Volume 5, Issue 4, April 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Special Issue on Impact of Technology on Skill Development

Conference Held at IETE Amravati Center, Maharashtra, India

ECATP: An Efficient Clustering Algorithm Based on Nodes Trusts and Performances for MANETs

[1]Payal P. Khatri, [2]Dr. R.V. Dharaskar, [3]Dr. V. M. Thakare

[1]Student from PG department of Computer Science and Information Technology , SGBAU Amravati, India

[2]Professor and Head, PG Department of Computer Science and Engg., G H Raisoni College of Engg., Nagpur, India

[3]Head of department of PG department of computer science and information technology SGBAU Amravati, India

Abstract−A mobile ad hoc network (MANET) is a wireless network without the support of any fixed infrastructure. Security is one of the main challenges in ad hoc network due to dynamic topology and mobility of nodes. Organizing mobile nodes into manageable clusters can limit the amount of secure routing information. Under a cluster structure, mobile nodes are managed by nodes called cluster heads. The role of cluster head is resource consuming since it is always switched on and is responsible for the long-range transmission. For example, to send a bit over a distance, nodes in MANET consume resources that can perform around thousands to millions of arithmetic operations. In this paper, an efficient clustering algorithm is introduced based on node's trust and performances called ECATP, where the clusters are formed around the trustworthy, the densest and the most powerful nodes.With the use of the trust metric in the ECATP algorithm, the network becomes much more resistant to the selfishness attack. It minimizes the transmission delay, maximizes the successful data delivery rate, and consumes less energy of nodes.

Index Terms—Clustering, cluster head, MANET, trust

I. INTRODUCTION

Rapid development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications. Ad-hocnetworks are known for the lack of infrastructure and the possibility movement of the nodes.In MANET, all nodes are routers and forward packets without any infrastructure. This kind of network is spontaneous, self-organized, and self-maintained, which make them an ideal choicefor uses such as communication and information sharing [1,2].The performanceof an ad hoc network heavily depends on therouting process. Adverse propagation conditions, bandwidthlimitations and topological changes lead to the development ofdifferent routing protocols for an ad-hoc network.As nodes perform various computations, a lot of battery power gets consumed, which in turn reduces the network lifetime. Thus, there is a clear demand for routing protocols for such networks which are energy-efficient and consume very less power of nodes while forwarding data [3].

Currently, there are several routing protocols for eachtype of network. However, even this efficiency on small and medium size networks, neither of them can be used on large scales because they generate too much control traffic or would require too large routing tables[4,8]. One common solution proposed for routing is to introduce a hierarchical routing by grouping the closer nodes geographically. Each group, is called a cluster and is represented and managed by a particular node called cluster head.The cluster head possesses valuable information regarding nodes' location and their contacts. Most clustering algorithms assume that the network setting is reliable and has no threats. In fact, ad hoc networks are simple to be wiretapped, intruded and attacked, due to the open distributed network structure[5].However, when applying any of the protocols, many attacks could occur by malicious nodes which causes inefficiency in the functionality of the network. As a result, toensure that the network provides its services without any problem, a trust based protocol helps to resolve this issue. Based on the trust level, each node communicates with its neighbors. Trust can help to sustain the stability of the network and enhance the communication process between nodes. In addition, trust can be implemented to reduce the size of the data sent from node to node and thus decrease the needed power consumption. With the increase in trust level at each node, less encryption or cryptography is used [6].

In this paper, a new clustering approach based on the trust metric is introduced. The proposed algorithm computes trust value and also calculates overall performance of each node in the network. Thus, it provides longer network lifetime, as well as reduces energy consumption for ad hoc network, particularly in clustering and routing. The proposed approach aims to enhance the routing process and produces trustworthy cluster heads.

II. RELATED WORK

A. BACKGROUND

Clustering is a well-known technique highly used within MANETs. It is mainly employed to reduce the complexity of proactive routing protocols (e.g. OLSR) by dividing the entire network in small and manageable areas. Mobile nodes will elect a cluster head based on some QoS criteria. Ad hoc networks use clustering algorithms to reduce power consumption. This power saving aspect is important because nodes in ad hoc networks do not easily obtain power. The common absence of a constant power supply in adhoc networks have led researchers to propose new routing metrics that seek to increase energy efficiency. Several proposals have been explored in order to maximize the network lifetime.

