International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223425 Volume 10, Issue 5, September – October (2023)

RESEARCH ARTICLE

Delay Aware Clustered Service Discovery Scheme Based on Trust for Mobile Ad Hoc Networks (MANET)

Prabu B
PG & Research Department of Computer Science, Karuppannan Mariappan College, Muthur, Tamil Nadu, India.
kmcprabuphd@gmail.com

G. Jagatheeshkumar
PG & Research Department of Computer Science, Karuppannan Mariappan College, Muthur, Tamil Nadu, India.
jagatheeshkumaar@gmail.com

Received: 25 July 2023 / Revised: 23 September 2023 / Accepted: 01 October 2023 / Published: 30 October 2023

Abstract – Service discovery is one of the most difficult aspects of MANETs. The primary concern is the assignment of the optimal service to the service requester. This work intends to address this issue by proposing a clustered trustworthy service discovery scheme. The Cluster Head (CH) node selection and recycling, $SERV_{AD}$, request, response and service ranking are the crucial phases of this work. The CH node is chosen by considering the trust parameters like mobility, energy and number of neighbors. The selected CH node calculates the level of trust for each of its member nodes by employing trust criteria such as energy consumption, packet forwarding ratio, and node behavior. The node responsible for requesting services delivers the $SERV_{Req}$ packet to the CH node, which thereafter searches its local memory for the corresponding service. Finally, the matching services are evaluated based on the distance of the service, the level of trust and the workload of the service provider. As significant metrics are considered for recommending service, the service requester is assured with reliable and faster service provisioning, which is proven by the experimental results.

Index Terms – MANET, Service Discovery, Service Provision, Service Ranking, Trust, Energy Efficiency.

1. INTRODUCTION

Mobile Ad hoc Networks (MANET) have recently received considerable attention due to its low cost, scalability, and adaptability. MANET nodes possess the characteristic of mobility and operate independently from any fixed infrastructure, hence resulting in the absence of a centralized authority. This characteristic of MANET has both advantages and disadvantages. Location independence and scalability are the primary benefits of MANET's infrastructure-free nature [1-3].

Complexity in routing and security concerns are, on the other side, a major concern related with this point. In addition, mobile nodes have limited energy or battery backup, as well as an unstable architecture. The communication method between nodes is determined by the forward range of the nodes. If the forward range of any two nodes remains the same, data can be transmitted directly. When the forward range of the nodes is different, transmission of data between nodes may require the assistance of intermediary nodes [4-6].

1.1. Problem Statement

MANET is centered on exchanging data and utilizing the services of other participating nodes. Thus, a system is required to manage the transmission of service packets, $SERV_{AD}$, service selection, etc. Service discovery protocol is therefore required for the automatic detection of services provided by mobile nodes. The process of service discovery permits nodes to inquire about the services supported by other nodes, to list the services supported by the node itself (advertisement), and to choose and contact the appropriate service. However, achieving this task is difficult due to the node's movement and consequent frequent disconnection.

Service discovery is a distinct topic of research in MANET that aims to provide the service requester with the optimal service. Service, service requester and provider are the fundamental terms of service discovery. A service is the software or hardware function that enables a node to complete specific tasks or make life easier. The service provider is the entity that furnishes services to the service requester. The entity that requests a service from other nodes is referred to as the service requester [7].

A service-requesting node generates and forwards a $SERV_{Req}$ packet. When $SERV_{Req}$ is received, the node checks for the requested service. If the service sought and service provided matches, the service provider sends a $SERV_{Res}$ packet in

RESEARCH ARTICLE

response. The primary objective of a service discovery protocol in a MANET is to properly detect services in a dynamic environment. This study proposes an energy efficient clustered service discovery scheme for MANET that emphasizes service quality. This makes sense that the nature of service providing node is considered for effective service allocation. A clustered technique is used to conserve energy [8-10].

This entire work is divided into five phases: selection and recycling of Cluster Head node (CH), $SERV_{AD}$, $SERV_{Req}$, $SERV_{Res}$ and service routing. By means of $SERV_{AD}$ and $SERV_{Req}$ packets, the nature of the service-providing node and the expectations of the service-requesting node are transmitted. Utilizing the quality of service characteristics, the optimal service is thereby allocated to the service-requesting node. The major contributions of this work are as follows.

- A clustered trustworthy service discovery scheme is presented to make service accessibility better.
- The service is chosen on the basis of trust score, workload and the distance, which assures better Quality of Service (QoS).
- Energy is conserved, owing to the optimal choice of service and clustering concepts.

The remaining sections of this work are structured as follows. Section 2 contains a comprehensive overview of service discovery procedures. In section 3, the recommended approach is presented. In part 4, the performance of the proposed work is evaluated and experimental outcomes are provided. The conclusion is provided in section 5.

2. REVIEW OF LITERATURE

This section discusses the existing works concerning trust and energy efficiency in MANET. The solution proposed by the authors in reference [11] utilizes fuzzy logic and trust as a mechanism to enhance the security of MANETs and mitigate vulnerabilities associated with attacks. Due to the inherent decentralized structure of Mobile Ad hoc Networks (MANETs), scholars have identified a multitude of vulnerabilities that render them susceptible to various forms of attacks. Consequently, ensuring a robust degree of trust becomes imperative in such networks. The reliability of the proposed model is ascertained by the amalgamation of two distinct perspectives, with its quantifiable measure ranging from 0 to 1. The aim of this work is to mitigate the adverse consequences of vampire attacks, ultimately leading to an enhancement in its overall efficacy. The study involves a comparative analysis between the proposed model and an existing trust model, with a focus on evaluating the effectiveness of the proposed model in identifying malicious nodes. This evaluation is conducted using three key parameters: precision, recall, and communication overhead.

