ISSN (Print) : 2347-6729
ISSN (Online) : 2348-3105

International Journal on Recent Researches In Science, Engineering & Technology
(Division of Computer Science and Engineering)
A Journal Established in early 2000 as National journal and upgraded to International journal in 2013 and is in existence for the last 10 years. It is run by Retired Professors from NIT, Trichy. It is an absolutely free (No processing charges, No publishing charges etc) Journal Indexed in JIR, DIIF and SJIF.
Research Paper
Available online at: www.jrrset.com

Volume 3, Issue 9
September 2015.

JIR IF : 2.54
DIIF IF : 1.46
SJIF IF : 1.329

INTERRUPTION DISCOVERY IN MOBILE AD-HOC NETWORK

N.Satish[1], G.Arul Dalton[2]
[1,2]Associate Professor, Department of Computer Science and Engineering, Mahendra Engineering College, Mahendhirapuri, Namakkal District, Mallasamudram, Tamilnadu, India.

Abstract

Mobile Ad-hoc Network is a network of a number of mobile routers and associated hosts, organized in a random fashion via wireless links. Service Discovery is one of the most important issues in MANET. It is defined as the process of facilitating service providers to advertise their services in a dynamic way and to allow consumers to discover and access those services in an efficient and scalable manner. In this paper, we are proposing a flexible and efficient approach to service discovery for MANET. Most of the service discovery protocols proposed in literature don't provide an appropriate route from consumer to service provider. Hence after services are discovered, a route request needs to be initiated in order to access the service. In this paper, we are proposing a robust and flexible approach (RFA) to service discovery for MANET that not only discovers a service provider in the vicinity of a node, but at the same time, it also provides a route to access the service.
Keywords: MANET, Ad-hoc Network, RFA

Introduction

Wireless Sensor Networks (WSNs) have been widely applied in various industrial applications, e.g., surveillance operations, an analysis of disease, monitoring of patient and equipment, source detection, fault prediction, pollution monitoring, sea searching, tide monitoring and report collected data to the sink by using multi-hp wireless communications. The nodes are able to collaborate and self organize together in order to establish and maintain the network[1]. Clustering means grouping of nodes that are close to each other and the main purpose is to reduce the energy consumption and routing overhead[2]. However, the wireless and resource-constraint nature of a sensor network creates it an ideal medium for malicious attackers to intrude the system. Thus, providing security is extremely important for the safe application of WSNs. To establish secure communications, we need to ensure that all communicating nodes are trusted. This highlights the fact that it is critical to establish a trust model allowing a sensor node to infer the trustworthiness of another node.

Distributed and Safe Weighted Clustering Algorithm[3] detects common routing problems and attacks in clustered WSNs that depend on behavioral level in order to remove the malicious node. This weighted clustering algorithm detects the internal misbehavior nodes during distributed monitoring process. It also decrease energy utilization and guaranties the choice of legitimate CHs. Light Weight Intrusion Detection System[4] integrated for clustered sensor

networks uses an over hearing mechanism to reduce the sending alert packets. This approach focuses around strategy of distributed resolution enables to generate a reduced number of balanced and homogeneous clusters that reduces the energy utilization of the network and prolongs the sensor lifetime.

Literature survey

A distributed Hierarchical Dynamic Trust Management Protocol (HTMP) [4] that contains two trust values that is social trust and QoS (Quality of Service) trust. A probability model to examine protocol performance and declared subjective trust against the objective trust obtained based on truth node status. However, implementing a complex trust evaluation at each CM of the cluster is unrealistic. An Energy efficient Reliable Trust-based Data Aggregation protocol (ERTDA) [5] monitors and evaluates the trust values of the nodes and it detects and excludes the compromised nodes in a timely manner. The ERTDA protocol can effectively improve the accuracy of the aggregation, reduce both the node death rate and node energy consumption, improve the reliability of the data communication and lengthen the life of the networks.

