International Journal of Computer Applications Technology and Research
Volume 2– Issue 3, 289 - 292, 2013, ISSN: 2319–8656

AN INVERTED LIST BASED APPROACH TO GENERATE OPTIMISED PATH IN DSR IN MANETS – A REVIEW

Sunita
Department of Computer Science and Engineering
BPSMV, Khanpur Kalan
Sonepat,India

Kusum Lata
Department of Computer Science and Engineering
BPSMV, Khanpur Kalan,
Sonepat,India

Rashmi Jatain
Department of Computer Science and Engineering
UIET,MDU
Rohtak,India

Abstract: In this paper, we design and formulate the inverted list based approach for providing safer path and effective communication in DSR protocol.Some nodes in network can participate in network more frequenctly whereas some nodes are not participating. Because of this there is the requirement of such an approach that will take an intelligent decision regarding the sharing of bandwidth or the resource to a node or the node group. Dynamic source routing protocol (DSR) is an on-demand, source routing protocol , whereby all the routing information is maintained (continually updated) at mobile nodes.

Keywords:*MANET,Ad hoc, DSR, Routing Algorithm, Reverse Route*

1.INTRODUCTION

A Mobile ad hoc network is a group of wireless mobile computers (or nodes). In which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. Ad hoc networks require no centralized administration or fixed network infrastructure such as base stations or access points, and can be quickly and inexpensively set up as needed.A MANET is an autonomous group of mobile users that communicate over reasonably slow wireless links. The network topology may vary rapidly and unpredictably over time, because the nodes are mobile.

Dynamic Source Routing (DSR)

Dynamic Source Routing (DSR) is a routing protocol for wireless mesh networks. It is similar to AODV in that it establishes a route on-demand when a transmitting mobile node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Dynamic source routing protocol (DSR) is an on-demand, source routing protocol , whereby all the routing information is maintained (continually updated) at mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network .

An optimum path for a communication between a source node and target node is determined by Route Discovery process. Route Maintenance ensures that the communication path remains optimum and loop-free according the change in network conditions, even if this requires altering the route during a transmission. Route Reply would only be generated if the message has reached the projected destination node (route record which is firstly contained in Route Request would be inserted into the Route Reply).

Advantages and Disadvantages

DSR uses a reactive approach which eliminates the need to periodically flood the network with table update messages which are required in a table-driven approach. The intermediate nodes also utilize the route cache information efficiently to reduce the control overhead.

The disadvantage of DSR is that the route maintenance mechanism does not locally repair a broken down link. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length. In this work the main concern is about to find the frequency of node participation over the network. Lot of work is done in the same direction. Here we are presenting the improved inverted table mechanism to find the most frequent nodes over the network. The method is introduced by K.V.S.R.P.Varma in year 2010. This approach is used by him to idenfiy the similarity and frequency analysis in case of DNA sequencing. He performed the work to find the largest possible node sequence over the network. Lot of work is already done in terms of string extraction, string matching and pattern identification over the string. Frequent Item set Mining plays an essential role in many data mining tasks and applications, such as mining association rules, correlations, sequential patterns, classification and clustering. Frequent item set construction has been a major research area over the years and several algorithms have been proposed in the literature to address the problem of mining association rules.

We are performing the same kind of pattern discovery in case of Mobile pattern identification. For this the improved

inverted table approach is used. The complete work is divided in three basic steps.

