VOL. 11, NO. 3, FEBRUARY 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences

www.arpnjournals.com

TRPSD: TRUSTWORTHY ROUTING POLICY FOR SERVICE DISCOVERY IN MANET

Shirin Bhanu Koduri[1] and M. Seetha[2]
[1]Jawaharlal Nehru Technological University, Hyderabad, India
[2]G. Narayanamma Institute of Technology and Science, Hyderabad, India
E-Mail: shirinbhanukoduri@gmail.com

ABSTRACT

MANET faces many challenges owing to its infrastructure-less nature. The central governing authority is absent in the jargon of MANET and thus, this work exploits clustering technique. The clustering technique relies on the leader node and this work elects a leader node by means of trust mechanism. The elected leader node is recycled for every period of time, so as to preserve the energy of that node. The trust metrics employed to elect a leader node of a cluster are energy, packet delivery ratio and mobility. Besides this, a trustworthy routing policy is introduced, so as to increase the reliability and the quality of the service. A trustworthy route depends on the count of trustworthy nodes being present along the specific path. The experimental results prove the efficacy of this work.

Keywords: MANET, cluster, routing, trust.

1. INTRODUCTION

A Mobile Ad hoc Network (MANET) is a self-governing network that is composed of several mobile nodes. The main challenge of MANET is its dynamic nature. The motion of the nodes cannot be pre-determined and thus any number of nodes can join and leave the network, at a specific point of time. The mobile nodes are capable to provide services to other nodes. For instance, a service can be a simple file or software which can be utilized by other nodes [1-3].

The important terminologies associated with this issue are service requester, service provider and service. Service requester is the node that requests for service. The nodes that offer services to others are service providers. At this juncture, a mechanism is needed to list all the possible services, service providing nodes and the optimal service must be located for the service requester.

When a node looks for a specific service, a mechanism is needed to trace and invoke the service from the service provider. This job is done by the service discovery protocol. The major challenge being faced by any service discovery protocol is that the mobility of the nodes, such that the nodes can join and leave the network at any point of time. Thus, the protocol must be updated then and there, in order to have the recent list of available services being provided by the service providing nodes.

The main components of a service discovery protocol are service description, service discovery and routing. Service description is the summary of the functionality of the service being provided by the service provider. Service discovery is the major part of the service discovery protocol, as this phase involves searching and selecting the optimal service from the list of available services of the moment. Finally, the optimal service providing node must be routed to the service requested node [4, 5].

In this work, the routing issue in service discovery protocol is focussed. The main goal of this work is to arrive at a trustworthy route. A route can be claimed as trustworthy, with respect to the count of trustworthy nodes along the computed path. This work gives more preference to the trustworthy route than the shortest route. This paves way for effective mapping of the service between the service requesting and providing nodes.

This remainder of the paper is organized as follows. Section 2 presents the review of existing literature related to the service discovery process. The proposed methodology is presented in section 3. The performance of the proposed work is evaluated in section 4. Finally, the concluding remarks are presented in section 5.

2. REVIEW OF LITERATURE

This section reviews the existing literature with respect to clustering and routing mechanism in MANET.

2.1 Clustering in MANET

MANET faces many problems, as it has got no central authority. Clustering technique imitates the functionality of the fixed infrastructure, such that the nodes are controlled and monitored by some central authority. Every cluster has a head node and it is responsible for all activities of the cluster. However, choosing the right node as a cluster is a challenging task [6]. Some of the cluster head selection algorithms for MANET are lowest ID, highest degree, distributed clustering algorithm, weighted clustering algorithm, distributed weighted clustering algorithm [7 - 11].

Linked Cluster Algorithm is an algorithm that prompts each node to behave as a cluster head, gateway or simple nodes [7]. Initially, all the nodes are normal and each node broadcasts its own ID for every time period. In [12], an adaptive clustering algorithm in which all the

nodes act in the same way, once the cluster is formed and the cluster head has no role to play.

The algorithm proposed in [8] takes the connectivity of the nodes alone into account and the cluster head is selected. In [13], an algorithm namely associativity based cluster formation and management is proposed. This algorithm focuses on the stability of the node alone to elect the cluster head.

2.2 Routing in MANET

A dynamic source routing protocol is presented in [14] that quickly adapts to route change. Some of the routing protocols paired with cryptography are proposed in [15] and [16], namely SAODV and Ariadne. However, these protocols are central agents or trusted third parties, which are not feasible.

An enhancement of DSR is presented here and is named Trusted DSR and proposed in [17]. This protocol chooses a path based on the trust value of the nodes ranging from the source to the destination. The trust value is calculated by the number of acknowledgements sent from the node. As the number of acknowledgements increase, the trust value also increases.

