Volume 2, No. 2, Mar-Apr 2011
ISSN No. 0976-5697
International Journal of Advanced Research in Computer Science
RESEARCH PAPER
Available Online at www.ijarcs.info

An Optimal Energy Efficient And Secure Multicast Routing Protocol For key Distribution In Ad-Hoc Networks (MANETS)

Venkata Sai karteek . N *
School of Information Technology & Engineering,
VIT University
Vellore, India.
nerellakarteek@yahoo.com

Shakti Ganesh . M
Assistant Professor,
School of Information Technology & Engineering,
VIT University,
Vellore, India.
sakthiganesh.m@vit.ac.in

Abstract: Many emerging applications in adhoc networks require Multicast communication for reliability and efficiency. Multicast communication is challenging in adhoc networks due to its some of the vital characteristics such as infrastructure-less architecture, lack of central authority, high packet loss rates and limited resources such as bandwidth, time, power, and other security issues. Key management is the fundamental challenge in achieving secure multicast communication using multicast key distribution in mobile adhoc networks. This paper proposes a new optimal energy efficient and secure multicast routing protocol (OEESMRP) for secure multicast key distribution, in which nodes uses Destination Sequenced Distance Vector (DSDV) routing protocol format to know the neighbour node address with that optimal energy efficient and secure multicast routing protocol (OEESMRP) forms a tree structure for multicast communication with energy efficiency. Simulation results from the NS2 shows the demonstration of Multicast Tree using OEESMRP have better system performance than using DSDV in terms of end to end delay, throughput, packet drop rate and key delivery ratio under varying network conditions.

Keywords: Mobile adhoc networks, DSDV, Optimal Energy Efficient and Secure Multicast Routing Protocol (OEESMRP), Multicast Tree

I. INTRODUCTION

Multicasting [9] in wireless ad – hoc network is a one of the emerging topic in recent years. Multicasting is a fundamental communication paradigm for group-oriented communications such as video conferencing, discussion forums, frequent stock updates, video on demand, pay per view programs, and advertising. By multicasting, the transmission of packets from a source or a group of sources to a group of one or more hosts that are identified by a single destination address. Through Multicasting greatly reduces the transmission cost when sending the same packet to multiple recipients. A multicast packets is normally send to all members of its destination group with the same reliability as regular unicast packets. Multicast communication services [1, 2, 3] can reduce communication costs, the link bandwidth consumption, sender and router processing, increase throughput and delivery rate. In addition, it can provide a simple and robust communication mechanism when the receiver's individual address is unknown or changeable. It improve the usage of wireless links by sending multiple copies of data packets using inherent multicast behavior of wireless transmission through reducing transmission overhead and power consumption is a very challenging part in multicasting. There are many applications where one-to-many and many-to-many transmissions [13] are required.

The multicast services with ad hoc networks need to face some security related challenges such as authentication, data integrity, access control and group confidentiality are required. In above issues group confidentiality is the most important service for several applications [4] in which only valid users could decrypt the multicast data. This can be done using key distribution rules [2, 12] as follows:
Forward secrecy, Collusion freedom, backward secrecy, Non-group confidentiality.

The Key management [5] includes creating, distributing and updating the keys these are the basic things for secure multicast communication [12] applications.

In key management rekeying is the one of the demanding job because each and every member holds a key to encrypt and decrypt the multicast data. When a member joins and leaves a group, the key has to be updated and distributed to all group members in order to meet the above secure requirements. A critical problem with any rekey technique is scalability [6].

This rekey process may affect some of the quality related aspects such as 1-affect-n, low bandwidth overhead, packet drop rate, energy consumption. Thus a secure multicast communication will face both secure and quality of service related aspects.

To solve these problems this paper proposed a energy efficient multicast routing protocol which includes DSDV protocol formats for forming the multicast tree structure.

This overcomes the 1-affect-n phenomenon and also this tree structure will reduce the energy consumption and overcome low bandwidth overhead and packet drop rate. Several methods applied in this paper are as follows:
DSDV[7] routing protocol to maintain routing table periodically and simultaneously exchanges the routing table for electing the tree root and distributing the keys when a node joins and leaves.

In order to reduce the retransmission it sends acknowledgement for each transmission.

MAC 802.11 for providing communication between nodes.

Channel bandwidth for minimization of congestion that occurs during transmission.

Congestion control mechanism to control flooding message.

The remainder of this paper is structured as follows. Section 2 presents the proposed works about energy efficient multicast routing protocol approaches. Section 3 describes the key distribution scheme. Section 4 explains about simulation environment in NS2. In Section 5 describes the comparison of this developed routing protocol with DSDV by showing simulation results and analysis which routing protocol is better Section 6 describes conclusion.

II. PROPOSED WORK

A. Optimal Energy Efficient And Secure Multicast Routing Protocol (OEESMRP)

OEESMRP provides the capability to manage multicast address assignment and enables a single source to send data addressed to a unique multicast group address. Receivers join this group if they are interested in receiving data for this group. In support of these functions, OEESMRP involves a number of services. The discussions that follow focus on the key processes and technologies that enable OEESMRP services, including address management, the Multicast Transaction Protocol (MTP), node management, multicast route management, data forwarding, and topology management.