Energy-efficient Trust based data Aggregation (ETA) [6] achieves reliable and energy-efficient data transmission and aggregation. ETA uses the concept of functional reputation and trust as a means to reach reliability. Efficient reputation is used to select nodes that best satisfy the criteria to be collector on the basis of the quality of the node.

Trust-based CH Election Mechanism (TCHEM) [7] can decrease the likelihood of malevolent or compromised nodes from becoming CHs. It does not encourage sharing of trust information among sensor nodes. Therefore, this mechanism reduces the effect of bad mouthing attacks. However, TCHEM does not cover trust in detail, due to numerous key issues of trust management.

Trust Aware Geographical Routing scheme (TAGR) [8] relies on both direct and indirect observations to derive the trustworthiness of each adjacent node while it is capable of defending against routing attacks. This scheme reduces the routing overhead and resists some common attacks. However, this trust aware scheme depends on the specific routing scheme that limits the scope of applications.

Proposed System

The proposed improvement is mainly in the area of enhancing the QoS of the network. The introduction of a counter at every node is to fix a time interval to check the quality of service at every node within the interval of time K_{ij}.

The quality of service is measured using the QoS ratio defined as the difference between by the Equation (4.1).

$$QoS\ Ratio = \frac{\sum_i^j Pkts\ Flowing\ In / \sum_i^j Pkts\ Flowing\ Out}{k_{ij}} \tag{4.1}$$

where i is the previous instant of time and j is the current instant of time. The QoS ratio is individually measured for every node present in the network. The usual HDCR algorithm measures the link residual life and distance between nodes to find a good forwarder. Apart from that, the proposed method also estimates the QoS of each node in the network. The working flow of the proposed system that has been integrated with the HDCR algorithm is illustrated in figure 4.1.