It is generally agreed that the use of sensor nodes is the most effective way to collect data from difficult-to-reach and potentially dangerous regions, such as civil and military zones. Because the radio transceiver uses a substantially higher amount of power than the hardware components, the limitation on available energy is the most significant problem with sensor nodes. Therefore, the use of routing algorithms that have lower energy consumption is an absolute necessity for the long-term longevity of the network lifeline.

The authors of the article [12] developed three measures that are linked to energy optimization. These metrics are the degree to which a node is close to the shortest route, the degree to which a node is close to a sink through a single hop or multiple hops, and the degree to which energy is balanced. The values of these parameters are entered into an algorithm for fuzzy logic-based routing in order to maximize energy, hence rising the network's lifetime and making it easier for sensor nodes to exchange data with one another. Coverage and connectivity are seen as being absolutely necessary for the transfer of data from the target region to the BS in a target-based WSN. The challenge, however, is in the placement of sensor nodes in the most advantageous locations so as to guarantee coverage and connectivity.

The authors of [13] introduced a solution to this NP-complete problem by using the Genetic Algorithm (GA). This research makes use of an evolutionary algorithm (GA) that takes into account proper chromosome representation, the formulation of a fitness function, and operations like selection, crossover, and mutation. The findings illustrate that the method proposed has a more manageable level of temporal complexity in comparison to existing GA-based algorithms. The process of localization, also known as accurately locating the sensor nodes, is an important challenge for WSN. A high level of precision is required in order for there to be effective data transfer between sensor nodes.

The authors of the paper [14] propose a localization algorithm that makes use of fuzzy logic. The weighted centroid localization technique, which determines the location of unknown nodes using inference systems such as Fuzzy Mamdani and Sugeno, is the foundation for the proposed algorithm. It is also the name of the technique. Next-hop CH is selected after an accurate determination of the positions of the sensor nodes. This decreases the amount of energy that is wasted and increases the sensor nodes' lifetime.

The authors of this study [15] devised a heuristic and distributed route that uses a new methodology to improve the QoS need for MANETs. This route was included in their research. The learning method known as Reinforcement Learning (RL) is combined with a distributed algorithm for route finding. The findings of the suggested technique demonstrate that network performance has been boosted by optimizing timeliness, effectiveness, and efficiency. This is in

RESEARCH ARTICLE

comparison to the usual methodology, which did not produce these findings.

The authors of [16] have placed a strong emphasis on the utilization of RL in order to achieve adaptive routing in MANETs. The authors have decided to use multiple Markov Decision Processes (MDP) in order to provide an explicit formalization of the routing problem so that the research may move further. The authors of [17] presented a proposal for an intelligent routing control system for MANET with RL. By engaging with the surrounding environment and providing optimal transmission pathway coverage, the technology that is being used has the potential to optimize the selection strategy of nodes. The results demonstrate that, in contrast to earlier algorithms, the proposed algorithm is able to identify an acceptable path under constrained conditions and achieve superior optimization targets. This is indicated by the fact that the proposed approach achieved the best optimization targets.

The authors of the work [18] used the attributes to correlate permanence with route length. RL was used to propose a method to choose among the neighbors to forward the packet to its destination at any time. The authors of the work [19] anticipate the pattern of behavior exhibited by the nodes in conjunction with the node by making use of RL. The results illustrate that the strategy that was proposed is superior to the MANET routing models.

An intelligent routing protocol with biobjective was proposed in the study [20] with the purpose of lowering a predicted long-run cost function that was comprised of an end-to-end delay as well as the pathway energy cost. The goal of the protocol was to reduce this cost function. In order to achieve this goal, a method based on multiagent RL has been created. This approach can estimate the optimal routing strategy even when there are no system data available. According to the results of the research, the model-based technique is superior to model-free alternatives and comes close to the conventional value iteration, which presupposes that statistics are flawless.

In [21], a work is presented for increasing the level of trust that exists within the MANET. The methodology for the investigation was based on something called the RL Trust Manager (RLTM). The results showed that the resulting RL is very accurate when assessing trust levels based on assumptions, and this was proved by the findings. Motivated by these existing works, this research work intends to present an energy efficient service discovery approach, which can effectively function with minimal energy requirement, while ensuring better QoS.

3. PROPOSED ENERGY EFFICIENT SERVICE DISCOVERY APPROACH BASED ON TRUST

The main objective of this study is to provide the client with the highest quality service available. There are a multitude of approaches for effectively aligning the service requester with the service provider who can deliver the highest quality service. This study employs a trust-based approach to allocate the most suitable service to the service requester. The determination of node types is based on the calculation of trust levels, which takes into account several trust attributes before allocating the service. Figure 1 illustrates the comprehensive flow of the proposed study.

