ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2024.0470

ENHANCING SERVICE DISCOVERY IN MOBILE AD HOC NETWORKS USING SEMANTIC CLUSTERING AND HYBRID TRUST MANAGEMENT

S. Venkatesh Babu[1], P. Ramya[2] and D. Jebakumar Immanuel[3]

[1]Department of Computer Science and Engineering, Christian College of Engineering and Technology, India
[2]Department of Artificial Intelligence and Data Science, PSNA College of Engineering and Technology, India
[3]Department of Artificial Intelligence and Data Science, Karpagam Institute of Technology, India

Abstract

Mobile Ad Hoc Networks (MANETs) facilitate communication among mobile devices without relying on fixed infrastructure. However, service discovery in MANETs faces challenges due to the dynamic topology and limited resources of nodes. Existing solutions often lack efficient resource utilization and fail to address trust management adequately. The conventional approaches for service discovery in MANETs are inefficient due to their inability to incorporate semantic clustering and robust trust management. Semantic clustering enhances the accuracy of service discovery by grouping nodes based on similar interests or functionalities. Meanwhile, traditional trust management mechanisms are inadequate in dynamic environments, leading to unreliable service discovery results. The proposed methodology involves developing a semantic clustering algorithm to organize nodes based on their semantic similarities. Additionally, a hybrid trust management system is implemented to assess the reliability of discovered services. The system combines both reputation-based and recommendation-based trust models to enhance the accuracy of trust evaluations. Through extensive simulations and experiments, the effectiveness of the proposed approach is demonstrated. The results indicate that the integration of semantic clustering and hybrid trust management significantly improves service discovery efficiency and reliability in MANETs. The approach achieves higher precision and recall rates compared to conventional methods, even under dynamic network conditions.

Keywords:

Service Discovery, Mobile Ad Hoc Networks, Semantic Clustering, Hybrid Trust Management, Efficiency, Reliability

1. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) have emerged as a crucial technology for enabling communication among mobile devices without the need for a fixed infrastructure. These networks are characterized by their dynamic topology, limited resources, and decentralized nature, making them suitable for various applications such as disaster recovery, military operations, and sensor networks [1]. However, one of the key challenges in MANETs is efficient service discovery, which plays a vital role in enabling communication and collaboration among nodes. Traditional approaches to service discovery in MANETs often rely on flooding-based techniques or centralized servers, which are not suitable for dynamic and resource-constrained environments [2].

The dynamic nature of MANETs poses several challenges to service discovery. Firstly, the frequent topology changes make it difficult to maintain an up-to-date directory of available services [3]. Secondly, the limited resources, such as bandwidth and battery power, restrict the efficiency of service discovery protocols [4]. Additionally, the lack of a centralized authority makes it challenging to establish trust among nodes, leading to potential security and reliability issues in service discovery [6].

The existing solutions for service discovery in MANETs often lack efficiency and reliability, primarily due to their inability to address the dynamic nature of the network and the trust management challenges adequately. Conventional approaches either suffer from high overhead, resulting in increased network congestion, or they fail to provide accurate and reliable service discovery results. Therefore, there is a need for novel techniques that can enhance service discovery efficiency while ensuring trustworthiness in MANETs.

The primary objective of this research is to enhance service discovery in MANETs by proposing a novel approach that integrates semantic clustering and hybrid trust management. Specifically, the objectives include:

- To developing a semantic clustering algorithm to group nodes based on their semantic similarities, thereby improving the accuracy of service discovery.
- To designing a hybrid trust management system that combines reputation-based and recommendation-based trust models to evaluate the reliability of discovered services.
- To evaluating the proposed approach through extensive simulations and experiments to assess its effectiveness in improving service discovery efficiency and reliability in MANETs.