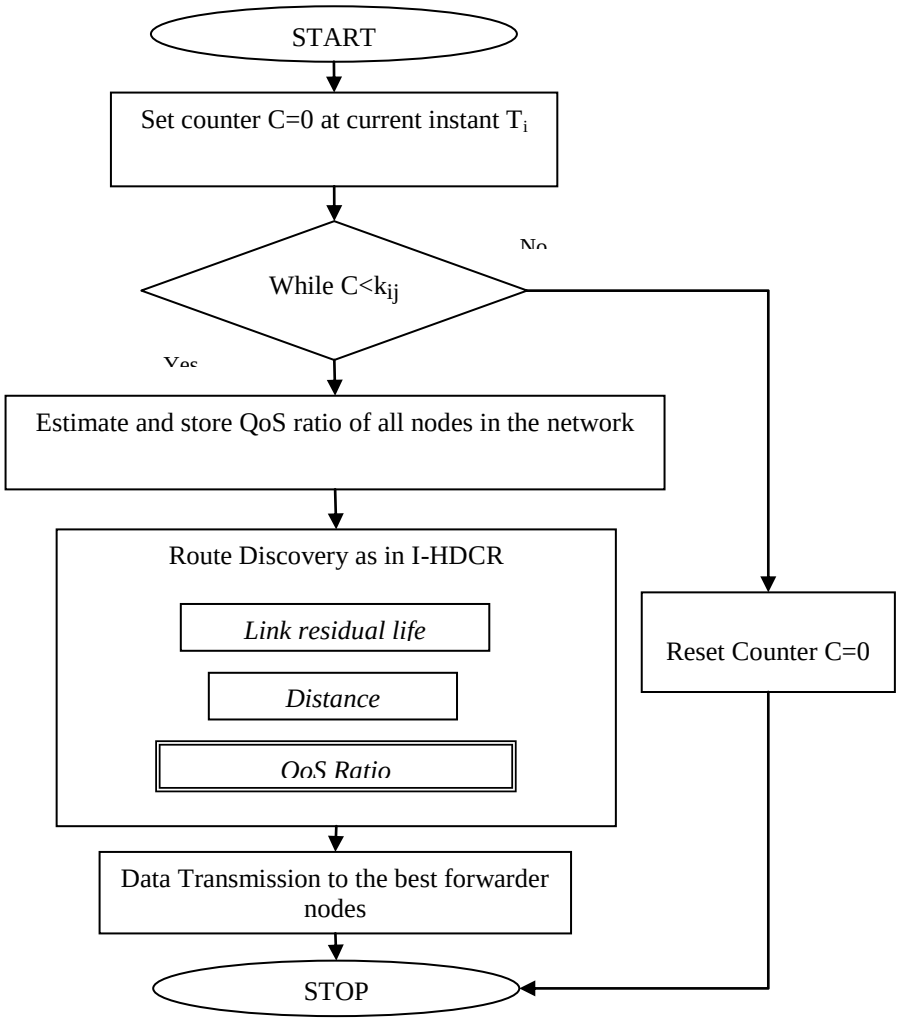

Figure 4.1 Working flow of the I-HDCR scheme

The figure 4.1 shows that a counter C is reset after every K interval of time which is a difference in the current time Tj and the previous instant Ti. K is considered to be fixed to assess the QoS ratio for a node in order to maintain uniformity so each node can be compared against each other for their QoS performance. The QoS estimated at every node is flushed at the Counter's reset. This ensures that only the latest QoS ratios would be available for routing operations.

The link residual life and distance based node selection can give a completely different result from that of the QoS ratio based selection. And QoS based selection of the node that has minimal LRL does not improve the system's throughput. Hence the QoS ratio based selection is performed as in the algorithm below.

The I-HDCR method assumes two values as fixed constants to perform simulations, Kij and W.

- **K_{ij}**

Technically, the K_{ij} value represents the time interval for the flushing of the buffer that aggregates the QoS Ratio. In other words, the time duration at which the counter C will be reset is denoted by K_{ij}. The figure 4.2 illustrates how this works considering the data

transmission between the nodes i and j. The number of data packets transmitted between the time, 0 to T are taken for the QoS ratio estimation. Breaking the entire T value into fixed time instants can produce an effective expected output. Some example values for K_{ij} are shown in the figure 4.2. The value of K_{ij} can be in the range of a few milliseconds for good operation.

- **W**

The threshold value of the LRL is dynamically estimated to ensure that the right node is picked from a node's neighbour list as the next node. This is achieved by considering a percentage of the maximum LRL (denoted by LRL_{MAX}) as a dynamic threshold and it is estimated by the Equation (4.2),

$$LRL_{THRESHOLD} = W \times LRL_{MAX} \quad , \quad 0.5 \le W \le 1 \tag{4.2}$$

Since the QoS ratio is introduce to only improve the performance of HDCR, the range of W lies only between 0.5 and 1.

Simulation Analysis

The performance of the RFA is analyzed by using the Network simulator (NS2). The NS2 is an open source programming language written in C++ and OTCL (Object Oriented Tool Command Language). NS2 is a discrete event time driven simulator that is used to mainly model the network protocols. The nodes are distributed in the simulation environment. The parameters used for the simulation of the RFA scheme are tabulated in Table 1. The simulation of the proposed scheme has 50 nodes deployed in the simulation area 1000×600. The nodes are communicated with each other by using the communication protocol User Datagram Protocol (UDP). The traffic is handled using the traffic model CBR. The radio waves are propagated by using the propagation model two-ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery rate, packet loss rate, average delay, throughput and residual energy.

Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of number of packets delivered to all receivers to the number of data packets sent by the source node.