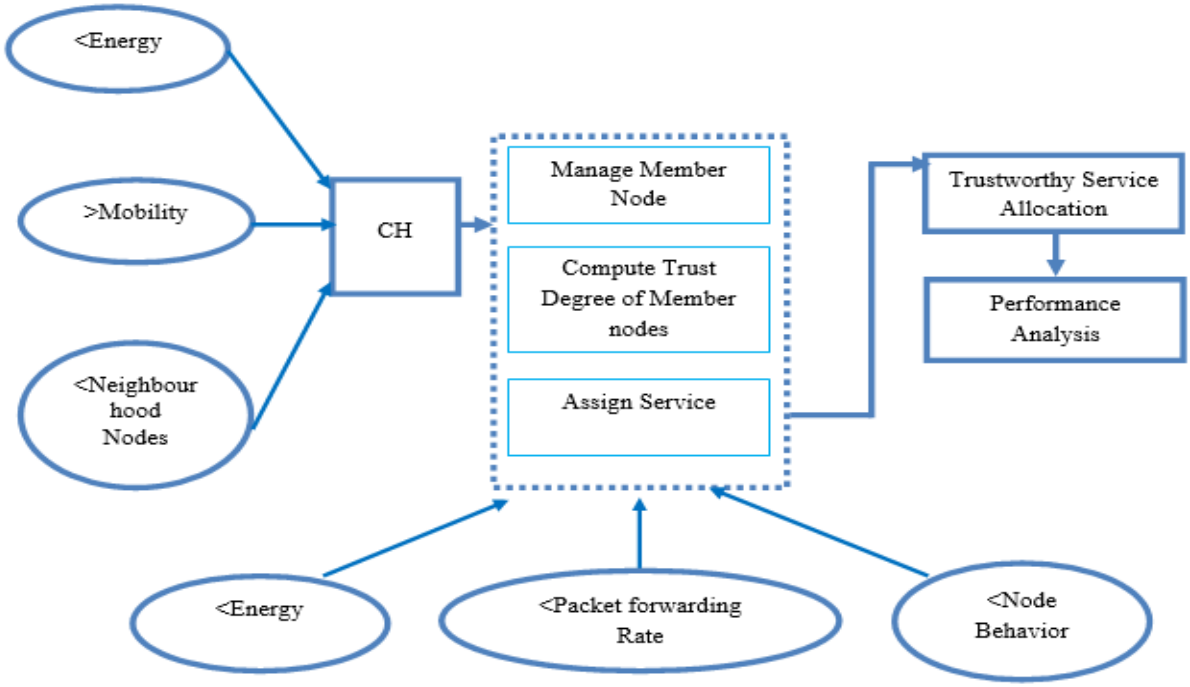

Figure 1 Overall Flow of the Work

RESEARCH ARTICLE

This section presents the work overview and the proposed work is elaborated in the forthcoming sub-sections. The complete work is divided into five phases: selection and recycling of CH nodes, $SERV_{AD}$, $SERV_{Req}$, $SERV_{Res}$ and service routing.

- CH Selection and Recycling:

A cluster's head node, known as the CH node, is responsible for managing the operation of all of the cluster's member nodes (CM). This node needs to be able to provide efficient management for the other nodes in the network. As a result, there is a need for a mechanism that can determine which CH node is the best. On the other hand, for saving energy and avoiding the resource wastage, a single CH node should not be kept active for an excessive amount of time.

- Service Advertisement

The procedure of informing CM nodes about the services provided by other nodes is known as the notification process. This $SERV_{AD}$ packet contains information on the services offered by the node, as well as the node's location, degree of trustworthiness, and average response time.

- Service Request

The node that requires a service sends the $SERV_{Req}$. The $SERV_{Req}$ is initially sent to the CH node. The $SERV_{Req}$ packet includes things such as the required service, the workload of the node, energy, CPU speed and memory.

- Service Response

The $SERV_{Res}$ is transmitted to the service requesting node. The $SERV_{Res}$ packet includes entities such as degree of trust, service being provided, average response time, service distance, workload and energy.

- Service Routing

After the receipt of a $SERV_{Res}$ packets, they undergo a sorting process in which they are arranged in ascending order according to the average response time, distance, and workload priorities. The characteristics, such as the degree of confidence and energy, are arranged in a descending order to ascertain the most favorable service, which is afterwards delivered to the service requester.

3.1. CH Node Selection

Selection of the CH node is a crucial step, since the CH node must be capable of handling all of the CM nodes. This paper presents a technique for selecting CH nodes based on the trust metrics such as energy ($\mathcal{E}$), mobility ($\mathbb{M}$), and neighbor count ($\mathcal{N}$), which are explained below. This study examines the node's energy as it degrades with regard to time. The consideration of mobility is essential as a node with high mobility may not be capable of effectively performing its designated functions. Consideration is given to the number of surrounding neighbors, as a node with a large number of neighbors is best suited to serve as CH.

The determination of the CH node is based on the sorting of the parameter values of energy, mobility, and neighbour count. In this study, it has been shown that the most number of CM nodes connected to a CH node, is seven. The rationale behind the aforementioned claim is that the quantity of nodes exhibits a direct correlation with the effective management of the cluster. The arrangement is conducted in a decreasing order. Consequently, all these parameters are considered while selecting a CH node, as represented in following equation (1).

$$CH = \mathcal{E} + \mathbb{M} + \mathcal{N} \quad (1)$$

By adhering to the above criteria, the ideal CH node is chosen. However, because nodes are mobile, their values vary often. Thus, the values are evaluated every minute, in order to preserve the best node as the CH node. It is not advisable to keep the same node as the CH node for an extended period of time due to excessive energy consumption. The overall algorithm of this work is presented in algorithm 1. Hence, the CH node is recycled for every time period.

