2011 International Conference on Advancements in Information Technology
With workshop of ICBMG 2011
IPCSIT vol.20 (2011) © (2011) IACSIT Press, Singapore

Global Contribution Robots Secure Multichannel Routing Protocol in MANET

Mahesh.K.Kaluti[1+], Harshal Shah[2], Nihil Khagram[3] and Paresh Tanna[4]

[1]Dept of IT, OSEC
[2] CSE/ IT, OSEC
[3] IT, OSEC
[4]RK-Univeristy

Abstract: Know a day's achieving a most reliable security in the field of the MANET is emerging as a new way and new approach to achieve better Quality of service and making the system more Robust, More Secure but achieving reliability is one of the challenging task which further opens a new way to carry out more research in the field of MANET. Here in this paper we are introducing GCRSMR (Global Contribution Robots Secure Multichannel Routing Protocol) protocol which is designed by using various approaches that includes GC-Algorithm, Robust Source Routing Mechanism and the concept of Multicast routing scheme to make reliable robust secure communication in MANET.

Keywords: global, quality, robust, multicast, reliable.

1. Introduction

In the earlier research towards achieving secure multichannel robust transmissions in MANET introduces the various methodologies but here we are introducing the a protocol known as Global Contribution Robots Secure Multichannel Routing Protocol[5] which includes concept of GC algorithm which first calculates a global score for each peer that accurately reflects its bandwidth contribution to the entire network. Ones global score was calculated then these scores are used in a proposed data transfer policy to determine whether one peer can download data from other peers. Basically the approach of the GC Algorithm[1] is to achieve efficiently preventing free riding, naturally balancing the upload and download amounts in each peer, reducing rejections in transactions between cooperative peers. Moreover, the GC algorithm requires only private transaction history as an input and can be fully decentralized. Also, its time complexities are approximately O(N2) in a centralized system and O(N) per peer in a decentralized system and the further the concept of achieving security is also to be considered to make the system more robust, stable and reliable multicast routing protocols for MANETs to ensure better packet delivery ratio, lower delays and reduced control overheads.

To achieve the above task, its necessity to consider the aspects of mesh based multicast routing scheme where one can find stable multicast path from source to receivers. and is constructed by using route request and route reply packets with the help of multicast routing information cache and link stability database maintained at every node. The stable paths are found based on selection of stable forwarding nodes that have high stability of link connectivity. The link stability is computed by using the parameters such as received power, distance between neighboring nodes and the link quality assessed using bit errors in a packet. The securities measures are to be assured by using by using secure on-demand MANET routing protocol, which leads to the to achieve the a reliable, Global Contribution Robust Source Routing (GCRSR). In addition to all

+ Corresponding author. Tel.: + 08353223615.
E-mail address: Mahesh.rkcet@gmail.com.

concept here this protocol also able to mitigate against intelligent malicious agents which selectively drop or modify packets they agreed to forward. Simulation studies confirm that GCRSMR is capable of maintaining high delivery ratio in MANET.

2. How GC Algorithm Works?

GC algorithm work with such a mechanism that balances each node's upload/download amounts of data in the MANET network, where simple 'Upload/Download Balance' (UDB) technique is used, in which basically a peer is allowed to download from any other peer only if its upload amount ≥download amount in order to make an unfair network fairer, intuitively following rules are adapted:

- Give high contribution nodes priority for downloading from other nodes.
- Restrain low contribution nodes from downloading.
- Encourage every node to download from low contribution nodes rather than from high Contribution nodes.

Based upon the rules described above, the following keys to be used for determining the GC as follows:

- A node which uploads much data and downloads little data, obtains a high contribution.
- Upload to a high contribution node increases more contribution than upload to a low contribution node such as a free rider.
- Download from a high contribution (busy) node loses more contribution than download from a low contribution (free) node.

To achieve multicast routing and assuring the security in MANET we also consider the behavior of the network where actually nodes misbehave which will leads to the malicious behavior of the network &the broken nodes are non-functional at this level to achieve the security a node can agree to forward its traffic on behalf of other nodes but becomes non-functional prior to it filling this agreement and selfish nodes can agree to forward packets but silently drop the packets in attempt to conserve energy and bandwidth. Malicious nodes may seek to disrupt a network and hide their malicious behavior by selectively dropping packets they agreed to forward.

And our proposed protocol to achieve the above criteria it considers the concept of associativity-Based Multicast Routing[5] which will improve the routing based on mesh structure for connecting multicast members in the network here the concept of next hop information is considered during data transmission, and uses periodical queries/replies to refresh routes constituting the mesh, requiring more control and communication overhead.