In [18], the performance of three different protocols namely Trusted AODV, DSR and TORA were compared and the results concluded that Trusted AODV works well with a stable throughput. A Fuzzy based Ad hoc On-demand Distance Vector (FAODV) routing protocol is proposed in [19]. In [19], a threshold value is set for trust verification and the trust value is evaluated by imposing fuzzy rules.

Trust based intrusion detection system is presented in [20], in which three types of trust are defined. They are subjective, indirect and functional reputation. The work proposed in [21] analyses the trust level of all nodes by employing entropy based trust system. In [22], every device is protected with Trusted Platform Module (TPM), which is a cryptographic protocol. This hardware chip makes it possible to fix its local state and also can predict the states of remote systems too.

Thus, malicious devices are automatically detected and are not allowed to take part in the network. The work proposed in [23] presents a reputation system along with the trust system. In this work, both personal and general evidences are used to decide packet transmission.

3. OVERALL FLOW OF THE WORK

The central theme of this work is to present a service discovery mechanism, which focuses on clustering, service discovery and routing. The concept of clustering preserves as much energy as possible. As MANETs are energy constrained, clustering is a boon to this type of network. Service discovery is the primary scope of this work. The process of service discovery has two phases and they are service search and selection. Finally, the selected service is ideally routed by means of trust mechanism.

3.1 Clustering mechanism

The root of clustering mechanism relies on a head node, which can manage its constituent nodes effectively. MANET is energy restricted and the energy of the nodes gets deteriorated during packet forwarding, routing and other operations. The idea of clustering mechanism is to designate a node as leader node, such that the leader node takes care of its member nodes.

However, selection of the leader node is not simple to achieve. The leader node is responsible for all the operations associated with the cluster member nodes. This leads the way for energy preservation of all the member nodes, at the energy of the leader node. Still, the energy of the leader node drains sooner, as it is responsible for all the activities of the member nodes. Thus, it becomes necessary to recycle the leader node for every period of time. This is to prevent energy depletion of the leader node and to balance the energy level of all the participating nodes in the network.

3.2 Trust degree computation

The underlying base of this work is the trustworthiness. The trust level of the nodes is decided by certain trust metrics. The leader node is elected on the basis of trust. The leader node then computes the trust level of all its member nodes. Finally, the route is defined by taking the trust level of nodes into account. The main scope of this work is trustworthy routing. The overall flow of the work is presented in Figure-1.

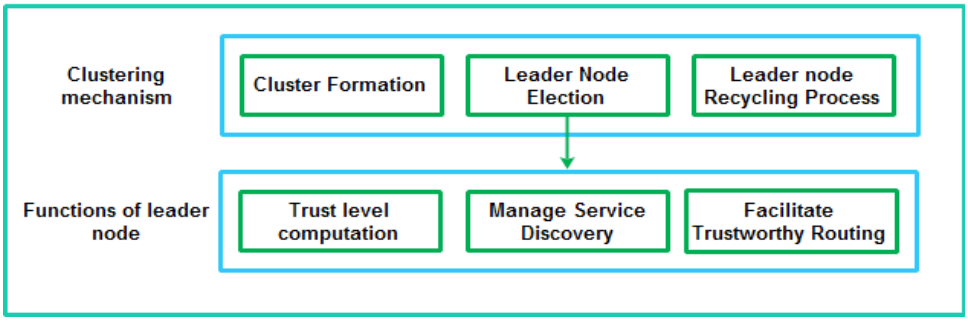

Figure-1. Overall flow of the work.

3.3 Service discovery

Service discovery is the process of searching for a service which is requested by the node and locate the service for the requested node. Another important phase of service discovery is the selection of optimal service. The optimal service can be picked up by several Quality of Service (QoS) parameters.

3.4 Service routing

The final step associated with service discovery is the effective routing between the service requester and provider. Routing is the most crucial step, as it consumes more energy. Besides this, an unfair routing mechanism may result in time delay. Thus, a fair routing policy is the need of this hour.

In substance, this work strives to present trustworthy routing between the service requesting and the responding nodes. The trust degree of the nodes is calculated by the head node for every period of time. The route is finalized based on the trustworthiness of the nodes. This means that a trustworthy route possesses several trustworthy nodes in it. Thus, a high quality and reliable service can be provided without any delay.

4. PROPOSED WORK

This work is broken down into four major phases, as mentioned in the previous section. Every phase has its own significance; however routing is the major scope of this work. All these phases are described in detail and are as follows.

4.1 Cluster formation and leader node election

A cluster is formed for every time interval and the maximum size of the cluster is fixed as 20. For every time period, a node is chosen randomly and the surrounding 20 nodes are selected and the CLTR_JOIN request is broadcasted.