Input : Sensor nodes

Output : Trustworthy service allocation

Begin

//Clustering

For every forty seconds

Select a random node and encircle 7 neighbourhood nodes;

Compute CH;

Declare the node with greatest CH as cluster head;

CH computes TV′;

Store it in local memory;

// Service request

For every request

CH checks the service availability;

Rank the available service and respond the requester;

End

Algorithm 1 Proposed Service Discovery Algorithm

3.2. CH Node Recycling

Due to the mobility of nodes and in an effort to conserve energy, the CH node is renewed each time interval and is referred to as CH node recycling. This recycling process is required for efficient energy consumption. In every mobile

RESEARCH ARTICLE

network, node energy is rapidly exhausted and so, maximum energy conservation is necessary.

Utilizing the concept of clustering, emphasis is placed on energy conservation in this work. The inclusion of CH node recycling serves as a preventive measure against the depletion of energy within the node. When a network optimizes energy conservation to the greatest extent possible, it results in an increase in its durability. This study imposes a constraint on the maximum number of nodes that can be present below a CH node, limiting it to a maximum of seven. This number is selected to improve node management and conserve energy on the CH node. Hence, a maximum of seven nodes is encircled. In order to ascertain the value of CH, many aspects pertaining to CH node selection, including energy, mobility, and the quantity of surrounding nodes, are calculated. The node possessing the greatest value is designated as the CH node. This procedure is done every minute to conserve energy on the CH node. Additionally, the mobility of the nodes necessitates the immediate election of the major node.

3.3. Trust Metrics and Trust Degree Computation

This section discusses the trust metrics that are employed for the choice of CH node and the trust score computation of CM nodes for service provisioning.

3.3.1. Energy ($\mathcal{E}$)

All nodes in a MANET are energy restricted. Therefore, the existing energy must be utilized effectively. A CH node is employed to preserve energy and ensure proper management. Here, energy is included as one of the criteria for picking a CH node, as a node with insufficient energy cannot fulfill its function, as indicated in the equation (2).

$$\mathcal{E} = \begin{cases} 1; \text{Full energy} \\ 0.5; \text{Partial energy} \\ 0; \text{No energy} \end{cases} \quad (2)$$

The value of this option varies between 0 and 1. A node that possesses complete energy is designated as 1, whereas a node that lacks energy is assigned the value 0. The assigned value of this variable spans a continuum from 0 to 1, reflecting its quantitative representation of energy magnitude.

3.3.2. Mobility ($\mathbb{M}$)

The mobility of nodes is taken into consideration, since a steady node has the potential to provide more effective service compared to a dynamic node. Each individual node is observed for a designated duration, during which its level of mobility is quantified using a numerical value ranging from 0 to 1, as denoted in equation (3).

$$\mathbb{M} = \begin{cases} 1; \text{Steady} \\ 0.5; \text{Min movement} \\ 0; \text{Max movement} \end{cases} \quad (3)$$

If the node is very mobile, it is assigned a value of 0. In the event that the node is steady with minimal movement, its mobility value is 1. Similarly, the mobility of nodes is assigned a value between 0 and 1 on a scale from 0 to 1. Therefore, the node with the value 1 is vastly preferred.

3.3.3. Neighborhood Nodes($\mathcal{N}$)

A node is considered to be in a healthy state when it possesses a substantial quantity of adjacent nodes. The selection of a CH node is most favorable when it is surrounded by multiple adjacent nodes. The node that possesses the highest number of neighbors is sometimes referred to as "fat," while a node is deemed "thin" when it exhibits a relatively low number of neighbors, as denoted in equation (4).

$$\mathcal{N} = \begin{cases} 1; \text{More neighbours} \\ 0.5; \text{Min neighbours} \\ 0; \text{No neighbours} \end{cases} \quad (4)$$

The nodes are arranged in a descending order based on the quantity of neighboring nodes. The node exhibiting the highest score is considered the most optimal option for the CH node. The node possessing a rank of 1 exhibits a higher number of neighboring nodes, while the node with a rank of 0 lacks any neighboring nodes.

3.3.4. Packet Forwarding Ratio ($\mathcal{P}$)

$\mathcal{P}$ is an additional crucial factor that determines the character of a node. The intention behind introducing this parameter is to establish the packet forwarding ratio by comparing the number of incoming and exiting packets. Three cases are discussed concerning the packet in and outflow. In the first case, the pace of incoming ($\mathcal{I}$) and outgoing ($\mathcal{O}$) packets matches with each other, which proves the packet forwarding ability of the node, as shown in the equation (5).

$$\mathcal{P} = \begin{cases} 1(\mathcal{I} = \mathcal{O}) \\ 0.5\ (\mathcal{I} = \frac{\mathcal{O}}{2}) \\ 0(\mathcal{O} = 0) \end{cases} \quad (5)$$

In the second case, the node shows less interest in packet transmission, such that partial packets alone are forwarded, as represented in eqn.4. In the third case, the node completely denies packet transmission and the outgoing packet rate is nil, as given in eqn.5. Out of all the three cases, case one highly preferable, as the node is considered trustworthy.

3.3.5. Node's Behaviour (в)

The behavior of each node is monitored over a predetermined time interval. The nodes have the potential to partake in several undesired actions, such as the deliberate deletion and manipulation of packets. The monitoring of node behavior is conducted by the CH node, which also governs the behavior of the nodes, as expressed in equation (6).

RESEARCH ARTICLE

$$\text{B} = \begin{cases} 1; \text{Normal} \\ 0.5; \text{Suspicious} \\ 0; \text{Malicious} \end{cases} \quad (6)$$

A node is considered trustworthy and assigned a value of 1 if it does not engage in malicious activities such as changing or deleting packets. A node will receive a grade of 0 if it deletes any of the packets it receives and manipulates the content of the incoming packet.

