the performances of other existing methods. [12]. The performance is measured by taking the average throughput in Y-axis and number of nodes in X-axis.

Figure 8 depicts the average performance delay, and it is obvious that the proposed method outperforms the other existing proposals [9, 12]. The average delay performance is taken as the product of time taken to get and deliver a packet. It describes

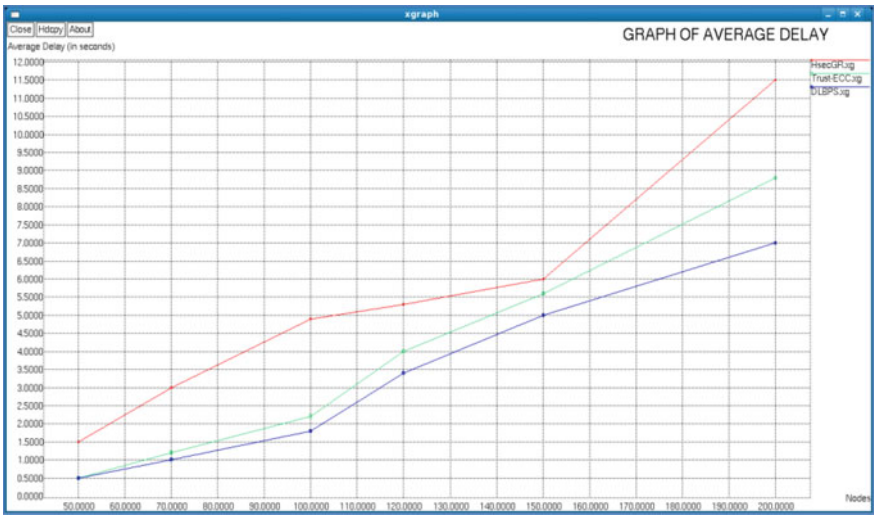

Fig. 7 Graph of average delay

the average delay of performance result. It is the product of time taken to obtain packets delivered to number of mobile nodes in network.

6 Conclusion

The dynamic load balancing privacy path selection (DLBPS) algorithm is evaluated and analyzed for mobile ad hoc networks on the strength of packet transmission and attack prevention. The DLBPS method performs gateway mobility load balancing in the network order to achieve higher aggregated throughput among data transfer. Meanwhile, the proposed algorithm establishes detection, privacy collector privacy manager, and privacy propagator to complete the privacy path selection. An experimental result shows that the proposed algorithm performs better than existing HsecGR and Trust-ECC methods3

References

1. Chatterjee, M., SK Das., Turgut,D., : WCA: a weighted clustering algorithm for mobile ad hoc networks. Clust. Comput., Kluwer Adademic Publishers, Manufactured in The Netherlands, Vol. 5 (2002) 193–206
2. Ephremides., Jeffery Wieselthier., Dennis Baker., : A Design Concept forReliable Mobile Radio Networks with Frequency Hopping Signaling. Proceedings of the IEEE Vol. 75,No. 1, (1987) 56–72

3. Bednarczyk, W., Gajewskil,p., : An enhanced algorithm for MANET clustering based on weighted parameters. Universal J. Commun. Netw. Vol. 1(3) (2013) 88–94
4. Jayaprakash.R., and Radha,B., : CBPPRS: Cluster Based Privacy Preserving Routing Selection in Wireless Networks, International Journal of Engineering & Technology, Vol. 7 (3.12) (2018) 439–443
5. Jayaprakash.R., and Radha,B., : LBCPR: Load Balancing Cluster Based Privacy Routing In Wireless Networks, International Conference on Recent Trends in Automation (ICRTA-2018)
6. Gupta AK, Sadawarti H, Verma AK (2011) Review of various routing protocols forMANETs. Int. J. Inf. Electron. Eng. 1(3):251–259
7. Kaur H, Singh H, Sharma A (2016) Geographic routing protocol: a review. Int. J. Grid Distrib. Comput. 9(2):245–254
8. Sarika S, Pravin A, Vijayakumar A, Selvamani K (2016) Security issues in mobile adhocnetworks. Procedia Comput. Sci. 92:329–335
9. Boulaiche M, Bouallouche-Medjkoune L (2017) Hsecgr: highly secure geographic routing. J. Netw. Comput. Appl. 80:189–199
10. Kaur M, Kaur S (2016) Analyze and implementation of cluster based routing protocol inMANETs. Int. J. Innov. Res. Sci. Eng. Technol. 5(3):3098–3107
11. Rajasekar S, Subramani A (2016) Performance analysis of cluster based routing protocol For MANET using RNS algorithm. Int. J. Adv. Res. Comput. Sci. Softw. Eng. 6(12):234–239
12. S. Syed Jamaesha and S. Bhavani, A secure and efficient cluster based location aware routing protocol in MANET, Springer Science + Business Media, LLC, part of Springer Nature 2018