Volume 2, No. 4, July-August 2011

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Comparison of ODMR and IODMR Protocols in Manets using PKC Security Model

Shavinder Bajwa*
M.tech Student of CSE Dept.
CEC, Landran. Mohali, INDIA
Shavinder_87@hotmail.com

Sandeep Kang
Assistant professor of CSE Dept.
CEC, Landran. Mohali, INDIA
Cecm.cse.skang@gmail.com

Amanjot Singh
CSE Dept. CEC,Landran.
Mohali, INDIA
Amanjotmundi@gmail.com

Abstract: Mobile Ad-hoc networks have been the focus of reseacrch interest in wireless networks. An ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use any existing network infrastructure or centralized administration. Mobile ad-hoc networks are open to a wide range of attacks due to their unique characteristics like open medium, dynamically changing topology,absence of infrastructure, resource constraint and trust among nodes This paper focuses on the comparison between two Multicast Routing Protocols ODMRP and Improved ODMR (IODMRP) with PKC security Model.

Keywords: Multicast, Ad-hoc wireless networks (MANETS), ODMRP, IODMRP, PKC.

I. INTRODUCTION

A mobile ad-hoc network is a self-configuring network of mobile routers (and associated hosts) connected by wireless links—the union of which form an arbitrary topology. The routers are free to move randomly and organize themselves arbitrarily; thus, the network's wireless topology may change rapidly and unpredictably. The mobile nodes co-operate with each other to perform a particular task [1]. The node acts as a sender, receiver or relay. Every node will discover the routing path by using route request and route reply packets. Route maintenance is also required as the node changes its position so its route also. Mobile ad-hoc network is presently applicable everywhere in real life like in business meetings outside the offices,Bluetooth , etc.

A. General Ad-Hoc Network:

The following flowchart depicts the working of any general ad-hoc network

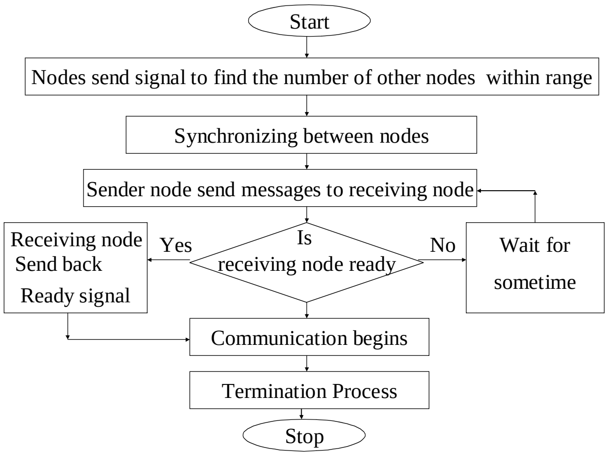
Start
Nodes send signal to find the number of other nodes within range
Synchronizing between nodes
Sender node send messages to receiving node
Receiving node
Send back
Ready signal
Yes
Is
receiving node ready
No
Wait for
sometime
Communication begins
Termination Process
Stop

Figure 1: Working of a general Ad-Hoc Network

II. `MANET MULTICAST ROUTING

Multicasting [2] can defined as transmission of data packets to several destinations at the same time. Transmitter may be a single or multiple nodes which are said to be "one to many" nodes or " many to many" nodes.

In general multicast routing is achieved using either

a. Source based-when no. of multicast senders in a group are small(e.g.-video on demand application)
b. Core based trees-uses a multicast tree shared by all members of a group.

Multicast forwarding is based on nodes rather than on links.

III. ROUTING PROTOCOLS

The main objectives of MANET routing protocols are to maximize network throughput, to maximize network lifetime, to maximize energy efficiency and to minimize delays. The network throughput is measured by packet delivery ratio and energy contribution is measured by routing overhead which is number or size of routing control packets.

A. Multicast Topology:

Topology[1] is defined as how multicast session's nodes are arranged in a known topology shape. Multicast routing protocols can be divided into two main categories: Tree-based protocols and Mesh-based protocols.

Tree-based proposals are also divided into two subcategories:

Source-based tree and shared-based tree approaches.

a. In source-based tree approaches, each source builds its single tree.
b. In shared-based tree approaches, all sources share only a single tree that is controlled only by one or more specific nodes.