This is followed by the computation of trust metrics and the most trustworthy node is chosen as the leader node. The key task of the leader node is to compute the trust level of all the member nodes. The leader node maintains three tables namely TR_LVL, SERV_ADV and NEGBR tables. TR_LVL table maintains the trust level of all the member nodes. The service advertisements are stored in the SERV_ADV table and the neighbourhood cluster details are saved in the NEGBR table. For every thirty seconds, all the tables are updated by overwriting the existing data, so as to save memory.

4.1.1 Leader node election

The leader node from a cluster of 20 nodes is elected by taking trust metrics such as energy level, packet delivery ratio and the mobility into account. The significance of these parameters is realized and thus employed. The trust model is provided in the following sections. The trust metrics for electing the leader node is depicted in Figure-2.

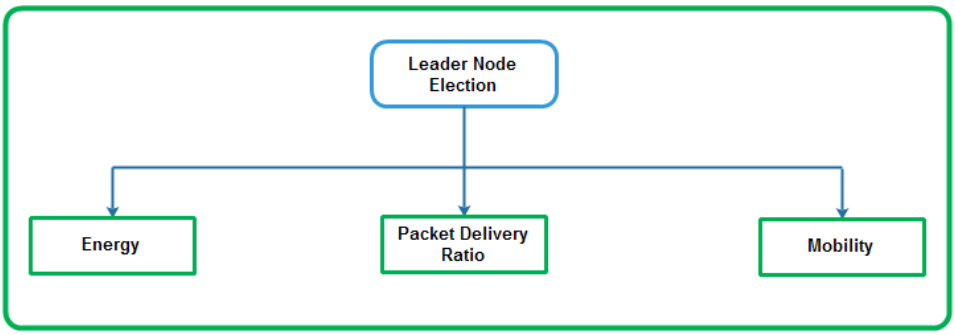

Figure-2. Metrics to elect leader node.

4.1.1.1 Energy [$\mathcal{E}$]

Energy is the vital parameter to calculate the trust level. This is because, no node can achieve its goal, unless it has reasonable amount of energy. Thus, energy is considered as the primary parameter. A fully charged node is given the value 1 and null energized node is assigned with the value 0.

Table-1. Energy table.

Energy table	
Energy value	Node type
0	Null energized
0.5	Partially energized
0.75	Three-fourth energized
1	Fully charged node

The value of this parameter varies from 0 and 1, based on the energy of any node.

4.1.1.2 Packet delivery ratio [P]

The packet delivery ratio indirectly decides the behaviour of the node, which makes sense that the incoming and the outgoing packets are taken into account. To exemplify this concept, consider a node with certain incoming and outgoing packets. In this scenario, there are two possible cases. They are these nodes may not forward all the incoming packets, may duplicate the incoming packets and forward them, which is replay attack.

Let a be the number of incoming packets and b be the number of outgoing packets. The node is claimed as normal node, provided it adheres to the following equation.

$$a = b \quad (1)$$

Equation (1) states a normal and a healthy flow of packets, in which the received packets are equal to the forwarded number of packets.

The below equations showcase the attitude of the misbehaving nodes. In the first case, the misbehaving node transmits only half the count of received packets. This makes sense that the node forwards about fifty percent of the total packets needed to be forwarded.

The second case illustrates the scenario in which the node attempts to forward twice the count of packets to be forwarded. This is the attempt to waste the resource and to shatter the entire network.

$$a = b/2 \quad (2)$$

$$a = 2b \quad (3)$$

$$a = 0b \quad (4)$$

Finally, eqn. 4 exemplifies the situation that the node shows no interest in forwarding the packets. This situation may occur due to energy drop or complete disinterest to forward packets for the sake of other nodes. The above equations show the misbehaving tendency of nodes. Packet delivery ratio can judge the varying behaviour of the nodes and this is the most effective parameter to calculate the trust level.

4.1.1.3 Mobility [μ]

The concluding parameter for computing trust level is the degree of mobility. A node with highest degree of mobility can play the role of a leader in the cluster. Apart from this, the most dynamic node cannot serve its purpose effectively. Thus, this work considers mobility pattern of node to compute the trust level.

Table-3. Mobility table.

Mobility table	
Mobility value	**Node type**
0	Intensely mobile
0.5	Modest mobility
0.75	Tolerable mobility
1	Stable node

When the node is extremely mobile, then the mobility value of that node is assigned as 0. On the other hand, the value 1 is assigned to a stable node.

4.2 Leader node recycling process

It is not advisable to maintain the same node as leader node for a longer period of time. The energy of the leader node will get depleted very fast, so it is necessary to preserve the energy of the leader node. This is possible only when the leader node is recycled then and there. Thus, the chief node is re-elected for every thirty seconds.