Machado et al.,[1] analyzed the most relevant modificationsfor OLSR in order to make it energyefficient and compares their performances in terms ofthroughput, network lifetime and node energy level. Additionally, an extension to OLSR-ETX, named ETXEMPR, is also proposed which provides a longer network lifetime. To deal with the high cost and resource constraint problem in MANETscost Shen et al [2]., proposed Anonymous Location-based Efficient Routing Protocol (ALERT) that dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, whichform a non-traceable anonymous route. In addition, it hides the data initiator/receiver among many initiators/receivers to strengthensource and destination anonymity protection. It hasstrategies to effectively counter intersection and timing attacks. Also, ALERT achieves comparable routing efficiency to the GPSR geographical routing protocol. However,it is not completely bulletproof to all attacks.

Genetic algorithms have been used to identify the nodes which are best suitable among various neighbors for carrying the message towards the destination.Sharma et al.,[3] proposed a novel routing protocol named genetic algorithm-based energy-efficient routing (GAER) protocol for infrastructure-less Oppnets that uses personal information of nodes, and then applies the genetic algorithm (GA) to select a better next hop among a group of neighbor nodes for the message to be routed to the destinationWith the application of GA optimal results are obtained thatlead to prolonged battery life.

Almasri et al.,[6] proposed a novel trusted and energy efficientrouting protocol (TERP) based on the Destination SequencedDistance Vector Protocol (DSDV)that helps to maximize the lifetime of network.TERP helps to increase thesecurity level in the network and thus avoid any malicious nodesor untrusted nodes. It also reduces the power consumption byusing the trust factor. The higher the degree of trust, the lessencryption is used which results in less energy. Three levels of trust are discussed and compared to DSDV in terms of power consumption. When compared to DSDV, TERP has less drop ratio and more delivery ratio.

Cheng et al.,[7] proposed a position-based routing protocol with a power-saving scheme (called NRP-PB protocol) for ad hoc environments. The proposed protocol registered a better performance than did the ILAR protocol and resolved problems that plagued the ILAR protocol. This protocol is more effective and reliable algorithm than the ILAR protocol, especially in regards to adaptation under dynamic ad hoc environments. The integration of power-saving technology into the protocol increases the work life of nodes and networks. The NCRP includes a cluster scheme and a power-balance scheme, and provides a routing protocol for discovering and maintaining routing paths in order balance the energy of each node.This mechanism reduces simultaneousloading of networks, providingenergy conservation and ensuring prolonged lifetime of nodes and networks.

B. Existing Methodologies

1. Energy aware OLSR clustering

The energy aware OLSR clustering [4] uses the residual energy with some related approaches based on the density parameter. The selected cluster heads by this protocol have more residual energy and can live more than in the other approaches thereby increasing the network lifetime. Two scenarios are taken into consideration: one varying the number of nodes (density of the network) and the second varying the speed of nodes (mobility of the network). An improvement is noticed with the OLSR clustering solution when compared to others based on the density criterion. The RPGM model behaves well and produces reasonable number of clusters as well as consumes less energy within the network. However, (Hello and TC) and will never be elected as cluster heads in the proposed algorithm. It also optimizes the delay of carried flows by adopting a selective forwarding approach based on a hierarchical routing model.

2. Reputation based clustering algorithm (RECA)

RECA [5] aims to elect trustworthy, stable and high energy cluster heads that can be used to manage the security of the hierarchical network. RECA takes under consideration a combined weight metric as well as, the reputation value. The reputation of the node is evaluated through the capability of the node in dealing with packets in the routing process. To resolve nodes' reputation as a function of its centrality characteristics, it is classified as high, medium or low Centrality. In addition, the degree and relative mobility are considered within the cluster to ensure reliability and stability of clusters. It's used to elect the secure backbone nodes within the networks. Moreover, the reconstruction and the recovering mechanism in the algorithm are able to resist attacks on the cluster structure.

3. Trusted Weight Clustering Algorithm (TWCA)

TWCA [8] is similar to WCA in terms of cluster formation and cluster head election. However, in WCA security features are not included. The proposed TWCA is a cluster based trust evaluation, in which the mobile nodes are grouped into clusters with one cluster head The trust relationship is established in two ways: Direct observation and recommendation. Four parameters are considered in the weight computation, namely the node degree, the battery power, the mobility and the transmission power for the selection of cluster head election.However, TWCA proved to be more efficient than WCA and SEMC scheme.