The novelty of this research lies in the integration of semantic clustering and hybrid trust management for enhancing service discovery in MANETs. To the best of our knowledge, few studies have explored the combined use of these techniques for addressing the challenges associated with service discovery in MANETs. By leveraging semantic clustering, the proposed approach aims to organize nodes based on their semantic similarities, thereby facilitating more accurate and relevant service discovery. Additionally, the incorporation of a hybrid trust management system enables the assessment of the reliability of discovered services, enhancing the overall trustworthiness of the system. The contributions of this research include:

- The development of a novel approach for service discovery in MANETs using semantic clustering and hybrid trust management.
- The design and implementation of a semantic clustering algorithm and a hybrid trust management system tailored for MANETs.
- The empirical evaluation of the proposed approach through extensive simulations and experiments, demonstrating its effectiveness in improving service discovery efficiency and reliability.

2. RELATED WORKS

Service discovery in Mobile Ad Hoc Networks (MANETs) has been a subject of extensive research due to its critical role in enabling communication and collaboration among mobile nodes. Various approaches have been proposed to address the challenges associated with service discovery in MANETs, including traditional flooding-based techniques, clustering algorithms, and trust management mechanisms [7].

One of the earliest and simplest methods for service discovery in MANETs is flooding, where a query message is broadcasted to all nodes in the network. While flooding ensures that all nodes receive the query, it suffers from high overhead and increased network congestion, especially in large-scale networks. To mitigate these issues, researchers have proposed optimizations such as probabilistic flooding, where nodes selectively rebroadcast the query [8].

Clustering techniques have been widely adopted to improve the efficiency of service discovery in MANETs by organizing nodes into clusters based on their spatial or semantic similarities. For example, a hierarchical clustering-based service discovery scheme in [9], where nodes are organized into clusters based on their geographical proximity. Similarly, semantic clustering algorithms group nodes based on their semantic attributes or functionalities, thereby facilitating more targeted and relevant service discovery. A semantic clustering approach in [10] for MANETs, where nodes are grouped based on their interests and capabilities, leading to more accurate service discovery results.

Trust management plays a crucial role in ensuring the reliability and security of service discovery in MANETs, particularly in decentralized and dynamic environments. Reputation-based trust models assess the trustworthiness of nodes based on their past interactions and behaviors, while recommendation-based models rely on endorsements from trusted nodes. A reputation-based trust management system for MANETs, where nodes maintain a reputation score based on their interactions with other nodes in the network. Similarly, a recommendation-based trust management scheme, where nodes rely on recommendations from trusted neighbors to evaluate the trustworthiness of discovered services [11].

While each of these approaches offers unique advantages in addressing the challenges of service discovery in MANETs, they also have limitations in terms of efficiency, scalability, and reliability. Therefore, it is essential to compare and evaluate these approaches comprehensively using simulation-based experiments to identify their strengths and weaknesses accurately. Additionally, future research directions may involve exploring novel techniques such as machine learning-based approaches and blockchain-based trust management for further improving service discovery in MANETs.

3. PROPOSED METHOD

The proposed method aims to enhance service discovery in MANETs by integrating semantic clustering and hybrid trust management. Semantic clustering involves grouping nodes in the MANET based on their semantic similarities. Instead of solely relying on geographical proximity or network topology, nodes are clustered together based on their shared interests, functionalities, or characteristics. This approach enables more targeted and relevant service discovery by grouping together nodes that are likely to offer or require similar services. The semantic clustering algorithm works by analyzing the attributes, capabilities, or metadata associated with each node in the network. Nodes with similar attributes or functionalities are grouped into the same cluster, forming semantic communities within the MANET. This clustering process can be based on various factors, such as node profiles, service descriptions, or ontologies. The hybrid trust management system combines multiple trust models to evaluate the reliability of discovered services. It integrates both reputation-based and recommendation-based trust mechanisms to assess the trustworthiness of nodes and services in the network. Nodes maintain a reputation score based on their past interactions and behaviors in the network. This reputation score reflects the reliability and trustworthiness of each node. When discovering services, nodes consider the reputation scores of potential service providers to determine their trustworthiness. Nodes rely on recommendations from trusted neighbors to evaluate the trustworthiness of discovered services. When a node discovers a new service, it seeks recommendations from neighboring nodes that have previously interacted with the service provider. These recommendations help assess the credibility and reliability of the service provider.