4.3 Trust model

The trust model of this work relies on three trust metrics that are considered as the most important. The trust metrics are chosen by paying more attention, as these parameters are the base of the performance of the entire system.

All the chosen metrics of trust range from 0 to 1. Finally, the average of all the three parameters is computed and this range determines the leader node. The below given equation finds the average of the trust metrics and the leader node is selected.

$$l_n = \frac{\mathcal{E}+P+\mu}{3} \quad (5)$$

Where $\mathcal{E}$ is the energy, P is the packet delivery ratio and μ is the mobility of the node.

Table-4. Nature of node.

S. No.	l_n	Nature of node
1	0.8 to 1.0	Trustworthy node
2	0.5 to 0.7	Partially trustworthy node
3	0-0.4	Malicious node

The node which has the greatest l_n is chosen as the leader node. The leader node then computes the same trust metrics for all the nodes, as given in section 4.1.1 respectively. The trust values are updated for every thirty seconds and the contents are overwritten. This is to save memory of the network.

4.4 Service discovery

The process of service discovery involves two phases and they are searching and selecting the optimal service. Service advertisement is the most important step in this stage. The service providing nodes must advertise the nature of service it provides, the location of the service, trust level and average response time.

The service advertisement is forwarded to the leader node of that particular cluster. The leader nodes maintain the important attributes such as type of service, trust level, location and average response time into its local memory and is updated periodically.

The service requesting node forwards a SERV_REQ packet to the leader node. The attributes of this packet are service required, present energy and memory of the node. On receiving the SERV_REQ, the leader node checks whether or not the requested service is present in the corresponding cluster.

In case, if the requested service exists in the same cluster then, the process is very simple. The leader node simply redirects the service request to the service providing node. On the other hand, if suppose the requested service does not exist in the cluster then, the leader node forwards the SERV_REQ to the nearby leader nodes.

The neighbourhood leader nodes check for the service and respond the requested leader node accordingly. In case, if the requested service is not present in any of the clusters then, the service request is denied. In case of presence of the requested service, then the service is routed to the service requester. By this way, the service search takes place.

4.4.1 Optimal service selection

After successful location of the requested service, the optimal service providing node must be selected. The optimal service can be picked up by certain Quality of Service (QoS) parameters such as average response time, trust level and the load of the service providing node.

The leader node checks for the above mentioned parameters and effectively selects the node with the least response time and load and the highest trust level. This optimal service selection and ranking mechanism is provided in [24]. The optimal service is chosen by this way and this step is followed by the routing process.

4.5 Trustworthy service routing

Service routing is the main scope of this work and is achieved by trust mechanism. The routing policy of a service protocol must be fair, such that the delay associated with the service delivery can be eliminated. Besides this, the energy consumption can be considerably reduced.

The trustworthy routing makes sure that the chosen route possesses as many trustworthy nodes as possible. This work alters Ad hoc On Demand Vector (AODV) protocol, so as to make up the trustworthy route. AODV protocol by itself selects the shortest path.

However, this work focuses on trustworthiness rather than shortest path. Whenever a service is needed to be provided to the requesting node, the requesting and the providing node must be interconnected. For this interconnection, many paths can be framed to reach the destination, but still, not all the paths are feasible.

This is the reason for why routing is given much importance. The proposed work calculates the trust of every path and arranges them in descending order. The path with maximum trust is chosen as the optimal path for transmission. The computation of trustworthy path depends on the count of trustworthy nodes being present in a specific path.

In case, if the count of trustworthy nodes along the path is equal to the total number of nodes, then the path is completely trustworthy and it is given in the equation 6.

$$CT_n = CP_n \quad (6)$$

$$CT_n = \frac{CP_n}{2} \quad (7)$$

$$CT_n = \frac{CP_n}{4} \quad (8)$$

$$CT_n = 0 \quad (9)$$

Where CT_n is the count of trustworthy nodes along a path and CP_n is the total count of nodes being present in the path.

Case 1: The first case illustrates the situation in which the total number of trustworthy nodes in the path equals the total count of the nodes in the path. Thus, all the nodes present along the path are trustworthy and thus this path must be the best.

Table-5. Route table.

S. No.	CT_n	Nature of route
1	CP_n	Best route
2	$\frac{CP_n}{2}$	Better route
3	$\frac{CP_n}{4}$	Bad route
4	0	Worst route

Case 2: The second case is that the total number of trustworthy nodes is half the total count of nodes along the path, as represented in eqn.7. This path can be chosen in the case of the non-existence of case 1. This path is the better path.

Case 3: This case come into picture when the total count of trustworthy nodes is quarter the total count of nodes exist in a path. This path is considered as bad.