I. Identification of Node Sequence

II. Build the Inverted Table for the specific Node Sequence.

III. Frequent Pattern Identification.

1. Identification of Node Sequence

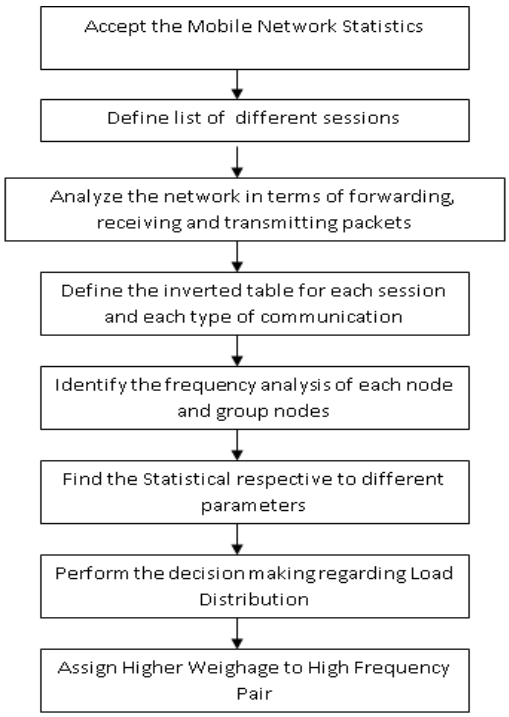
The node sequence is identified by analyzing the communication database of the complete network. We have collected this database from some secondary means that is used by some earlier researcher. The details about the database collection is given above in previous section.[20,27,29]

II. Build the Inverted Table

Inverted matrix is the numerical representation of a string. The rows of the matrix represent the various characters present in the string and are indexed in the order in which they appear in the string. In this proposed we have taken a sequence

III. Frequent Pattern Identification

As the inverted table built, it is capable to answer all the frequency oriented queries. We can find the occurrence of any of node or the node sequence by using inverted table. The main benefit of this approach is that the single inverted table is capable to answer all the user query in terms of node sequence of any length.



SIGNIFICANCE OF WORK

In this work presented work a to find the frequent communicating nodes over the network The proposed system can be implemented on a wired or wireless network. The proposed system is also independent to the network type. It can be mobile network or the wireless lan. . It is the intelligent system that uses the artificial intelligent system approach along with statistical analysis to derive the fair and quick results about the study of allocation of resources to the available nodes. It can search out the users that are doing more utilization of the bandwidth or the time slic. The proposed work we return a reliable and efficient communication over the network.

We focus on one important class of optimizations, index compression. Inverted index compression is used in all major engines, and many techniques have been proposed [26, 29]. Informally, an inverted index for a collection of documents is a structure that stores, for each term (word) occurring somewhere in the collection, information about the locations where it occurs. In particular, for each term t, the index contains an inverted list It consisting of a number of index postings. Each posting in It contains information about the occurrences of t in one particular document d, usually the ID of the document (the docID), the number of occurrences of t in d (the frequency), and possibly other information about the locations of the occurrences within the document and their contexts. The postings in each list are usually sorted by docID. For example, an inverted list It of the form {56, 1,34}{198, 2,14,23} might indicate that term t occurs once in document 56, at word position 34 from the beginning of the document, and twice in document 198 at positions 14 and 23. We assume postings have docIDs and frequencies but do not consider other data such as positions or contexts.Many techniques for inverted index compression have been studied in the literature; see [26, 29] for a survey and [1, 2, 3, 30, 27, 14] for very recent work. Most techniques first replace each docID (except the first in a list) by the difference between it and the preceding docID, called d-gap, and then encode the d-gap using some integer compression algorithm. Using d-gaps instead of docIDs decreases the average value that needs to be compressed, resulting in a higher compression ratio. Of course, these values have to be summed up again during decompression, but this can usually be done efficiently. Thus, inverted index compression techniques are concerned with compressing sequences of integOptimizing other methods We now present a few minor optimizations of some other methods that we used in our experimental evaluation.[23,24]

GammaDiff: This is a variation of Gamma coding that stores an integer x by encoding the unary part of the Gamma code (that is, 1+⌊logx⌋) as the difference between 1+⌊logx⌋and the number of bits required to represent the average of all gaps in the list. The motivation is that when docIDs areclustered, the differences between d-gaps and their average gap may be smaller than the gaps. S16-128: As S9 and S16 only have 9 or 16 possible cases for encoding numbers, sometimes they have to choose a wasteful case when a better one might exist. Now suppose we have a sequence of numbers consisting mainly of small values. In this case, a version of S16 called S16-128 can

do slightly better by providing more cases for small numbers and fewer for larger numbers.