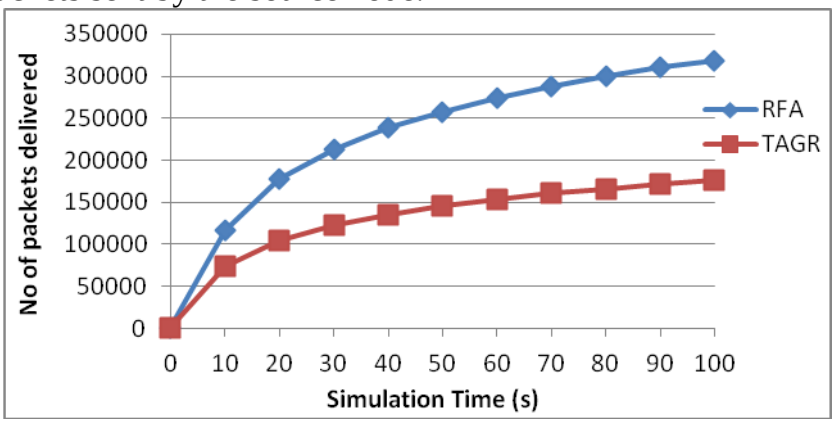

Fig:3 Packet Delivery Rate

The figure 3 indicates the PDR of the proposed scheme RFA is higher than the PDR of the existing method TAGR. The greater value of PDR means the better performance of the protocol.

Packet Loss Rate

The Packet Loss Rate (PLR) is the ratio of the number of packets dropped to the number of data packets sent.

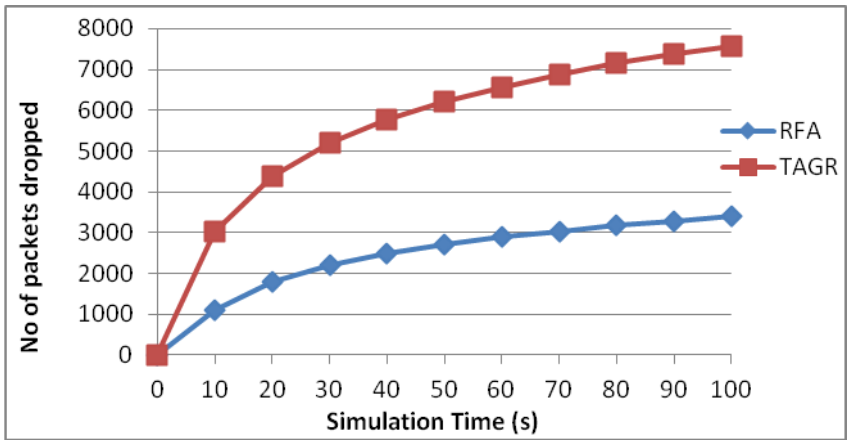

Fig:4 Packets Loss Rate

The PLR of the proposed scheme RFA is lower than the existing scheme TAGR in Figure 4. Lower the PLR indicates the higher performance of the network.

Average Delay

The average delay is defined as the time difference between the current packets received and the previous packet received. It is measured by Equation. 8.

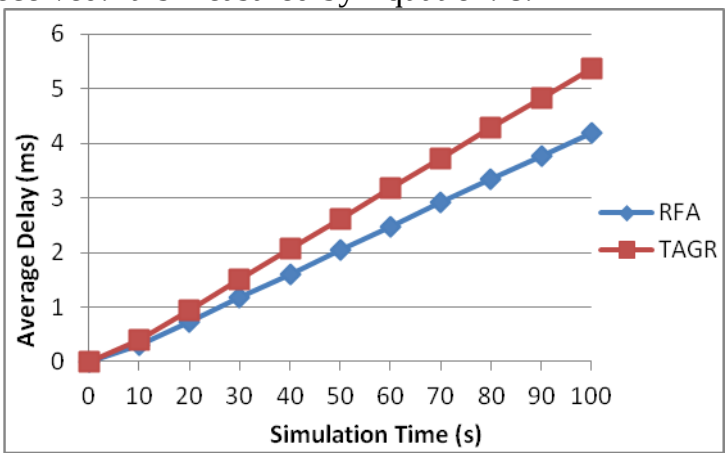

Fig:5 Average Delay

Figure 5 demonstrates that the delay value is low for the proposed scheme RFA than the existing scheme TAGR. The minimum value of delay means that higher value of the throughput of the network.