Case 4: The final case is the worst case, in which the presence of trustworthy nodes along a path is completely nothing. This path must not be chosen at any cost and is considered as the worst route. This work does not support such path, even when it is the shortest path.

Algorithm

// Cluster formation
Input: $Set\ of\ nodes$
Output: Clusters
Begin
$max_n = 20$;
For every 30 seconds
Select a node randomly;
Encircle 20 nodes;
If ($max_n \leq 20$)*then*
Broadcast join request;
// Leader node election
For every node of a cluster
Do
Compute l_n;
Find the ID of node with greatest l_n;
Declare it as leader node;
Maintain tables R_LVL, SERV_ADV and NEGBR;
// On receiving Serv_Req
Check local memory for the existence of the service;
If present then
Respond to the Serv_req;
Else
Forward the Serv_req to the Negbr leader nodes;
Wait for response;
If positive response then
Respond to the Serv_req;
Else
Reject the Serv_req;
End;
// Service routing
Compute CT_n *and* CP_n *in a route;*
If $CT_n = CP_n$ *then*
Declare the route as best;
Else if $CT_n = \frac{CP_n}{2}$ *then*
Declare the route as better;
Else if $CT_n = \frac{CP_n}{4}$ *then*
Declare the route as bad;
Else
Declare the route as worst;
End;

The above presented algorithm describes the entire process of the work. The results of the work are satisfactory, as this work stems on trust mechanism. Trustworthy route improves the quality of service than when the trustworthy nodes are treated alone. Thus, this work focuses on both the trustworthy route and trustworthy nodes. The trustworthy route is dependent on the count of trustworthy nodes in that particular route.

5. EXPERIMENTAL ANALYSIS

The performance of TRPSD is analysed in terms of response time, throughput, energy consumption, quality of service and lifetime of the network. The experimental results of this work prove that the system works better than the scenario which considers trustworthy nodes alone.

i. Response time: Response time is the time it takes to respond to a service requesting node with a high quality service. The response time of any service must be as minimal as possible. Response time is calculated by the following equation and the results are shown in Figure-3.

$$res_{time} = sd_{time} - sr_{time} \quad (10)$$

Where sd_{time} is the service delivery time and sr_{time} is the service requesting time.

ii. Throughput: Throughput is the measure of successful service delivery within the network. A system with maximum throughput is preferable for efficient communication. Throughput is the total amount of data being transferred at a given period of time. Fig.4 shows the graphical results for throughput.

iii. Energy consumption: Energy consumption is calculated for achieving an operation successfully and is shown in Figure-5. Energy consumption is indirectly proportional to the lifetime of the network. It is measured in joules.

iv. Quality of Service: Quality of service must be the maximum and it can be achieved by incorporating certain parameters. The quality of service of the proposed work is presented in Figure-6.

v. Lifetime of the network: MANET is energy constrained and the lifetime of network is the major concern. The lifetime of the network must be the maximum. Figure-7 depicts the lifetime of the network.

The graphical results of all the above mentioned parameters are presented in the following Figures from 3-7.

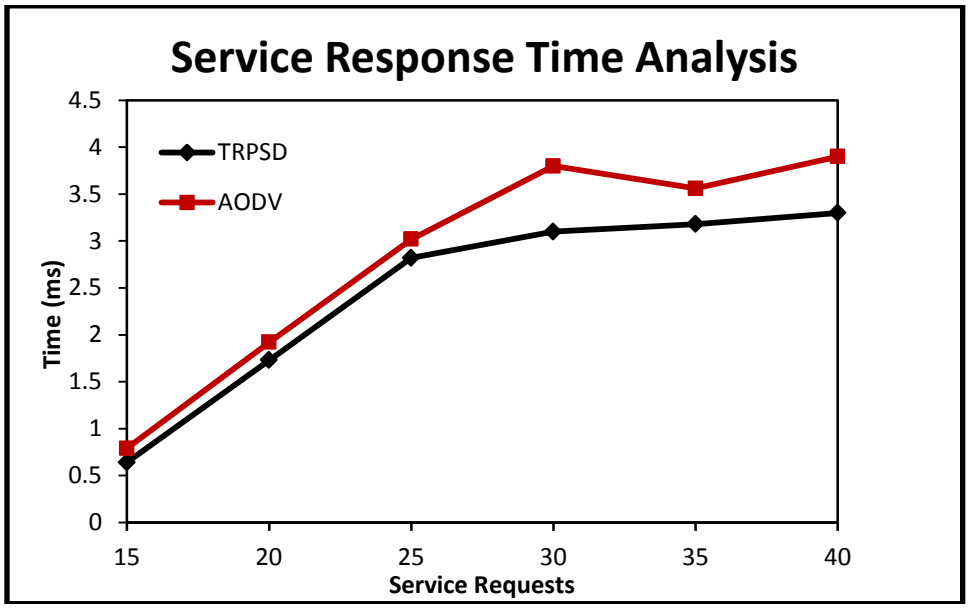

Figure-3. Service response time analysis.