Optimized IPC: Recall that the key step of interpolative coding (IPC) is to encode a number x in the range < lo, hi >, where lo and hi are respectively the lowest and highest possible values of x. The original IPC encodes the offset o = x−lo using a b-bit number, where b = ⌈r⌉ and r = hi−lo+ 1 is the number of possible values of the offset. we apply it to blocks of a certain size. As it turns out, this also improves compression if we choose a good block size. In particular, block sizes of the form 2b−1 appear to work best, and thus we usually choose blocks of size 127.

Frequency Compression

In this section, we first discuss the effect of docID reordering on frequencies, and then propose more effective compression algorithms. In particular, we show that reordered frequencies can be transformed in such a way that their entropy is lowered significantly, leading to better compression.[35 ,37]

5.1 Effect of Reordering on Frequencies

Frequency values by themselves are not changed at all by reordering, and thus reassigning docID by sorting URLs does not affect the distribution of frequencies. However, such an ordering results in more local clusters of similar values. This can be shown by comparing the compressed size of context sensitive and context-free methods.

CONCLUSION

The proposed work is about the prevention of Selfish Node attack. The proposed work is about to improve the DSR protocol in terms of security. As in case of multicast network because of lot of communication the network suffer from some attack that results the packet loss over the network. The proposed work is about to minimize this packet loss over the network. The work will increase the throughput with this improved DSR protocol. The system is providing better throughput and less packet loss over the network. The system is implemented in a wireless network with DSR protocol. In this system an improved inverted list approach is defined to perform the analysis among neighboring nodes and to provide the communication from effective path

REFERENCES

[1] Debdutta Barman Roy,” MADSN: Mobile Agent Based Detection of Selfish Node in MANET”, International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011

[2] Shailender Gupta,” IMPACT OF SELFISH NODE CONCENTRATION IN MANETS”, International Journal of Wireless & Mobile Networks (IJWMN), ISSN : 0975-3834 [Online] ; 0975-4679, Volume: 3 - volume NO: 2 - Issue: April 2011

[3] Dipali Koshti,” Comparative study of Techniques used for Detection of Selfish Nodes in Mobile Ad hoc Networks”, International Journal of Soft Computing and Engineering (IJSCE) ISSN: 2231-2307, 2011

[4] S.Usha,” Multi Hop Acknowledgement Scheme based Selfish Node Detection in Mobile Ad hoc Networks”, International Journal of Computer and Electrical Engineering, International Journal of Computer and Electrical Engineering, Vol. 3, No. 4, August 2011

[5] Martin Schütte,” Detecting Selfish and Malicious Nodes in MANETs”, SEMINAR: SICHERHEIT IN SELBSTORGANISIERENDEN NETZEN, HPI/UNIVERSITÄT POTSDAM, SOMMERSEMESTER 2006

[6] Li Zhao,” MARS: Misbehavior Detection in Ad Hoc Networks”, Global Telecommunications Conference, 2007. GLOBECOM '07. IEEE, 26-30 Nov. 2007, 941 - 945

[7] Md. Amir Khusru Akhtar,” Mathematical Model for the Detection of Selfish Nodes in MANETs”, International Journal of Computer Science and Informatics (IJCSI) ISSN (PRINT): 2231 –5292, Volume-1, Issue-3

[8] Khairul Azmi Abu Bakar,” Contribution Time-based Selfish Nodes Detection Scheme”.

[9] Hongxun Liu,” USING A CACHE SCHEME TO DETECT SELFISH NODES IN MOBILE AD HOC NETWORKS”, Proceeding CIIT '07 The Sixth IASTED International Conference on Communications, Internet, and Information Technology, ACTA Press Anaheim, CA, USA ©2007

[10] Rekhakaushik,” DETECTION AND ISOLATION OF RELUCTANT NODES USING REPUTATION BASED SCHEME IN AN AD-HOC NETWORK”, International Journal of Computer Networks & Communications (IJCNC), Vol.3, No.2, March 2011.

