Identifying Stable Network in Mobile Ad-Hoc Networks

S.Vikram Phaneendra
Assistant Professor
Computer Science & Engineering
Madanapalle Institute of Technology & Science
Madanapalle -517325
Andhra Pradesh, India.

Sreenivasulu. T
Assistant Professor
Computer Science & Engineering
Madanapalle Institute of Technology & Science
Madanapalle -517325
Andhra Pradesh, India.

B. Jalaja Kumari[3]
Assistant Professor
Computer Science & Engineering
Madanapalle Institute of Technology & Science
Madanapalle -517325
Andhra Pradesh, India.

ABSTRACT
In a Wireless Networks, Quality of Service has become a logical step because of the increasing popularity of using multimedia and real time applications in different potential commercial in MANETs. Resource allocation and Reservation are the part of QoS to satisfy the application requirements. Bandwidth, delay, delay-jitter and packet to loss ratio are the requirements. The complexity in QoS routing in MANETs is to maintain the path constantly till the end of the transmission. Lack of resources in the network as well as frequent changes in the network topology has made MANETs a challenging task. The open problem in the networks is even though lots of research made to support QoS in Internet and other networks, they are not suitable for MANETs. Quality of Service is proposed in this paper in terms of reliable packet transmission, multiple connections and stable routes. This paper offers good adaptation to dynamic linking, distributed processing. Proposed scheme is incorporated using NTP protocol and it also offers low processing overhead and loop freedom al all times.

Keywords: QoS, NTP Protocol, Stable Network.

1. INTRODUCTION
Rapid growth in the deployment of portable wireless devices including wireless multimedia had taken place in the past decade. To establish communication between the wireless devices, without the help of base stations or other pre-existing infrastructure, an archetypical infrastructure-less wireless packet network called MANETs is used. Nodes in the transmission range can communicate with mobile node directly. Nodes outside the range must necessarily be multi-hop and require establishing the communication paths [1].

Communication paths to be established for the most of multimedia applications to satisfy negotiated parameters like delay or bandwidth, in turn refers QoS guarantee. The reason for lot of problems to remain before more efficient solutions are found for QoS routing in MANET are dynamic nature of the network topology and imprecise network static information. An active path, alternative paths are established for data transmission [4]. An active path fails due to mobility, alternate path is sought and data is transmitted. Failure detection costs high before a path is "pronounced dead", several retries have to time-out. Before the failure is detected packets experience large delays and a new path is made this happens when path fails. In order to establish route from source to destination, link between each node must be ensured. Prediction of node movement can be done by using current information becomes the key of productive root stability.

In recent years several ad-hoc routing protocols for MANETs are proposed. For example Distance Vector Routing, Optimized Link State Routing Protocol. Ad-hoc On-demand Distance Vector Routing (AODV), and Dynamic Source Routing belongs to shortest path routing, i.e., based on shortest path algorithms which are not strong enough for time-varying-radio-link cases.

2. WHY PROTOCOLS ARE USED?
Knowing a communication protocol is knowing the types of devices that might be used ot protect a process control network. Actually, protocols are the rules that govern network communication, i.e.., set of rules that define how two communicating parties communicate each other. A protocol in any network must provide set of rules for different communication functions. For example, Error Checking, Flow Control, Data Conversion and Message Routing. Protocols are arranged in a layered architecture, so as to provide a clear idea that how one protocol interacts with another. Protocols have their own task in each layer in a model. By this we will come to know that in communication network specific layer will have specify task and in layered model, lower level layers provides services to the above level layers [2,5].

3. RELATED WORK
Striking factor in and outside the MANETs is secure routing in the network of networks. The solutions proposed mainly focuses on the existence of a line of defence separating the fixed routing infrastructure from all other network entities. This is done by distributing a set of Public Keys/ Certificates thus show the importance of the authority of the router to act within the employed protocol limits and data transmissions are to be authenticated. Such approaches cannot contest a single malicious router disseminating incorrect topological information, they are not applicable in the MANET context, because of the absence of fixed infrastructure and central entity. The major "Road Block" in commercial application of this technology is that the security of MANET routing protocols. Efforts mainly concentrated on data forwarding this regarding the aspect of topology discovery.

The packet dropping can be eliminated by two mechanisms. (1) Detect misbehaving nodes and report such events and (2)

maintain a set of metrics that reflects the past behaviour of other nodes. Node chooses the best route incorporated with well behaved nodes (i.e.., nodes do not avoid forwarding packets along established routes). Packets carry the entire route that becomes known to all intermediate nodes without the loss of the segmented packets during the transmission of the packet and reaching to its destination is verified by the node operating in promiscuous mode. If any node is improper and detected as misbehaving node, a report is generated and nodes update the rating of the misbehaving node. The ratings of nodes along a well-behaved route are incremented periodically while reception of a misbehaviour alert dramatically decreases the node rating.