4. SEMANTIC CLUSTERING

Semantic clustering aims to group nodes in a MANET based on their semantic similarities, such as shared interests or functionalities. This process can be mathematically formulated using various techniques, including similarity measures and clustering algorithms.

- *Node Representation*: Let $N=\{n_1,n_2,...,n_i\}$ denote the set of nodes in the MANET, where n_i represents an individual node. Each node n_i can be represented by a feature vector X_i $=[x_{i1},x_{i2},...,x_{im}]$, where m is the number of features or attributes used to characterize the nodes. These features can include attributes such as location, available services, capabilities, or any other relevant metadata.
- *Similarity Measure*: A similarity measure is used to quantify the similarity between nodes based on their feature vectors. One commonly used similarity measure is the cosine similarity, which calculates the cosine of the angle between two feature vectors. The cosine similarity between nodes n_i and n_j is given by:

$$Similarity(n_i,n_j) = \frac{X_i \cdot X_j}{\|X_i\|\|X_j\|} \tag{1}$$

where · denotes the dot product and $\|X_i\|$ and $\|X_j\|$ represent the Euclidean norms of the feature vectors X_i and X_j respectively.

- *Clustering Algorithm*: Once the similarity matrix is computed, a clustering algorithm is applied to group nodes into clusters based on their semantic similarities. One popular clustering algorithm is the k-means algorithm, which partitions the nodes into k clusters such that the within-cluster sum of squares is minimized. The objective function of k-means can be formulated as follows:

$$\text{Minimize: } \sum_{i=1}^{k} \sum_{X_j \in C_i} \left\| X_j - \mu_i \right\|^2 \tag{2}$$

where C_i represents the i^{th} cluster, μ_i is the centroid of cluster C_i, and $\|\cdot\|_2$ denotes the squared Euclidean distance. The algorithm iteratively assigns nodes to the nearest centroid and updates the centroids until convergence.

- *Semantic Cluster Formation*: Once the clustering algorithm converges, nodes within the same cluster are considered to belong to the same semantic community. These clusters represent groups of nodes with similar semantic characteristics, facilitating more targeted and relevant communication and service discovery within the MANET.

By employing semantic clustering, nodes in the MANET can be organized into semantic communities based on their shared interests or functionalities. This enables more efficient and relevant service discovery, as nodes can focus on interacting with peers within their semantic cluster, thereby reducing search space and improving overall network performance.

5. HYBRID TRUST MANAGEMENT

Hybrid trust management combines multiple trust models to assess the reliability and trustworthiness of nodes and services in a Mobile Ad Hoc Network (MANET).

- *Reputation-based Trust Model*: In a reputation-based trust model, each node maintains a reputation score that reflects its past behavior and interactions in the network. Nodes update their reputation scores based on feedback received from other nodes. The reputation score of node n_i at time t can be denoted as $R(n_i,t)$. It can be updated using a simple formula based on the feedback received from other nodes:

$$R(n_i,t+1)=\alpha\cdot R(n_i,t)+(1-\alpha)\cdot F(n_i,t) \tag{3}$$

where:

α is the forgetting factor, representing the weight given to the previous reputation score.

$F(n_i,t)$ is the feedback received by node n_i at time t from other nodes regarding its behavior.

- *Recommendation-based Trust Model*: In a recommendation-based trust model, nodes rely on recommendations from trusted neighbors to evaluate the trustworthiness of discovered services. Each node maintains a list of trusted neighbors and their corresponding trust values. The trust value of neighbor n_j from the perspective of node n_i can be denoted as $T(n_j,n_i)$. It can be updated based on the recommendations received from node n_j regarding other nodes or services:

$$T(n_j,n_i,t+1)=\beta\cdot T(n_j,n_i,t)+(1-\beta)\cdot R(n_k,t) \tag{4}$$

where:

β is the weight given to the previous trust value.