From the results, it is evident that the service response time grows gradually with respect to the service request time. The maximum time is 3.3 milliseconds for 40 service requests.

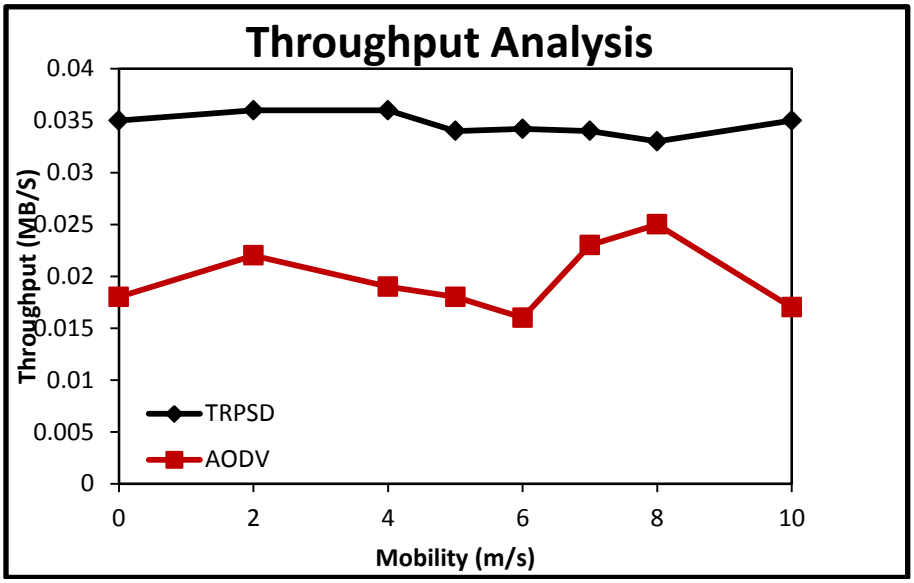

Figure-4. Throughput analysis.

The throughput of the proposed work is analysed with respect to the mobility of the nodes. The throughput of the system is satisfactory even when the mobility is increased to 10 m/sec.

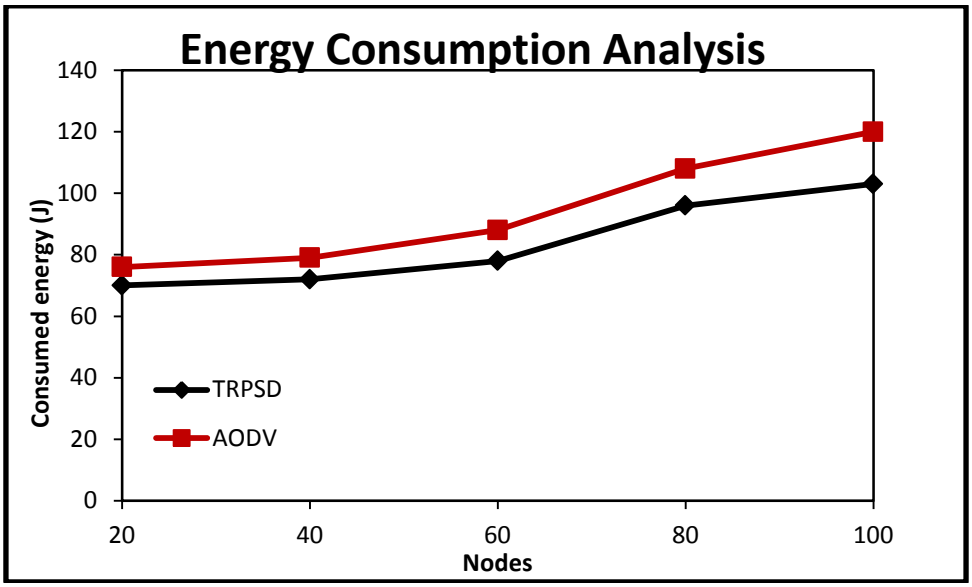

Figure-5. Energy consumption analysis.

The energy must be consumed in an effective way, such that the usability and the lifetime of the system are satisfactory. A system with ineffective energy utilization cannot serve the purpose for a longer period of time. On analysing the consumption of energy, it is concluded that the energy consumption pattern of this work is reasonable.