Throughput

Throughput is the average of successful messages delivered to the destination.

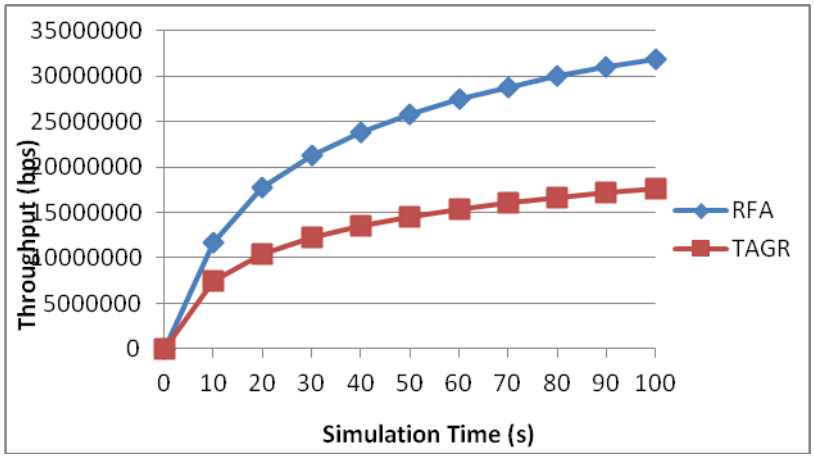

Fig: 6 Throughput

Figure 6 proves that the proposed scheme RFA has greater average throughput when compared to the existing scheme TAGR.

Conclusion

In this paper we have proposed a novel approach towards service discovery in MANET. The proposed approach is very flexible, efficient and can be adopted to work in any environment. The current work can be extended to represent the service using better representation language like DAML etc. In addition broadcasting of service advertisement is right now done periodically. We can improve the broadcasting mechanism. The broadcasting can be a function of network congestion, service popularity factor etc.

References

[1] Bao F., Chen I. R., Chang M.and Cho J. H. 2012. Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection. Network and Service Management, IEEE Transactions on. 9(2): 169-183.

[2] Alshehri M. D.and Hussain F. K. 2015, November. A Comparative Analysis of Scalable and Context-Aware Trust Management Approaches for Internet of Things. In Neural Information Processing (pp. 596-605). Springer International Publishing.

[3] Taghikhaki Z., Meratnia N. and Havinga P. J. 2011, April. Energy-efficient trust-based aggregation in wireless sensor networks. In Computer Communications Workshops (INFOCOMWKSHPS), 2011 IEEE Conference on (pp. 584-589). IEEE.

[4] G. V. Crosby, N. Pissinou, J. Gadze. 2006. A framework for trust-based cluster head election in wireless sensor networks, Second IEEE Workshop on Dependability and Security in Sensor Networks and Systems. pp. 10-22.

[5] A. Boukerche, X. Li and K. EL-Khatib. 2007. Trust-Based Security for Wireless Ad Hoc and Sensor Networks, Computer Comm. 30: 2413-2427.

[6] Z. Cao, J. Hu, Z. Chen, M. Xu, and X. Zhou. 2008.Fbsr: feedback-based secure routing protocol for wireless sensor networks. International Journal of Pervasive Computing and Communications.

[7] A. Jsang, R. Ismail and C. Boyd. 2005. A Survey of Trust and Reputation system for online service provision [C]. Decision Support System. pp. 618-644.

[8] T. Zahariadis, P. Trakadas, H. C. Leligou, S. Maniatis and P. Karkazis. 2013. A novel trust-aware geographical routing scheme for wireless sensor networks. Wireless Personal Communications. 69(2): 805-826.