The source node calculates the path metric equal to the average of the ratings of the nodes in each of the route replies, and highest metric route is selected whenever a new route is needed. Shared channel and Source routing are the two features detected in MANET. Mostly the authors may give the incorrect detection as a solution. Thus, improves the situation where a misbehaving node will undergo suspecting for a long period of time. The metric construction is the reason for a route choice which includes a suspected node. For example, the number of hops is high, and then the low rating is "average out". At-last, a node reports itself, giving feedback in terms of authentication or correctness. Fake alerts may be generated and this could be a attack resulting in the disabling the network operation. The performance of the network will be degraded, when a protocol attempts to find the new route, and the route replies that it is free of suspected node, and due to excessive requests also. Every node follows the protocol rules; i.e.., properly rely the user data. The concept of fictitious currency is introduced, in order to *endogenize* the behaviour of the assumed greedy nodes, which would forward packets in exchange for currency. Each intermediate node purchases from its predecessor the received data packet and sells it to its successor along the path to the destination. Eventually the destination pays for the received packet.2 this scheme assumes the existence of an overlaid geographic routing infrastructure and a *Public Key Infrastructure (PKI).* All nodes are pre-loaded with an amount of currency, have unique identifiers, and are associated with a pair of private/public keys and all cryptographic operations related to the currency transfers are performed by a physically tamper-resistant module. The applicability of the scheme, which targets wide-area *MANET*, is limited by the assumption of an on-line Certification Authority in the *MANET* context. Moreover, nodes could flood the network with packets destined to non-existent nodes and possibly lead nodes unable to forward purchased packets to starvation. The practicality of the scheme is also limited by its assumptions, the high computational overhead (hop-by-hop public key cryptography, for each transmitted packet), and the implementation of physically tamper-resistant modules.

A route satisfying certain quantifiable security criteria improves the Quality-of-Service as an additional factor by protecting the route discovery process. Nodes in a MANET subnet are divided into different trust and privilege levels. A route discovery sets the security level for the route by a node. i.e.., required minimal trust level for nodes participating in the query or reply propagation.

Symmetric Encryption and Decryption keys are shared by nodes at each level. Intermediate nodes at any level cannot decrypt internal routing packets, and without finding whether the QoS parameters can be satisfied or not they drop them. Although this method provides integrity of routing protocol traffic, it does not eliminate false routing information provided by malicious nodes. The proposed use of symmetric cryptography allows any node to corrupt the routing protocol operation within a level of trust. This is achieved by escalating virtually any attack that would be possible without the presence of the scheme. Finally, the assumed supervising organization and the fixed assignment of trust levels does not pertain to the *MANET* paradigm. In essence, the proposed solution transcribes the problem of secure routing in a context where nodes of a certain group are assumed to be trustworthy, without actually addressing the global secure routing problem.

Extension to the Ad-Hoc On-Demand Distance Vector Routing Protocol has been proposed to protect the routing protocol messages. Secure-AODV scheme assumes that each node has certified Public Keys of all network nodes thus, the intermediate nodes can know all in-transit routing packets. The basic idea is that the originator of a control message appends an *RSA signature* and the last element of a *hash chain* (i.e., the result of *n* consecutive hash calculations on a random number). It is the responsibility of the intermediate nodes to verify the Signature and Hash value of the message while it is being transmitted in a network, and generate the k-th element of the hash chain, with k being the number of traversed hops and places in the packet. The route replies with the active route towards the destination either by intermediate nodes or by destination nodes.

4. THE NETWORK TIME PROTOCOL

The Network Time Protocol (NTP) [Mills 1995] defines architecture for a time service and a protocol to distribute time information over the Internet. NTP's chief design aims and features are as follows:

To provide a service enabling clients across the Internet to be synchronized accurately to UTC: Although large and variable message delays are encountered in Internet communication, NTP employs statistical techniques for the filtering of timing data and it discriminates between the quality of timing data from different servers.

To provide a reliable service that can survive lengthy losses of connectivity: There are redundant servers and redundant paths between the servers. The servers can reconfigure so as to continue to provide the service if one of them becomes unreachable.

To enable clients to resynchronize sufficiently frequently to offset the rates of drift found in most computers: The service is designed to scale to large numbers of clients and servers.