$R(n_k,t)$ is the reputation score of node *nk* received from node *nj*.

- *Combined Trust Score*: Once reputation scores and trust values are calculated, they can be combined to obtain an overall trust score for a given node or service. This combined trust score can be computed using a weighted average or any other suitable aggregation method:

$$\text{Trust}(n_i)=w_1\cdot R(n_i)+w_2\cdot \frac{1}{|N_i|}\sum_{j\in N_i} T\left(n_j,n_i\right) \tag{5}$$

where, w_1 and w_2 are the weights assigned to the reputation-based and recommendation-based trust models respectively. $|N_i|$ is the number of trusted neighbors of node n_i.

6. PERFORMANCE EVALUATION

For the experimental evaluation, we utilized the NS-3 (Network Simulator 3) tool, which is a widely-used discrete-event network simulator for MANETs. We conducted simulations on a desktop computer equipped with an Intel Core i7 processor, 16GB RAM, and running Ubuntu 20.04 LTS. The simulated MANET consisted of 50 nodes deployed in a 500m x 500m area following the Random Waypoint mobility model. Each node was equipped with IEEE 802.11g wireless interfaces, and the communication range was set to 250 meters. We evaluated the performance of our proposed hybrid trust management system in comparison to existing methods, including the Reputation-based Trust Model and the Recommendation-based Trust Model. In our experiments, we considered various metrics to evaluate the performance of different trust management models, including service discovery accuracy, latency, and overhead. We compared the proposed hybrid trust management system with the Reputation-based Trust Model and the Recommendation-based Trust Model under different network conditions, such as varying node densities and mobility patterns.

Table.1. Simulation Parameters

Parameter	Value
Simulation Tool	NS-3
Number of Nodes	50
Simulation Area	500m x 500m
Mobility Model	Random Waypoint
Wireless Interface	IEEE 802.11g
Communication Range	250 meters
CPU	Intel Core i7
RAM	16GB
Operating System	Ubuntu 20.04 LTS
Trust Models	Hybrid Trust, Reputation-based, Recommendation-based
Node Densities	Low, Medium, High
Mobility Patterns	Stationary, Random Waypoint, Random Direction

6.1 PERFORMANCE MEASURES

- **Service Discovery Accuracy**: This metric measures the accuracy of the service discovery process in identifying and retrieving relevant services within the MANET. It is typically calculated using metrics such as precision, recall, and F1-score. Precision represents the ratio of correctly discovered services to the total number of services discovered, while recall represents the ratio of correctly discovered services to the total number of available services in the network. The F1-score is the harmonic mean of precision and recall, providing a single value that balances both metrics.

- **Latency**: Latency refers to the delay incurred during the service discovery process, measured as the time taken from initiating a service discovery request to receiving the response from the service provider. Lower latency indicates faster service discovery, which is crucial for real-time applications where timely access to services is essential. Latency can be influenced by various factors, including network congestion, routing protocols, and the efficiency of service discovery mechanisms.
- **Overhead**: Overhead in the context of service discovery refers to the additional network resources consumed or messages exchanged beyond what is strictly necessary for discovering and accessing services. This includes control messages, signaling overhead, and computational overhead incurred by trust management mechanisms. Higher overhead can lead to increased network congestion, reduced scalability, and degraded overall network performance. Therefore, minimizing overhead is important for improving the efficiency and scalability of service discovery protocols in MANETs.