[11] Frank Kargl,” Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks”, Proceeding ESAS'04 Proceedings of the First European conference on Security in Ad-hoc and Sensor Networks Pages 152-165, ISBN:3-540-24396-8, 2005

[12] ”, Jamal N. Al-Karaki,”Stimulating Node Cooperation in Mobile Ad hoc Networks Wireless. Pers Commun (2008) 44:219-239

[13] Bo Wang,” Local Detection of Selfish Routing Behavior in Ad Hoc Networks”, ISPAN '05 Proceedings of the 8th International Symposium on Parallel Architectures, Algorithms and Networks Pages 392 - 399

[14] Deepak Kumar Dixit,” A Trust Based Scheme to Encourage Packet Forwarding in Mobile Ad-hoc Networks”, (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4327 – 4330, ISSN:0975-9646

[15] Anuj Joshi,” Efficient Content Authentication in Ad-Hoc Networks- Mitigating DDoS Attacks”, International Journal of Computer Applications (0975 – 8887)

[16] Alberto Rodriguez-Mayol,” Improving Selfishness Detection in Reputation Protocols for Cooperative Mobile Ad-hoc Networks”, Personal Indoor and Mobile Radio

Communications (PIMRC), 2010 IEEE 21st International Symposium on 26-30 Sept. 2010

[17] T. Jaya," Detection of selfish nodes in Wireless mesh networks using Hierarchial clustering", International Conference on Computing and Control Engineering (ICCCE 2012)

[18] Hadi Otrok," A game-theoretic intrusion detection model for mobile ad hoc networks", Journal of Computer Communications, 31(4):708 − 721, 2008.

[19] Sivaranjani V," Secure Cluster Head Election for Intrusion Detection in MANET", Journal of Computer Applications ISSN: 0974 – 1925, Volume-5, Issue EICA2012-4

[20] Thomas Lochmatter," Misbehaviour Detection using Network Topology and Route Information".

[21] K. Paul," Context Aware Detection of Selfish Nodes in DSR based Ad-hoc Networks", Global Telecommunications Conference, 2002. GLOBECOM '02. IEEE. Volume: 1 Page(s): 178 - 182 vol.1, 2002

[22] Preeti Nagrath," Authenticated Routing Protocol Based on Reputation System For Adhoc Networks", (IJCSE) International Journal on Computer Science and Engineering ISSN : 0975-3397

[23] Sunilkumar S. Manvi," Routing Misbehavior Detection in MANETs Using 2ACK".

[24] Frank Kargl," Sensors for Detection of Misbehaving Nodes in MANETs".

[25] Yanchao Zhang," SIP: A Secure Incentive Protocol against Selfishness in Mobile Ad Hoc Networks", WCNC 2004 / IEEE Communications Society 0-7803-8344-3/04© 2004 IEEE

[26] E.VENKAT REDDY," Trustworthy Robust Routing Protocol for Mobile Ad Hoc Network", International Journal of Engineering Science and Technology ISSN: 0975-5462

[27] Hugo Miranda," Preventing selfishness in open mobile ad hoc networks

[28] Isha V. Hatware," Detection of Misbehaving Nodes in Ad Hoc Routing", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-2459

[29] Hugo Miranda," A Two-Side Perspective on Cooperation in Mobile Ad Hoc Networks".

[30] Isha V. Hatware," Detection of Misbehaving Nodes in Ad Hoc Routing", International Journal of Emerging Technology and Advanced Engineering ISSN 2250-245

[31] Zahra Moradi," Intrusion Detection Model in MANETs using ANNs and ANFIS", 2011 International Conference on Telecommunication Technology and Applications Proc .of CSIT

[32] S. D. Khatawkar," Detection of Routing Misbehavior in MANETs", 2011 International Conference on Computer and Software Modeling IPCSIT

[33] Oscar F. Gonzalez," Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks", JOURNAL OF INTERNET ENGINEERING

[34] Michael Wayne Probus," SELFISH NODE ISOLATION IN MOBILE AD-HOC NETWORKS".

[35] Djamel Djenouri," Struggling Against Selfishness and Black Hole Attacks in MANETs".

[36] Oscar F. Gonzalez," Detection of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks".

[37] V.Vasanthi, P.Nagarajan, "A Perspective Analysis of routing protocols in wireless sensor network", International Journal on Computer Science and Engineering Vol. 02, No. 08, 2010, 2511-2518