3.3.6. Trust Degree Computation

The trust level of the CM nodes is determined through the evaluation of trust measures, including E, P, and B. The trust degree of the nodes is computed by the CH node by the aggregation of many trust attributes, including energy, in-out ratio, and behavior. The mean value is determined by adding all of these values together, as shown in equation (7).

$$\text{TD} = \sum_{i=0}^{6} \frac{\mathcal{E}+\mathcal{P}+\text{B}}{3} \quad (7)$$

As a result, the node possessing a trust degree of 1 can be identified as the reliable node, while the node with a trust degree of 0 can be classified as the malicious node. Thus, the CH node determines and stores the trust level of all other nodes in its internal memory. The degree of trust is not stable; therefore, the CH node calculates the trust value of all participating nodes every minute.

3.4. SERV_{AD}

The process of notifying other nodes of the services provided by a node is known as SERV_{AD}. This SERV_{AD} packet includes the service, trust value, its location, and the average response time. This packet of SERV_{AD} is sent to the CH node. The CH nodes store service advertising in their local memory and update them at regular intervals in order to properly manage the delivery of services.

3.5. Service Request (SERV_{Req})

The node requiring a particular service sends a SERV_{Req} to the CH node. The packet containing the SERV_{Req} is transmitted to the CH node, which then searches its local memory. The SERV_{Res} packet involves the entities such as required service, CPU speed, node energy, node's workload and node memory. Two cases are related with this. In the local memory, presence and lack of service exist.

Case 1: The CH node compares the requested service to the list of available services (SERV_{AD}). If the CH node discovers a match, the CM node can provide service to another CM node. This scenario results in significant time and labor savings.

Case 2: In the event that the CH node is unable to locate a suitable match for the requested service inside its local memory, the SERV_{Req} is disseminated to all CH nodes present in the network. After successfully SERV_{Req} packets, CH nodes await SERV_{Res} packets.

3.6. Service Response (SERV_{Res})

When the requested service is available in any of the CH nodes, the matching CH node responds to the sending CH node. The SERV_{Res} packet contains the provided service, service location, average response time, degree of trust and the workload. The SERV_{Res} packet is transmitted by the CH node in response to the CH node that requested its services. As the offered services are graded according to their level of trust, the scheme's security is ensured. The trust score of a node makes it simple to identify malicious nodes, hence enhancing network security.

3.7. Service Ranking

The CH node has the capability to offer services to its member nodes through two distinct methods. In the initial scenario, the requested service is stored within the local memory of the CH. In the present scenario, the provision of the service can be conveniently facilitated to the node making the request. In the second situation, if the requested service is not found in the local memory, the CH node proceeds to transmit the SERV_{Req} to all other CH nodes. Nevertheless, it is possible for many nodes to offer the requested service.

As a result, the CH node that is being asked receives several SERV_{Res} packets from various CH nodes. On the other hand, the indigenous CH node may encompass numerous nodes that offer the required service.In the given case, the assessment of the mentioned services is conducted by considering factors such as proximity, reliability, and the average duration of response. Let us consider a hypothetical situation where the desired service is stored within the local memory of the CH node. In the present scenario, the determination of service rating is accomplished through an examination of the degree of trustworthiness and the customary duration of response. The proximity between the nodes involved in the service exchange inside a cluster renders distance irrelevant. Hence, the most viable service is allocated to the requester node, and the evaluation of its performance will be conducted in the following section.

4. PERFORMANCE ANALYSIS

The performance of the proposed work is evaluated on a standalone computer with 8 GB of RAM, and the work is simulated in the MATLAB 2015a environment. The performance of the proposed task is evaluated using standard performance metrics such as precision ($\mathcal{PR}$), recall ($\boldsymbol{\mathcal{RC}}$), F-measure ($\boldsymbol{\mathcal{FM}}$) and time consumption. The performance of the proposed method is compared to that of existing methods such as the SSD, Cache, QoS. The simulation parameters are presented in Table 1.

International Journal of Computer Networks and Applications (IJCNA)
DOI: 10.22247/ijcna/2023/223425 Volume 10, Issue 5, September – October (2023)

RESEARCH ARTICLE

Table 1 Simulation Parameters

Simulation Parameters	Value
Simulation Time	250 sec
Dimension	$1000m \times 1000m$
Node count	30
Mobility Model	Random waypoint
Traffic Nature	Constant Bit Rate
Transmission Radius	250 m
Packet Size	512 bytes

Considered performance parameters include $True_{Positive}$ (TRP), $True_{Negative}$ (TRN), $False_{Positive}$ (FAP), and $False_{Negative}$ (FAN) rates. The $\mathcal{PR}$ is determined by dividing TRP by the total of TRP and FAP. Indirectly, the $\mathcal{PR}$ is related to the FAP rates. Likewise, $\boldsymbol{\mathcal{RC}}$ rates are derived from FAN rates. Therefore, when FAN rates are low, $\boldsymbol{\mathcal{RC}}$ rates improve. $\mathcal{PR}$ and $\boldsymbol{\mathcal{RC}}$ rates are utilized to determine the $\boldsymbol{\mathcal{FM}}$ value. Following are the formula for computing $\mathcal{PR}, \mathcal{RC}$ and $\boldsymbol{\mathcal{FM}}$ rates from below equations (8 – 10).

$$\mathcal{PR} = \frac{TRP}{TRP+FAP} \quad (8)$$

$$\mathcal{RC} = \frac{\text{TRP}}{\text{TRP+FAN}} \quad (9)$$

$$\mathcal{FM} = \frac{2(\mathcal{PR}\times\mathcal{RC})}{\mathcal{PR}+\mathcal{RC}} \quad (10)$$

When the $\mathcal{PR}$ and $\mathcal{RC}$ rates are higher, the FAP and FAN rates are presumably low. In this instance, FAP rates indicate that the node is recommended untrustworthy services. Consequently, a superior service discovery system must demonstrate improved $\mathcal{PR}$ and $\mathcal{RC}$ rates. By adjusting the number of nodes, the performance of the suggested method is examined and the experimental results of the proposed work are shown below.