C. Analysis and Discussion

In energy aware OLSR clustering [4] enables clustering for OLSR networks without causing any change in the structure of control messages. When compared with other mobility models it shows improvement based on the mobility models. It covers the performance and scalability issues to a greater extent. This solution needstocombinetheenergywithothercriteriain order toproducemore efficient clustering. It does not solve the problem of overlapped clustering.

RECA [7] achieves accurate definition and precise quantization of reputation for nodes in the network based on their behavior. This algorithm improvesthe cluster structure, as it considers the reputation, correlation and mobility of nodes in the method of electing cluster heads and gateways. It also includes the reconstruction and the recovering mechanism in the algorithm which helps in resisting attacks on the cluster structure and thereby improving reliability of the network. This algorithm needs to be evaluated for large scale ad hoc network.

TWCA [8] adapts itself in dynamic topology of ad hoc networks. It achieves significant performance compared to the WCA and SEMC algorithm in terms of average number of cluster member, average number of cluster head, energy, throughput and packed received ratio. However, more security concepts need to be implemented for large sized mobile ad hoc networks.

III. PROPOSED METHODOLOGY

An Efficient Clustering Algorithm based on Trust & Performance (ECATP)

Clustering is one of the main techniques that are used toincrease the scalability of MANETs, but without any securityconsiderations clustering is prone to various security attacks. The selfishness is one of the attacks that threaten the functioning of the network. The primary goal of the malicious nodeis to use their resources only for their own benefit. In terms ofresource consumption, data transmission is the mostexpensive function in the MANET environment. To send a bit over a distance, MANETs' nodes consumeresources. Thus, it may not forward others'packets and simply discard them on purpose. Or they mayexcessively reduce transmission power to save energy,resulting in network partitioning. Any such feature ofbehavior is called selfishness. Currently, mostclustering algorithms assume that the network environmentis reliable and has no threats. Clusterheads are the keynodes in hierarchical ad hoc networks. If cluster heads are attacked, the network performance decreases seriously. Therefore, to elect the suitablenode to be a cluster head the trust metric is added into the OLSR protocol.

A. Trust evaluation:

In ad hoc networks, the node process routing control messages and data messages. To calculate the trust metric ofa node, the algorithm use several types of messages, including: Hello message, TC message and data messagesto be routed through a node with weights associated to each message. The higher the weight, higher is the trust value.

B. The overall performance computation:

After evaluating the trust metric, the security of the proposed algorithm can be improved by adding the new metricin the computation of the overall performance of a node. To calculate the performance of a node, the clustering algorithm uses several metrics, including: residual energy, free memory, processor speed, disk space and node density.

C. OLSR Clustering algorithm:

In this paper, an improved version of the OLSR clustering algorithm is proposed, which takes into account thetrust metric of the MANETs node and then it computes the overall performance of nodes.

Step 1: In a clustered OLSR network, each node can be in one ofthree states:

- State 0: **not decided**. When a node has just arrived, or it hasjust left its cluster and has no neighbors in its neighborhood,its status is not decided yet. There is no cluster head or clustermember. It must wait for the receipt of HELLO messages.
- State 1**: Cluster head.** The node was exchanged HELLOmessages, and it has the highest performance. It creates acluster in which it was appointed head of the cluster.
- State 2: **member**. The node has exchanged HELLOmessages; it has a low performance compared to itssymmetric neighbors, and is part of the cluster members.

Step 2: Each node calculates:

- ✓ Its neighbor trust
- ✓ Its overall performance.

Both these information are carried in HELLO message.

Step 3: After receiving HELLO message, the node gets its trust metric.

Step 4: Then it can calculates its overall performance (OPerfi)

Step 5: Aftercomputing the overall performance the node sends its value throughthe broadcasted HELLO message.

Step 6: When the node receives its neighbor nodes' HELLO messages, it updates the related nodes'trust value and update its overall performance. Each node inthe network calculates its corresponding neighbor's trust and sends it through the HELLO message.