Actually, most existing multicast protocols face many problems in tree maintenance and frequent reconfiguration during link failures. Most of the protocols used in the MANET depend on upstream and downstream nodes requiring storage and control overhead. Moreover, and proposed Global Contribution[1] Robots Secure Multichannel Routing Protocol is one of secure novel multicast routing protocol for mobile ad hoc networks.

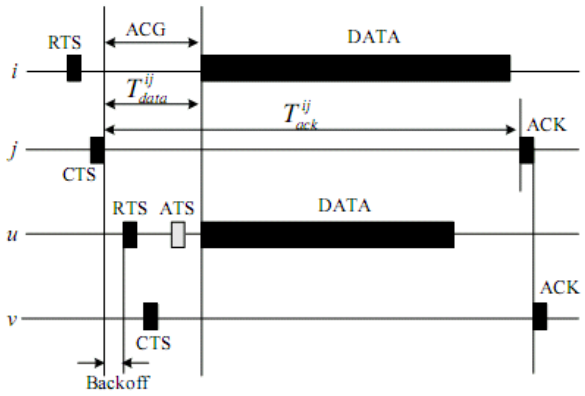

Fig.1: Basic Operation of GCRSMR between two nodes

3. At What Level GCRSMR-System Assure the Security?

In this section we mainly highlight the security [3] aspects of the GCRSMR which also present a more precise description of our proposed protocol in which priority for the multicast routing should be considered on the following issues of the MANET in which

- Each node has a unique identifier, and also it has a time bound
- Each node has a valid certificate and the public keys of the CAs
- The wireless communication links between the nodes are symmetric.
- The link-layer of the MANET nodes provides transmission error detection service.
- Any given intermediate node on a path from a source to a destination may be malicious and therefore cannot be fully trusted.

4. Criteria's for Robustness

The robustness feature of the proposed protocol was achieved by considering the major aspects and additional metrics.

- Delay: Delay is defined as the average time spent by a packet in the MAC queue, i.e. from the instant it is enqueued till its transmission is complete.
- Throughput: Throughput is the fraction of the channel capacity used for data transmission.
- Fairness: A MAC protocol is fair if it does not exhibit preference to any single node when multiple nodes are trying to access the channel. This results in fair sharing of the bandwidth [6].
- Stability: Due to overhead in the protocol, the system may be able to handle sustained source loads that are much smaller than the maximum transmission capacity of the channel.
- Robustness against Channel Fading: The wireless channel is time-varying and error- prone.
- Power Consumption: Most wireless devices have limited battery power. • Support for Multimedia: With the convergence of voice, video, and data networks.

5. Conclusion

GCRSMRis a secure MANET on-demand routing protocol which is capable of delivering packets to their respective destinations even in the presence of large proportions of active malicious or selfish agents which selectively drop packets they are required to forward. GCRSMR introduced the concept of forerunner (FR) packets which inform nodes along a path that they should expect specified data flow within a given time frame. The path elements can therefore be on the lookout for the given data flow, and in the event that they do not receive the traffic flow, they can transmit info to the source informing it that the data flow they expected did not arrive. In so doing, links with active malicious agents can be identified, and the malicious agents be eventually isolated GCSRS algorithm which Also calculates each peer's global contribution in a P2P network, and explained how to use it for transactions. However, it still requires much work to improve security and to investigate other transaction procedures. Furthermore,

6. References

[1] Claude Cr´ epeau, Carlton R. Davis∗ and Muthucumaru Maheswaran A secure MANET routing protocol with resilience against byzantine behaviours of malicious or selfish nodes,School of Computer Science, McGill University,

[2] Rajashekhar Biradar, Sunilkumar Manvi, Member, IACSIT , Mylara Reddy Mesh Based Multicast Routing in MANET: Stable Link Based Approach, International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010,1793-8163

[3] Kaan Bur, Cem Erosy, "Ad Hoc quality of service multicast routings",Computer communications, Vol. 29, 2005, pp. 136-148.

[4] Hui Cheng a, Jiannong Cao, Xingwei Wang, "A fast and efficient multicast algorithm for QoS group communications in heterogeneous network", Computer communications, Elsevier, Vol. 30, 2007 pp.

[5] Khalid A. Farhan, "Network sender multicast routing protocol", Proceedings of seventh IEEE International conference on networking,

[6] Ns2 network simulator. http://www.isi.edu/nsnam/ns.

[7] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens. An on-demand secure routing protocol resilient to byzantine failures. In Proceedings of the ACM workshop on Wireless security (WiSE ’02), pages 21–30, September