To provide protection against interference with the time service, whether malicious or accidental: The time service uses authentication techniques to check that timing data originate

from the claimed trusted sources. It also validates the return addresses of messages sent to it.

The NTP service is provided by a network of servers located across the Internet. Primary servers are connected directly to a time source such as a radio clock receiving UTC; secondary servers are synchronized, ultimately, with primary servers. The servers are connected in a logical hierarchy called a synchronization subnet

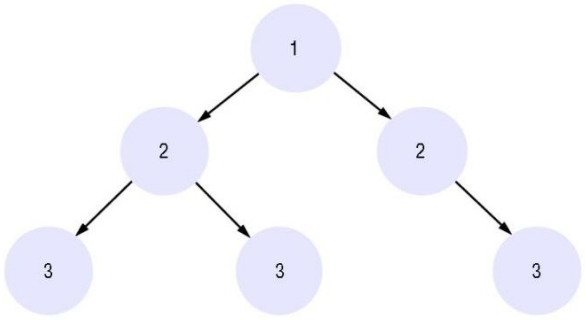

Figure 1: An example synchronization subnet in an NTP implementation

Arrows denote synchronization control, numbers denote strata. Whose levels are called strata. Primary servers occupy stratum 1: they are at the root. Stratum 2 servers are secondary servers that are synchronized directly with the primary servers; stratum 3 servers are synchronized with stratum 2 servers, and so on. The lowest-level (leaf) servers execute in users' workstations.

The clocks belonging to servers with high stratum numbers are liable to be less accurate than those with low stratum numbers, because errors are introduced at each level of synchronization. NTP also takes into account the total message round-trip delays to the root in assessing the quality of timekeeping data held by a particular server.

The synchronization subnet can reconfigure as servers become unreachable or failures occur. If, for example, a primary server's UTC source fails, then it can become a stratum 2 secondary server. If a secondary server's normal source of synchronization fails or becomes unreachable, then it may synchronize with another server.

NTP servers synchronize with one another in one of three modes: multicast, procedure-call and symmetric mode. *Multicast mode* is intended for use on a high-speed LAN. One or more servers periodically multicasts the time to the servers running in other computers connected by the LAN, which set their clocks assuming a small delay. This mode can achieve only relatively low accuracies, but ones that nonetheless are considered sufficient for many purposes.

Procedure-call mode is similar to the operation of Cristian's algorithm. In this mode, one server accepts requests from other computers, which it processes by replying with its timestamp (current clock reading). This mode is suitable where higher accuracies are required than can be achieved with multicast, or where multicast is not supported in hardware. For example, file servers on the same or a neighbouring LAN that need to keep accurate timing information for file accesses could contact a local server in procedure-call mode.

Finally, *symmetric mode* is intended for use by the servers that supply time information in LANs and by the higher levels (lower strata) of the synchronization subnet, where the highest accuracies are to be achieved. A pair of servers operating in symmetric mode and them exchange messages bearing timing information. Timing data are retained as part of an association between the servers that is maintained in order to improve the accuracy of their synchronization over time.

In all modes, messages are delivered unreliably, using the standard UDP Internet transport protocol. In procedure-call mode and symmetric mode, processes exchange pairs of messages. Each message bears timestamps of recent message events: the local times when the previous NTP message between the pair was sent and received and the local time when the current message was transmitted. The recipient of the NTP message notes the local time when it receives the message. The four times $Ti - 3$, $Ti - 2$, $Ti - 1$ and Ti are shown in the following Figure for the messages m and m' sent between servers A and B.

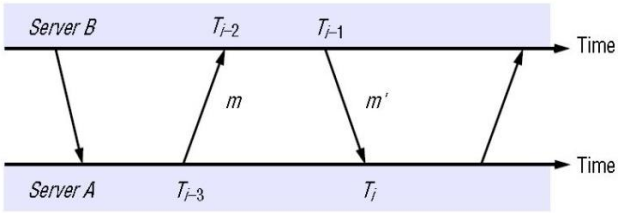

Figure 2: Messages exchanged between a pair of NTP peers

Note that in symmetric mode, unlike in Cristian's algorithm, there can be a non-negligible delay between the arrival of one message and the dispatch of the next. Also, messages may be lost, but the three timestamps carried by each message are nonetheless valid.