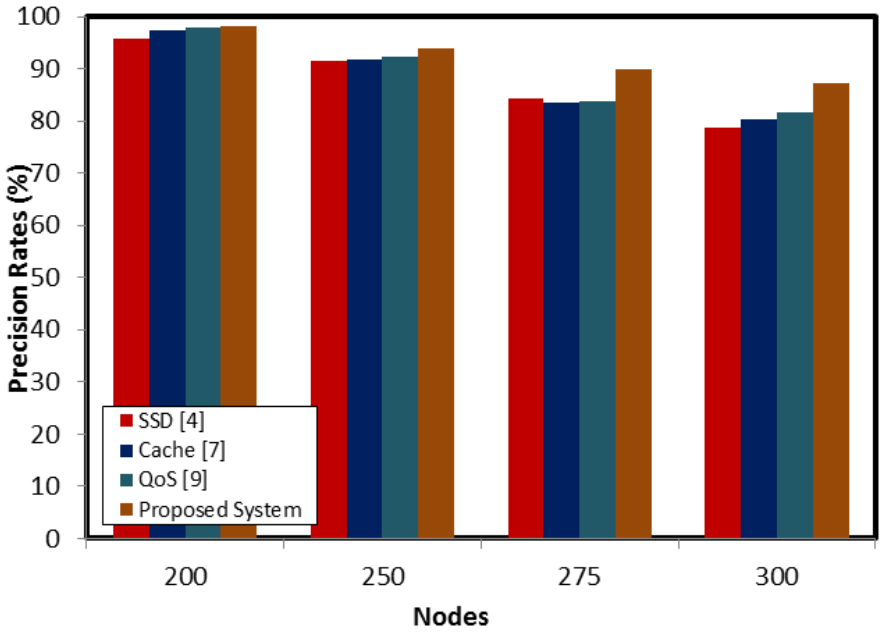

Figure 2 Comparison of $\mathcal{PR}$ Rate

Figure 2 makes it clear that the work has provided shows higher performance when compared to other existing strategies. The suggested method takes into account effective trust metrics for determining the degree and suggests the most trustworthy service that is currently available at any given time. This is the key reason for why the proposed method has better $\mathcal{PR}$ rates. The technique of clustering also makes it easier to manage the individual nodes that make up the cluster. Figure 3 provides an illustration of the $\mathcal{RC}$ rates obtained from the suggested work.

The $\mathcal{RC}$ rate of the study appears to be higher than that of previous approaches, indicating that the FAN rates of the suggested method are low. This indicates that the proposed method has not determined the matching services to be unreliable. This is required for any service discovery strategy to guarantee that nodes are always offered secure services.

Evidently, as the system's $\mathcal{PR}$ and $\mathcal{RC}$ rates improve, so does its $\mathcal{FM}$ rate. As the suggested method exhibits greater $\mathcal{PR}$ and $\mathcal{RC}$ rates, its $\mathcal{FM}$ rates are obviously greater than those of

RESEARCH ARTICLE

existing methods, as shown in figure 4. The greater the $\mathcal{FM}$, the more efficient the service discovery provided by the suggested task. In addition, the proposed solution combines the notion of trust by providing the nodes with the finest service possible.

The proposed task requires a decent amount of time to identify service providers, as shown in figure 5. Due to the incorporation of the clustering concept, time consumption has been decreased. This concept makes the proposed work time-effective. The shown data is the average execution timings of ten distinct executions.