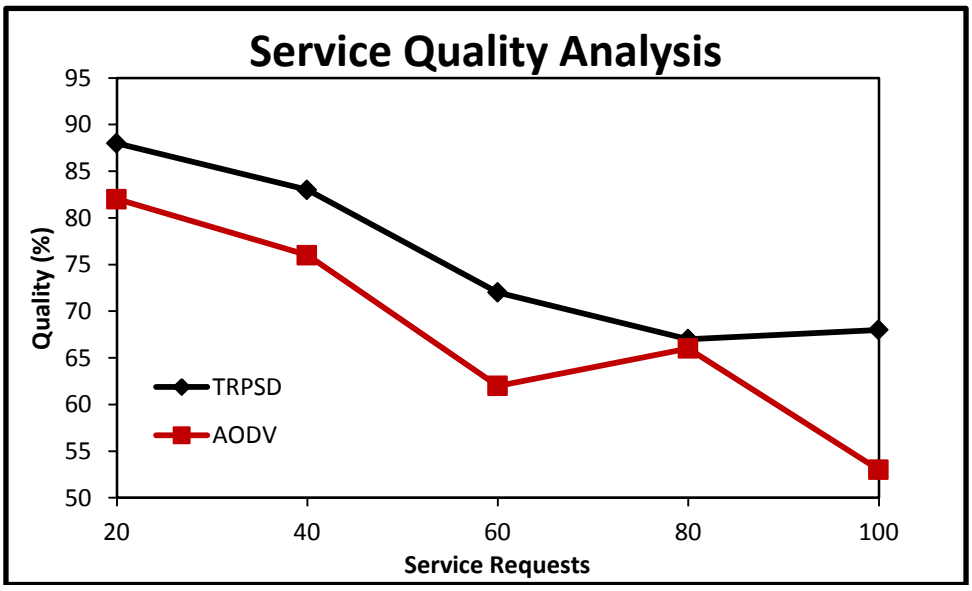

Figure-6. Service quality analysis.

The quality of the service is checked by increasing the number of service requests. Though, the proposed work works well with effective quality of service.

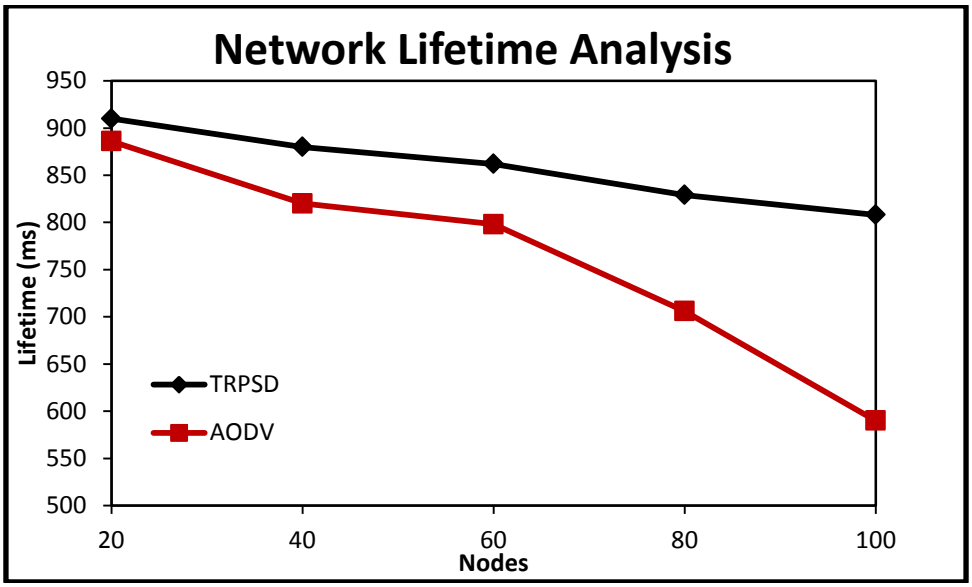

Figure-7. Network lifetime analysis.

The lifetime of the network is analysed with increasing number of nodes. The lifetime of the network is better, as the energy is effectively utilized. Besides this, clustering technique preserves more energy.

Thus, energy aware cluster based trustworthy service routing policy is designed and the results of this work are satisfactory.

6. CONCLUSIONS

This work proposes a trustworthy routing solution TRPSD, which is based on clustering technique for MANET. The possible routes are categorised on the basis of the count of trustworthy nodes along the path. The best route is selected such that this work weeds out delay and improves the quality of service. The response time taken by the system is extremely low. Besides this, the lifetime of the network is satisfactory which is very important for MANET.

REFERENCES

[1] Moussa Ayyash, Donald Ucci and Khaled Alzoubi. 2010. A Proactively Maintained Quality of Service Infrastructure for Wireless Mobile Ad Hoc Networks. International Journal of Communication Networks and Information Security (IJCNIS). 2(2).

[2] Lovdeep Grover, Lal Pratap Verma, and Aniket Mathuria. 2012. Comparison between SAR and NSAR in MANETs. International Journal of Data & Network Security. 1(1).