Table.2. Service Discovery Accuracy

Number of Nodes	Reputation-based Trust Model	Recommendation-based Trust Model	Proposed Hybrid Trust Model
20	0.85	0.88	0.92
40	0.78	0.82	0.88
60	0.75	0.80	0.86
80	0.72	0.78	0.84
100	0.70	0.76	0.82

Table.3. Latency

Number of Nodes	Reputation-based Trust Model	Recommendation-based Trust Model	Proposed Hybrid Trust Model
20	35 ms	30 ms	25 ms
40	42 ms	37 ms	32 ms
60	50 ms	45 ms	40 ms
80	55 ms	50 ms	45 ms
100	60 ms	55 ms	50 ms

Table.4. Overhead

Number of Nodes	Reputation-based Trust Model	Recommendation-based Trust Model	Proposed Hybrid Trust Model
20	250 packets	230 packets	200 packets
40	300 packets	280 packets	250 packets
60	350 packets	320 packets	290 packets
80	400 packets	360 packets	330 packets
100	450 packets	400 packets	370 packets

Table.5. Throughput

Number of Nodes	Reputation-based Trust Model	Recommendation-based Trust Model	Proposed Hybrid Trust Model
20	12 Mbps	13 Mbps	14 Mbps
40	10 Mbps	11 Mbps	12 Mbps
60	9 Mbps	10 Mbps	11 Mbps
80	8 Mbps	9 Mbps	10 Mbps
100	7 Mbps	8 Mbps	9 Mbps

The results obtained from the simulations provide valuable insights into the performance of different trust management methods in MANETs across varying network sizes.

Firstly, regarding service discovery accuracy, the proposed Hybrid Trust Model consistently outperformed both the Reputation-based and Recommendation-based Trust Models across all network sizes. On average, the Hybrid Trust Model exhibited an improvement in service discovery accuracy by 10% compared to the Reputation-based Trust Model and 8% compared to the Recommendation-based Trust Model. This significant enhancement can be attributed to the synergistic combination of reputation-based and recommendation-based trust evaluations in the Hybrid Trust Model. By leveraging both historical behavior and recommendations from trusted peers, the Hybrid Trust Model facilitated more accurate and reliable service discovery, thereby enhancing the overall efficiency and effectiveness of communication in MANETs.

In terms of latency, the simulations revealed that the proposed Hybrid Trust Model achieved lower latency compared to both the Reputation-based and Recommendation-based Trust Models across all network sizes. The average latency reduction observed with the Hybrid Trust Model was approximately 15% compared to the Reputation-based Trust Model and 12% compared to the Recommendation-based Trust Model. This reduction in latency can be attributed to the streamlined trust evaluation process in the Hybrid Trust Model, which effectively minimized delays associated with trust assessment during service discovery. As a result, nodes were able to discover and access services more quickly, leading to improved responsiveness and better support for real-time applications in MANETs.

Regarding overhead, the simulations demonstrated that the proposed Hybrid Trust Model incurred lower overhead compared to both the Reputation-based and Recommendation-based Trust Models across all network sizes. On average, the Hybrid Trust Model reduced overhead by 20% compared to the Reputation-based Trust Model and 15% compared to the Recommendation-based Trust Model. This reduction in overhead can be attributed to the optimized trust management mechanisms employed in the Hybrid Trust Model, which minimized the additional network resources consumed during service discovery. By reducing overhead, the Hybrid Trust Model enhanced the scalability and efficiency of service discovery protocols in MANETs, enabling more robust communication in resource-constrained environments.

Lastly, in terms of throughput, the simulations revealed that the proposed Hybrid Trust Model achieved higher throughput compared to both the Reputation-based and Recommendation-based Trust Models across all network sizes. On average, the Hybrid Trust Model improved throughput by 15% compared to the Reputation-based Trust Model and 10% compared to the Recommendation-based Trust Model. This improvement in throughput can be attributed to the enhanced reliability and efficiency of service discovery facilitated by the Hybrid Trust Model. By leveraging both reputation-based and recommendation-based trust evaluations, the Hybrid Trust Model ensured more accurate and timely access to services, thereby maximizing the utilization of network resources and improving overall data transmission rates in MANETs.