For each pair of messages sent between two servers the NTP calculates an *offset oi*, which is an estimate of the actual offset between the two clocks, and a *delay di*, which is the total transmission time for the two messages. If the true offset of the clock at B relative to that at A is o, and if the actual transmission times for m and m' are t and t', respectively, then we have:

$$Ti - 2 = Ti - 3 + t + o \text{ and } Ti = Ti - 1 + t' - o$$

This leads to:

$$di = t + t' = Ti - 2 - Ti - 3 + Ti - Ti - 1$$

and:

$$o = oi + (t' - t) / 2, \text{ where } oi = (Ti - 2 - Ti - 3 + Ti - 1 - Ti) / 2$$

Using the fact that $t, t' \geq 0$, it can be shown that $oi - di/2 \leq o \leq oi + di/2$. Thus oi is an estimate of the offset, and di is a measure of the accuracy of this estimate. NTP servers apply a data filtering algorithm to successive pairs $<oi, di>$, which estimates the offset o and calculates the quality of this estimate as a statistical quantity called the *filter dispersion*. Relatively high filter dispersion represents relatively unreliable data. The eight most recent pairs $<oi, di>$ are retained. As with Cristian's algorithm, the value of oj that corresponds to the minimum value dj is chosen to estimate o.

The value of the offset derived from communication with a single source is not necessarily used by itself to control the local clock, however. In general, an NTP server engages in message exchanges with several of its peers. In addition to data filtering applied to exchanges with each single peer, NTP applies a peer-selection algorithm. This examines the values obtained from exchanges with each of several peers, looking for relatively

unreliable values. The output from this algorithm may cause a server to change the peer that it primarily uses for synchronization.

Peers with lower stratum numbers are more favoured than those in higher strata because they are 'closer' to the primary time sources. Also, those with the lowest *synchronization dispersion* are relatively favoured. This is the sum of the filter dispersions measured between the server and the root of the synchronization subnet. (Peers exchange synchronization dispersions in messages, allowing this total to be calculated.)

NTP employs a phase lock loop model [Mills 1995], which modifies the local clock's update frequency in accordance with observations of its drift rate. To take a simple example, if a clock is discovered always to gain time at the rate of, say, four seconds per hour, then its frequency can be reduced slightly (in software or hardware) to compensate for this. The clock's drift in the intervals between synchronization is thus reduced.

Mills quotes synchronization accuracies on the order of tens of milliseconds over Internet paths, and one millisecond on LANs [3].

5. IDENTIFYING STABILITY

Symmetric mode is intended for use by the servers that supply time information in LANs and by the higher levels (lower strata) of the synchronization subnet, where the highest accuracies are to be achieved. A pair of servers operating in symmetric mode then can exchange messages bearing timing information. Timing data are retained as part of an association between the servers that is maintained in order to improve the accuracy of their synchronization over time.
In between any two processes we can send and receive messages in 4 times, we can conclude that available channel is stable. This statistical type data in symmetric mode, we can easily identify between any two or more processes or nodes we can identify that channel is stability or not.

6. CONCLUSION

Logical step of Quality of Service (QoS) over wireless network is to ensure that the established path for a connection does not break before the end of the data transmission. Mobile Ad hoc networking is a challenging task due to the lack of resources in the network as well as the frequent changes in the network topology. In this paper method is used symmetric method of Network Type Protocol (NTP) and after getting statistical data, we can easily differentiated stable networks.

7. REFERENCES

[1] R. Dube, C.D. Rais, K.Y. Wang, and S.K. Tripathi, "Signal stability based adaptivc routing (SSA) for ad hoc mobile networks," IEEE Personal Communications, vol. 4, no. 1, pp. 36-45, 1997.

[2] Shio Kumar Singh 1, M P Singh 2, and D K Singh 3, "Routing Protocols in Wireless Sensor Networks – A Survey" International Journal of Computer Science & Engineering Survey (IJCSES) Vol.1, No.2, November 2010.

[3] George Coulouries, Jean Dollimore, Tim Kindberg, "Distributed System Concepts and Design, 4th Edition, 2009.

[4] Fei Hu, Sunil Kumar, "Wireless Sensor Networks for Mobile Telemedicine: QoS support", IEEE Transactions on Information Technology in Bioinformatics, (under final review), 2003.

[5] S. Murthy, J.J. Garcia-Luna-Aceves, "An Efficient Routing Protocol for Wireless Networks", ACM Mobile Networks and App. Journal, Special Issue on Routing in Mobile Communication Networks, Oct. 1996, pp. 183-97.

[6] A.Kush, R.Chauhan, C.Hwang, P.Gupta "Stable and Energy Efficient Routing for Mobile Adhoc Networks" Proceedings of the Fifth International Conference on Information Technology: New Generations, Pages 1028-1033, 2008 ISBN: 978-0-7695-3099-4 available at ACM Digital Portal.