IV. MULTICAST PROTOCOLS REVIEW

A. *On-Demand Multicast Routing Protocol (Odmrp):*

ODMRP (On-Demand Multicast Routing Protocol) is a popular multicast protocol for wireless ad hoc networks. The strengths of ODMRP are simplicity, high packet delivery ratio, and non-dependency on specific unicast protocols. Owing to performing scoped flooding of packets ODMRP suffers from excessive control overhead and redundant data transmissions when the number of multicast source increases, which simultaneously leads to increasing network load and waste of the limited resources of the nodes. In order to cope with the problems, we propose an improved ad hoc multicast routing protocol based on ODMRP referred to as IODMRP.

In IODMRP, it is not all the nodes but partial nodes in forwarding group that relay packets, the partial ones are dynamic and chosen based on the forwarder's density and power state. Through a course of simulation experiments, the performance of IODMRP is compared to ODMRP, The simulation results show that IODMRP reduces the redundant data transmissions, enhances the transmission efficiency and extend the network lifetime, the performance of the network is improvedIt chooses partial forwarding nodes to relay packets, the number of which is decided by probabilistic forwarding algorithm based on forwarder’s density and the nodes are selected according to energy state.ODMRP has the following functions.

a. Provides a richer connectivity among multicast members using a mesh based approach.
b. Supplies multiple route for one particular destination.
i. Helps in case of topology changes and node failure.
a. Uses a concept of Forwarding Group.
ii. Only a subset of nodes forwards multicast packets via scoped flooding.

a) *Algorithm Description:*

a. S floods a Join Query to entire network to refresh membership.
b. Receiving node stores the backward learning into routing table and rebroadcasts the packet.
c. Finally when query reaches a receiver creates a Join Reply and broadcasts its to its neighbors.
d. Node receiving the Join Reply checks whether the next node id in Join Reply matches it own. If yes , it is a part of the forwarding group.
e. Sets its FG_FLAG and broadcasts its join reply built upon matched entries
f. Join Reply is propagated by each forwarding group member until it reaches source via a shortest path.
g. Routes from sources to receivers builds a mesh of nodes called “**forwarding group**”.

B. *Improved On-Demand Multicast Routing Protocol (Iodmrp):*

IODMRP is the enhanced result of ODMRP. It is a more efficient multicast routing protocol.It chooses partial forwarding nodes to relay packets, the number of which is decided by probabilistic forwarding algorithm based on forwarder’s density and the nodes are selected according to energy state.This protocol is implemented through simple modifications to existing ODMRP, but we reduce the redundant data transmissions and save energy significantly through decreasing the forwarding packets.It employs the algorithm of self-adapting probability, which means adjusting probability according to local density of forwarders. When the number of neighbor forwarding nodes is small the probability is 100% to guarantee high packet delivery ratio, on the contrary play down the probability to cut down partial contention and congestion, hence the transmission efficiency is heightened and the performance of the network is improved. The establishing and updating of the forward structure in IODMRP is the same as ODMRP. It has a better end to end delay and delivery ratio than ODMRP with increasing senders.

C. *Public Key Cryptography As A Security:*

The data transferred from one system to another over public network can be protected by the method of encryption. On encryption the data is encrypted/scrambled by any encryption algorithm using the ‘key’. Only the user having the access to the same ‘key’ can decrypt/de-scramble the encrypted data. This method is known as private key or symmetric key cryptography. In public key cryptography each user or the device taking part in the communication have a pair of keys, a public key and a private key, and a set of operations associated with the keys to do the cryptographic operations. Only the particular user/device knows the private key whereas the public key is distributed to all users/devices taking part in the communication. Since the knowledge of public key does not compromise the security of the algorithms, it can be easily exchanged online.

Cryptography is the science of writing in secret code and is an ancient art; the first documented use of cryptography in writing dates back to circa 1900 B.C. It is no surprise, then, that new forms of cryptography came soon after the widespread development of computer communications. In data and telecommunications, cryptography is necessary when communicating over any untrusted medium, which includes just about *any* network, particularly the Internet. PKC uses one key for encryption and another for decryption. Hash Functions are used as a mathematical transformation to irreversibly "encrypt" information.

V. PROPOSED METHODOLOGY

a. Create a Wireless Network.
b. Installation of Network Simulator Version 2.
c. Implementation of IODMR Protocol in NS 2.
d. Implementation of Seniority Based Pretty Good Privacy Model in NS 2.
e. Integrate the Security Model with IODMRP.
f. Compare the performance of new security model with ODMRP and PKC.

A. *Simulation Environment:*

NS2 is used to simulate the proposed algorithm. The distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol is used. It has the functionality to notify the network layer about link breakage.The trace files and nam files are to be generated according to the need. Nodes in simulation move according to "random way mobility model".ODMRP[5] is compared with IOMRP with PKC.