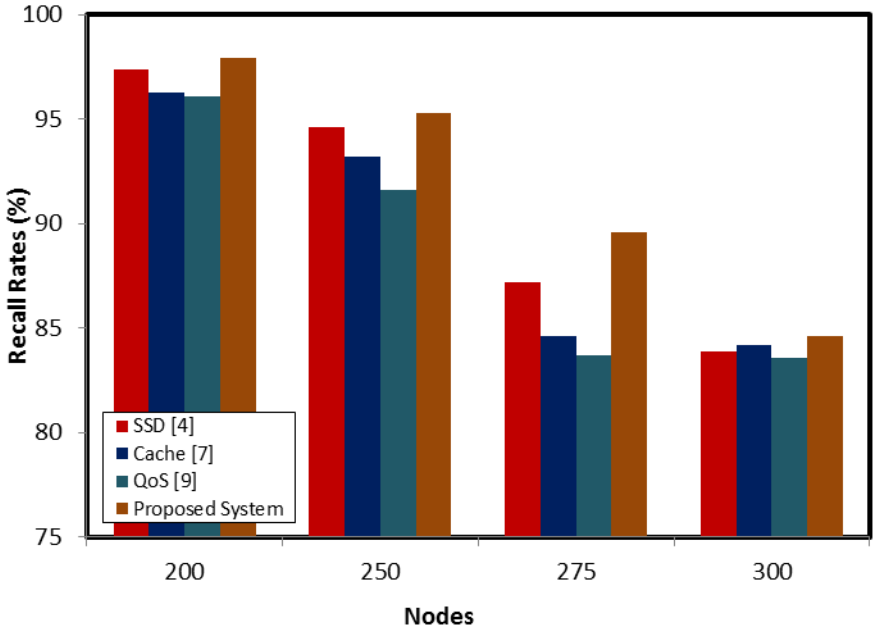

Figure 3 $\mathcal{RC}$ Rate Comparison

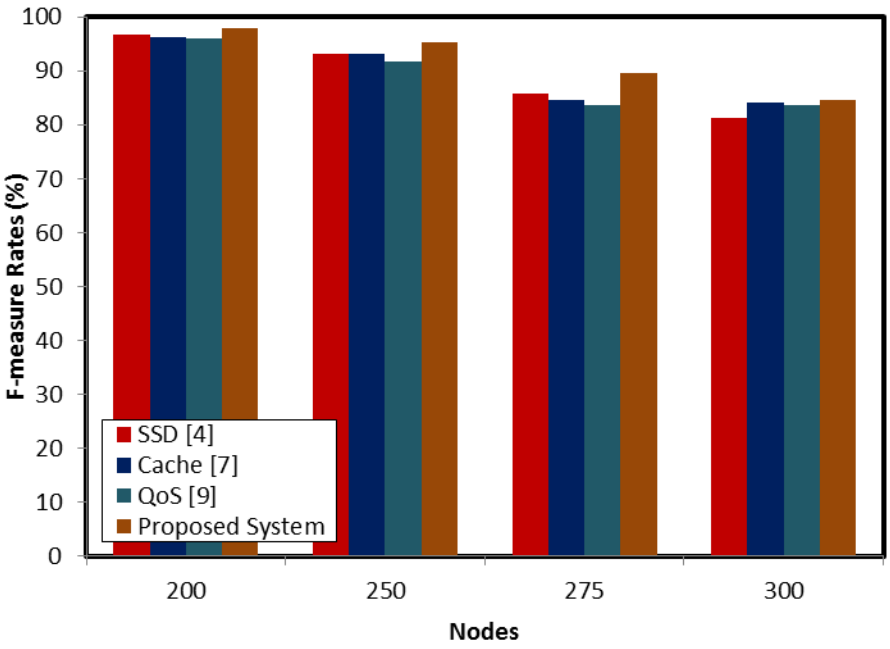

Figure 4 $\mathcal{FM}$ Rate Analysis

RESEARCH ARTICLE

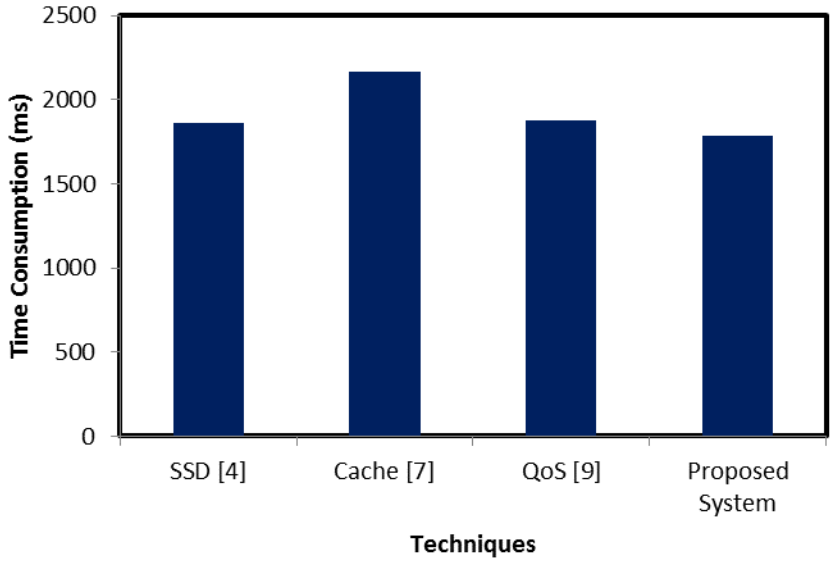

Figure 5 Time Consumption Analysis

5. CONCLUSIONS

This paper offers a clustered trustworthy service discovery scheme, which is based on different phases such as selection and recycling of CH, $SERV_{AD}$, request, response, and service ranking. The CH node is picked based on its energy, mobility, and number of neighbors. When a node receives $SERV_{Req}$ packet, it recommends the optimal available service by considering the distance, degree of trust and workload through service ranking. In future, this work aims to focus on secure service routing by employing the notion of trust.

REFERENCES

[1] N. Veeraiah and B. Tirumala Krishna, "Trust-aware fuzzyclus-fuzzy NB: Intrusion detection scheme based on fuzzy clustering and Bayesian rule", Wireless Netw., vol. 25, pp. 4021–4035, Jan. 2019, doi: 10.1007/s11276-018-01933-0.

[2] N. Veeraiah, ''A comparative analysis of energy efficient multipath routing in MANET,'' J. Adv. Res. Dyn. Control Syst., vol. 12, no. 3, pp. 261–267, Mar. 2020.

[3] Quy, V. K., Nam, V. H., Linh, D. M., Ban, N. T., & Han, N. D. (2021). A survey of QoS-aware routing protocols for the MANET-WSN convergence scenarios in IoT networks. Wireless Personal Communications, 120(1), 49-62.