Step 7: After receiving the HELLO messages, eachnode can have a vision of trust of the other nodes by computing the confidence i.e. average of each node (OPerf)

- If (OPerf < OPerfi), then the node goes to state 1 (cluster head) because its performance OPerfi is greater than OPerf of the received message. Once in state 1, node i triggers a counter Cptr. If after passing this timeout, the node i has received no HELLO message, that means it has no neighbors in its radio range, so it decides to move to state 0 (not decided state).
- If (OPerf > OPerfi), the node goes to state 2 (member)because its performance OPerfi is lower than that of thereceived message. Once in state 2, node i triggers a counterCptr. If after passing this timeout, the node i has received noHELLO message, that means it has no neighbors in its radiorange, so it decides to move to state 0 (not decided state).
- If the node i is in state 1 (respectively in state2), and itreceives a HELLO message with (OPerf < OPerfi)(respectively (OPerf > OPerfi)), it remains

in state 1(respectively remains in state 2) because its state has notchanged.

- If the node i is in state 1 (respectively in state2), and itreceives a HELLO message with (Operf > OPerfi)(respectively (OPerf < OPerfi)), it moves to state 2(respectively move to state 1) because its condition has tochange.

IV. Possible Outcome and Result

In an OLSR network, ECATP performs well when compared with existing protocols with, and without the selfishness attack. The performances of the cluster head in ECATP are much more important. The use of the trust metric offers a great improvement to the algorithm. The cluster life is affected by the selfishness attack, but with the use of the trust metric in the ECATP algorithm the network becomes much more resistant to the selfishness attack. It minimizes the transmission delay, maximizes the successful data delivery rate, and consumes less energy of nodes. Thus, this algorithm improves packet delivery ratio, average end-to-end delay and decreases the drop ratio to a great extent.

V. Conclusion

In MANETs, clustering is an important research topic. Clustering makes it possible to guarantee basic levelsof system performance. A large variety of approaches for adhoc clustering have been presented in recent times. In this paper, an algorithm for efficient clustering is introduced for mobile ad-hoc networks. Its contributions, comparison to existing solutions, are summarized as follows: it does not add any newcontrol message and the network is not overloaded or slowed at all, no changes are made to standard control messages. It works transparently with the standard OLSR protocol.Clusters are formed around the nodes with the highestperformance resources and the densest environment; in otherwords, the node that has the best material resources and has thelargest number of symmetric neighbors is selected as the cluster head. The proposed algorithm takes into account the nodereputation by including it in the calculation of the trust metric. To make the algorithm more stable, the concept of thethreshold of performance is added, which represents the performanceat which each node can act as cluster head. Agreatimprovement and better system stability can be implemented with the adoptedsolution. As future work, the clustering solution can be used to manage cryptographic key in MANETs.

References

[1] Diogo L. P. Machado, Ricardo C. Carrano, Debora C. MuchaluatSaade, “Analysis of Energy Efficient OLSR Extensions and OLSRETX Energetic Optimization Proposal”, *ACM* , pp.65-71, November 2013.

[2] HaiyingShen and Lianyu Zhao, “ALERT: An Anonymous Location-BasedEfficient Routing Protocol in MANETs”,*IEEE TRANSACTIONS ON MOBILE COMPUTING,*Vol. 12, No. 6, pp. 1079-1093, June 2013.

[3] S.K Dhurandher , D.K Sharma, Isaac Woungang, Rohan Gupta, Sanjay Garg, “GAER: genetic algorithm-based energy-efficient routing protocol for infrastructure-less opportunistic networks”,*J Supercomputing,* May 2014.

[4] Ahmed Loutfi , Mohammed Elkoutbi , JalelBenOthman , AbdellatifKobbane, “An energy aware algorithm for OLSR clustering”, *Springer*, pp. 201-207, November 2013.

[5] Keshav Kumar Tiwari and Sanjay Agrawal,” A Secure Reputation-Based Clustering Algorithm”,Vol. 3, Iss. 5,pp 232- 236, May 2013.

[6] MarwahAlmasri, KhaledElleithy, AnasBushang and RemahAlshinina,”TERP : A Trusted and Energy Efficient Routing Protocol for Wireless Sensor Networks(WSNs)”, *IEEE Computer Society*, pp.207-214, 2013

[7] Sheng-Tzong Cheng, Jian-Pan Li, Gwo-JiunHorng,”An Adaptive Cluster-Based Routing Mechanism for Energy Conservation in Mobile Ad Hoc Networks”, *Springer* , pp. 561–579, 15 June 2012

[8] V.G.Rani and Dr.M.Punithavelli, “Optimizing On Demand Weight -Based Clustering Using Trust Model for Mobile Ad Hoc Networks”,International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.1, No.4, December 2010.