The evaluation is mainly based on performance according to the following metrics:

© 2010, IJARCS All Rights Reserved

a. *Packet Delivery Ratio:*

Packet delivery ratio is calculated by dividing the number of packets received by the destination through the number of packets originated by source. It specifies the packet loss rate, which limits the maximum throughput of the network. The better the delivery ration, the more complete and correct the routing protocol.

b. *End to End Delay:*

Average end-to-end delay is the average time a data packet takes to reach to the destination in seconds. It is calculated by subtracting "time at which first packet was transmitted by source" from "time at which first data packet arrived to destination. It includes all possible delays caused by buffering during latency, queuing at the interface queue, retransmission delays at MAC, Propagation and transfer times. It is the metric significant in understanding the delay introduced by path discovery.

c. *Throughput :*

The number of routing packets transmitted per data packet delivered at the destination. Each hop-wise transmission of a routing packet is counted as one transmission**.**

VI. CONCLUSION AND DISCUSSION

This paper describes about the comparison of ODMRP and IODMRP multicast protocols with PKC security model. This paper describes only the outline of the research that is to be carried out. The comparison between the these two protocols is to be carried out based on the three metrics and to see which protocol is better among these two multicast protocols would take time.

VII. REFERENCES

[1] Moukhtar A. Ali, Ayman EL-SAYED and Ibrahim Z. MORSI," A Survey of Multicast Routing Protocols for Ad-Hoc Wireless Networks", Proceedings of the Minufiya Journal of Electronic Engineering Research (MJEER), Vol. 17, No. 2, July 2007

[2] Zhi Ren, Wei Guo, "Research Advance on Ad Hoc Multicast Routing Protocols", Computer Science (in Chinese), vol. 31, pp.7-14, Mar.2004.

[3] S.-J. Lee, W. Su, J. Hsu, M. Gerla and R. Bagrodia "A Performance Comparison Study of Ad Hoc Wireless Multicast Protocols", Proceedings of IEEE INFOCOM 2000,Tel Aviv, Israel, March 2000.

[4] Lee S J, Su W, Gerla M. "On-demand multicast routing protocol in multihop wireless mobile networks", Mobile Networks and Applications, vol.7, pp. 441-453, Jun, 2002

[5] V. Karpijoki, 'Security in Ad-hoc Networks', Helsinki University of Technology, *Tik-110.501 Seminar on Network Securit*y, Telecommunications Software and Multimedia Laboratory, 2000.

[6] M. Razi and S. Irfan Haider, 'Seniority-Based Distributed Key Authentication Service for MANET', *Proceedings, International Conference for Management and Technology 2007*, Mohali, India, March 2007.

[7] Kamal Kumar Chahaun, Amit Kumar Singh Sanger and Virendar Singh Kushwah, Securing On-Demand Sorce Routing in MANETS ", Second international conference on computer and network technology.

[8] Maqsood Razi and Jawaid Quamar, " A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANETS ", IEEE journal on security and authentication.

[9] N. Kettaf, H. Abouaissa, P. Lorenz, "An Efficient Heterogeneous Key Management approach For Secure Multicast Communication in Ad hoc networks", Springer, Telecommunication System, vol-37, February 2008, pp: 29-36.

[10] Y.Chun Hu, A. Perrig and David B. Johnson, "Wormhole Attack in Wireless Networks", IEEE Journal on Selected Areas in Communication, vol. 24, February 2006, pp: 370-380.

[11] R.A. Raja Mahmood, A.I. Khan, "A Survey on Detecting Black Hole Attack in AODV Based Mobile Ad hoc Networks", International Symposium on High Capacity Optical Networks and Enabling Technologies, November 2007, pp: 1-6.

[12] P. Papadimitratos, and Z. Haas, "Secure Routing for Mobile Ad hoc Networks", Proceeding of SCS Communication Networks and Distributed Systems Modeling and Simulation, January, 2002.

[13] Y.C. Hu, A. Perrig, and D. B. Johnson, "Ariadne: A Secure On-demand Routing Protocol for Ad hoc Networks", Proceeding of 8th Annual International Conference on Mobile Computing and Networking, (MobiCom 02), September 2002, pp: 12-23,.

[14] J. Liu, F. Fu, J. Xiao and Y. Lu, "Secure Routing for Mobile Ad Hoc Networks", Proceeding of 8th ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, vol-3, 2007, pp: 314-318.

[15] L. Buttyan, and I. Vajda, "Towards Provable Security for Ad hoc Routing Protocols", Proceeding of 2nd ACM Workshop on Security of Ad hoc and Sensor Networks, October 2005, pp: 94-105.

© 2010, IJARCS All Rights Reserved