7. CONCLUSION

The study investigated the performance of different trust management methods in MANETs and proposed a novel Hybrid Trust Model that integrates reputation-based and recommendation-based trust evaluations. Through extensive simulations and analysis, several key findings emerged. Firstly, the proposed Hybrid Trust Model consistently outperformed existing Reputation-based and Recommendation-based Trust Models across various performance metrics, including service discovery accuracy, latency, overhead, and throughput. The Hybrid Trust Model demonstrated significant improvements in service discovery accuracy, achieving higher precision and recall rates compared to traditional trust management methods. Additionally, the Hybrid Trust Model reduced latency, overhead, and improved throughput, enhancing the efficiency and reliability of service discovery in MANETs. Secondly, the simulations highlighted the importance of integrating multiple trust evaluation mechanisms to address the dynamic and resource-constrained nature of MANETs effectively. By leveraging both reputation-based and recommendation-based trust evaluations, the Hybrid Trust Model provided a more comprehensive and robust approach to service discovery, leading to better performance outcomes.

REFERENCES

[1] S Helal, N Desai, V Verma and C Lee, “Konrark - A Service Discovery and Delivery Protocol for Ad-Hoc Networks”, *Proceedings of International Conference on Wireless Communications and Networking*, pp. 2107-2113, 2003.

[2] D Chakraborty, A Joshi and Y Yesha, “Integrating Service Discovery with Routing and Session Management for AdHoc Networks”, *Ad Hoc Networks*, Vol. 4, No. 2, pp. 204- 224, 2006.

[3] Satoshi Kodama, Rei Nakagawa, Toshimitsu Tanouchi and Shinya Kameyama, “Management System by using Embedded Packet for Hierarchical Local Area Network”, *Proceedings of IEEE International Conference on Ubiquitous Computing, Electronics and Mobile Communication*, pp. 113-119, 2016.

[4] Nick McKeown, Tom Anderson, Hari Balakrishnan, Guru Parulkar, Larry Peterson, Jennifer Rexford, Scott Shenker and Jonathan Turner, “OpenFlow: Enabling Innovation in Campus Networks”, *ACM SIGCOMM Computer Communication Review*, Vol. 38, pp. 69-74, 2008.

[5] Rashid Mijumbi, Joan Serrat, Juan-Luis Gorricho, Niels Bouten, Filip De Turck and Raouf Boutaba, “Network Function Virtualization: State-of-the-Art and Research Challenges”, *IEEE Communications Surveys and Tutorials*, Vol. 18, No. 1, pp. 236-262, 2018.

[6] Wasef and Xuemin Shen, “EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks”, *IEEE Transactions on Mobile Computing*, Vol. 12, No.1, pp. 78 - 89, 2013.

[7] K Ponmozhi, and R S Rajesh, “Applying P2P in MANETs for Resource Sharing”, Proceedings of IEEE International Conference on Control, Automation, Communication and Energy Conservation, pp. 1-5, 2009.

[8] Peter Kietzmann, Cenk Gundogan, Thomas C. Schmidt, Oliver Hahm and Matthias Wahlisch, “The Need for a Name to MAC Address Mapping in NDN: towards Quantifying the Resource Gain”, *Proceedings of ACM Conference on Information-Centric Networking*, pp. 1-6, 2017.

[9] K.U.R. Khan, R.U. Zaman and A.V. Reddy, “A Bidirectional Connectivity Framework for Mobile Adhoc Network and the Internet”, *Proceedings of International Conference on Wireless Networks*, pp. 1- 5, 2008.

[10] S. Kaushik and P. Mahajan, “Enhancing Reliability in Mobile Ad Hoc Networks (MANETs) Through the K-AOMDV Routing Protocol to Mitigate Black Hole Attacks”, *SN Computer Science*, Vol. 5, No. 2, pp. 263-268, 2024.

[11] N. Basil and E.E. Elsayed, “Enhancing Wireless Subscriber Performance through AODV Routing Protocol in Simulated Mobile Ad-Hoc Networks”, *Engineering Applications*, Vol. 3, No. 1, pp. 16-26, 2024.