[3] Mamoun Hussein Mamoun. 2011. A New Reliable Routing Algorithm for MANET. International Journal of Research and Reviews in Computer Science (IJRRCS). 2(3).

[4] Zhenguo Gao, Ling Wang, Mei Yang and Xiaozong Yang. 2006. CNPGSDP: An efficient group-based service discovery protocol for MANETs. Elsevier, Computer Networks. pp. 3165-3182.

[5] Yuan Yuan and Ashok Agrawala. 2003. A Secure Service Discovery Protocol for MANET. 14th IEEE Proceedings on Personal, Indoor and Mobile Radio Communications, (PIMRC). 1: 502-506.

[6] L. Ramachandran, M. Kapoor, A. Sarkar and A. Aggarwal. 2002. Clustering Algorithms for Wireless Ad Hoc Networks. In Proceeding: Workshop on Discrete Algorithms and Methods for Mobile Computing and Communications, Boston. pp. 54-63.

[7] A.Ephremides, J. E. Wieselthier and D.J. Baker. 1987. A Design Concept for Reliable Mobile Radio Networks with Frequency Hopping Signaling. IEEE. pp. 56-73.

[8] M. Gerla and J.T. Tsai. 1995. Multicluster, Mobile, Multimedia Radio Network. Wireless Networks.

[9] S. Basagni. 1999. Distributed clustering for ad hoc networks.

[10] M. Chatterjee, S.K. Das, D. Turgut. 2002. WCA: A Weighted Clustering Algorithm for Mobile Ad Hoc Networks. 5(2): 193-204.

[11] W. Choi, M. Woo. 2006. A Distributed Weighted Clustering Algorithm for Mobile Ad Hoc Networks. Advanced International Conference on Telecommunications.

[12] C. R. Lin and M. Gerla. 1997. Adaptive Clustering for Mobile Wireless Networks. IEEE Journal on Selected Areas in Communications. 15(7): 1265-1275.

[13] A. Ramalingam, S. Subramani and k. Perumalsamy. 2002. Associativity-based Cluster Formation and Cluster Management in Ad Hoc Networks. HiPC.

[14] Johnson, D., Maltz, D. 1996. Dynamic source routing in ad hoc wireless networks. in Tomasz, I., Hank, K. (Eds.): 'Mobile computing' (Kluwer Academic Press, 1st edn.). pp. 153-181.

[15] Zapata, M.G., Asokan, N. 2002. Secure ad hoc on-demand distance vector routing. ACM Mobile Comput. Commun. Rev. 3(6): 106-107.

[16] Hu Y.C., Perrig A., Johnson D.B. 2002. Ariadne: a secure on-demand routing protocol for ad hoc networks. Proc. Int. Conf. Mobile Computing and Networking (Mobicom'02), Atlanta, Georgia. pp. 12-23.

[17] Jensen C.D., Connell P.O. 2006. Trust-based route selection in dynamic source routing. Proc. Int. Conf. on Trust Management, Pisa, Italy. pp. 150-163.

[18] Pirzada A.A., McDonald C., Datta A. 2006. Performance comparison of trust-based reactive routing protocols. IEEE Trans. Mobile Comput. 5(6): 695-710.

[19] Martin J., Manickam L., Shanmugavel S. 2007. Fuzzy based trusted ad hoc on-demand distance vector routing protocol for MANET. Adv. Comput. Commun. (ADCOM 2007). pp. 414-421.

[20] P. Michiardi and R. Molva. 2002. Core: A Collaborative Reputation mechanism to enforce node cooperation in Mobile Ad Hoc Networks. Communication and Multimedia Security Conference (CMS'02).

[21] Mouhannad ALATTAR, Franc¸oise SAILHAN, Julien BOURGEOIS. 2012. Trust-enabled Link Spoofing Detection in MANET. 32nd International Conference on Distributed Computing Systems Workshops. pp. 237-244.

[22] Alexander Oberle and Andr´e Rein, and Nicolai Kuntze and Carsten Rudolph, Janne Paatero and Andrew Lunn and Peter Racz. 2013. Integrating Trust Establishment into Routing Protocols of Today's MANETs. IEEE Wireless Communications and Networking Conference (WCNC): NETWORKS, pp. 2369-2374.

[23] Marcin Seredynski, Riad Aggoune, Krzysztof Szczypiorski and Djamel Khadraoui. 2013. Performance Evaluation of Trust-based Collaborative Sanctioning in MANETs. 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications. pp. 81-88.

[24] Shirin Bhanu Koduri, Dr. M. Seetha. 2015. Cluster based trustworthy service discovery scheme for MANET. International Journal of Applied Engineering Research. 10(13): 33132-33138.