[4] Kurian, S., & Ramasamy, L. (2021). Securing Service Discovery from Denial of Service Attack in Mobile Ad Hoc Network (MANET). International Journal of Computer Networks and Applications, 8(5), 619-633.

[5] Islam, N. (2019, December). A secure service discovery scheme for mobile ad hoc network using artificial deep neural network. In 2019 International Conference on Frontiers of Information Technology (FIT) (pp. 133-1335). IEEE.

[6] Veeresh, P., Praveen Sam, R., & Shoba Bindhu, C. (2018). Energy Constraint Service Discovery and Composition in Mobile Ad Hoc Networks. In Proceedings of the Second International Conference on Computational Intelligence and Informatics (pp. 175-187). Springer, Singapore.

[7] Jayapal, C., Jayavel, S., & Sumathi, V. P. (2018). Enhanced service discovery protocol for MANET by effective cache management. Wireless Personal Communications, 103(2), 1517-1533.

[8] Ramalingam, R., Muniyan, R., Dumka, A., Singh, D. P., Mohamed, H. G., Singh, R., ... & Noya, I. D. (2022). Routing Protocol for MANET Based on QoS-Aware Service Composition with Dynamic Secured Broker Selection. Electronics, 11(17), 2637.

[9] J. Manoranjini, A. Chandrasekar and S. Jothi, "Improved QoS and avoidance of black hole attacks in MANET using trust detection framework", Automatika, vol.60, no. 3, pp. 274-284, 2019. [Online]. https://doi.org/10.1080/00051144.2019.1576965.

[10] Setijadi, E., Purnama, I. K. E., & Purnomo, M. H. (2019, September). Analysis of reactive routing protocols in MANET based on quality of service. In 2019 International Seminar on Application for Technology of Information and Communication (iSemantic) (pp. 342-345). IEEE.

[11] R. Popli, V. Juneja, K. Garg, and D. V. Gupta, "Fuzzy based trust evaluation models for enhancing security in MANETs," International Journal of Engineering and Advanced Technology (IJEAT), vol. 8, no. 5, pp. 506–510, 2019.

[12] H. Jiang, Y. Sun, R. Sun, and H. Xu, "Fuzzy-logic-based energy optimized routing for wireless sensor networks," International Journal of Distributed Sensor Networks, vol. 9, no. 8, 2013.

[13] S. K. Gupta, P. Kuila, and P. K. Jana, "Genetic algorithm approach for k-coverage and m-connected node placement in target based wireless sensor networks," Computers and Electrical Engineering, vol. 56, pp. 544–556, 2016.

[14] S. Amri, F. Khelifi, A. Bradai, A. Rachedi, M. L. Kaddachi, and M. Atri, "A new fuzzy logic based node localization mechanism for wireless sensor networks," Future Generation Computer Systems, vol. 93, pp. 799–813, 2019.

[15] Kumanan, T., & Duraiswamy, K. (2010, February). Reinforcement learning for quality of service in mobile ad hoc network (MANET). In Proceedings of the 12th international conference on Networking, VLSI and signal processing (pp. 250-257).

[16] S. Chettibi and S. Chikhi, "Routing in mobile ad-hoc networks as a reinforcement learning task," in Networked Digital Technologies. NDT 2011. Communications in Computer and Information Science, S. Fong, Ed., vol. 136, Springer, Berlin, Heidelberg, 2011.

RESEARCH ARTICLE

[17] F. Dong, O. Li, and M. Tong, "Intelligent routing control for MANET based on reinforcement learning," MATEC Web of Conferences, vol. 232, article 04002, 2018.
[18] A. Ghaffari, "Real-time routing algorithm for mobile ad hoc networks using reinforcement learning and heuristic algorithms," Wireless Networks, vol. 23, no. 3, pp. 703–714, 2017.
[19] M. Maleki, V. Hakami, and M. Dehghan, "A model-based reinforcement learning algorithm for routing in energy harvesting mobile ad-hoc networks," Wireless Personal Communications, vol. 95, no. 3, pp. 3119–3139, 2017.
[20] G. Jinarajadasa, L. Rupasinghe, and I. Murray, "A reinforcement learning approach to enhance the trust-level of MANETs," in 2018 National Information Technology Conference (NITC), pp. 3119–3138, Colombo, Sri Lanka, October 2018.
[21] Juneja, K., & Singh, Y. (2021). Trust-adaptive Fuzzy-Statistical Protocol for Optimizing the Communication in Attacked Network. IETE Journal of Research, 1-18.

Authors

Mr. Prabu B, Received his Mphil Degree from Bharathiar university, Coimbatore, India. Pursuing his Ph.D., degree Under the Guidance of Dr.G.Jagatheeshkumarin, Karuppannan Mariappan College, Muthur. His area of Interest is Computer Networks.

Dr. G. Jagatheeshkumar, Received Ph.D Degree from Bharathiar University,Coimbatore, India in 2020. He is working as Associate Professor & Head, PG and Research Department of Computer Science and Computer Application in Karuppunnan Mariappan College at Muthur, Tamilnadu. His main area of research interests are data mining, Computer Networks and Cloud Computing. He published a number of papers in preferred Journals. He also presented various academic as well as research-based papers at several national and international conferences. He has been 16 years experience in Teaching Profession.

How to cite this article:

Prabu B, G. Jagatheeshkumar, "Delay Aware Clustered Service Discovery Scheme Based on Trust for Mobile Ad Hoc Networks (MANET)", International Journal of Computer Networks and Applications (IJCNA), 10(5), PP: 806-815, 2023, DOI: 10.22247/ijcna/2023/223425.