In the case of multicast address mapping, OEESMRP multicast addresses must be mapped to network-layer multicast addresses, and these in turn are mapped to data link layer multicast addresses. For each network-layer type, a block of multicast addresses must be obtained for OEESMRP

OEESMRP involves a multicast transaction protocol (MTP) that provides for three transaction types: node, endpoint, and simultaneously node/endpoint. Communications between adjacent nodes and between nodes and endpoints occurs through request/response transactions. The basic MTP design as implemented in OEESMRP routers uses two queues for all transactions: a request queue and a response queue. The response-queue entries are created upon receipt of a request packet. The entry is referenced during all processing of the request, and the processed entry remains in the queue until it expires and is deleted from the queue.

OEESMRP relies on a number of node relationships, including designated nodes, adjacent nodes, and tunnel nodes, to permit transport of multicast datagrams. Designated nodes are EEMRP routers that have been specified as primary or secondary nodes. A designated primary node is responsible for allocating group addresses [8]. A designated secondary node is required if a local network has more than one node. The secondary is used to maintain a copy of the Group Creation table, and it becomes the primary node if the primary node for a network fails. when a node first tries to become the designated secondary node on each local net. If successful, the node then tries to become the designated primary node. Nodes Periodically send out hello packets on each port. If a hello packet is not received from an adjacent node within a certain interval of time, the node's adjacency state is changed to Not Operational, and associated routes are marked unreachable.

Each node maintains an entry in the Node table for each an adjacent node. The table entry is allocated the first time it receives a packet from adjacent node. Table entries include the time of the most recent hello packet and its state.

B. Multicast Tree working procedure

OEESMRP relies on a spanning tree-based forwarding scheme to determine routing paths for multicast traffic. This route- determination process relies on the use of a distance-vector algorithm. A node sends distance-vector request packets to adjacent nodes at startup time and when routes change. When routes change, each node sends distance-vector request packets to every adjacent node.

A head node (root node) is selected dynamically depending on the node maximum reachability with other nodes that information is known from routing table of the node. The port-parent address must be set for the route for all ports. Because the group address is bound to the network address, the port-parent address also is used if a node is to handle a request for specified groups. When the port-parent address is the node's own address, the node is responsible for the request. Equal path nodes decide which node is responsible for a request by determining which node has the minimum reachability distance.

When a distance-vector request with entries for unknown node is received by a head node or its child node, network ranges for associated node are added to Route table for the node, with a received distance incremented by one. The adjacent node that sent the distance-vector packet then becomes the parent node for the new node. The table entry is updated if a distance-vector packet is received for known node, and the distance-vector packet plus one is less than the entry in the Node Route table

III. KEY DISTRIBUTION SCHEME

The proposed scheme is to achieve the multicast key distribution for secure communication. For this source node send encrypted multicast data to the members of the group[11] which following the multicast tree. For encrypting multicast data RSA[10] algorithm is used. From RSA algorithm public key and private key will generate. These keys must sent to the child nodes securely for that we must use the session keys of the groups.

With that session key help each group will pass public key to their group members securely depending up on the routing table here group node means head node for some set of nodes and again these set of nodes may be head node some set of nodes depending on their reachability.

Through this distribution scheme decryption and re-encryption process decreased because only group head need to be decrypt and encrypt but the group members just do decrypt for getting the public key.

With this approach key distribution done securely and efficiently to all nodes present in network. After receiving RSA keys by all nodes in the network multicast communication held securely.

Through this process rekeying is also decreased because if any node leave or join only that particular head node must do the rekeying to that newly joined node in unicast way or multicast way that depend upon the number of nodes joined in that group.

IV. SIMULATION ENVIRONMENT

This approach is simulated under Linux Fedora, using the network simulator NS2 version ns-allinone-2.34.This simulation environment is defined by the following parameters.

a) The density of group members within the ad hoc network: group members number (7 - 13 - 28).
b) Network surface (2000m*2000m).
c) The mobility scenarios are generated by the automatic.
d) Generator setdest provided by ns2.
e) The maximal speed of members is defined at 10km/h (2.77m/sec).
f) The pause time is 20 seconds.
g) The simulation duration is 200 seconds.
h) Physical/Mac layer: IEEE 802.11.
i) Mobility model: random waypoint model with pause time.
j) Equal to 20 sec and with maximum nodes movement speed equal to 3 m/s.
k) Routing protocol: OEESMRP
l) Traffic: only unicast distribution keys traffic exists in the simulation. The source of the group sends the KEYS to the group head, which forward it to their group members.

V. SIMULATION RESULTS

To evaluate performance characteristics of developed protocol in terms of end to end delay, packet drop rate, key delivery ratio and energy consumption.

A. Energy Consumption

Sum of units required for the keys transmission throughout the simulation. That can be measured by the summation of Emax and Emin. By seeing the Fig.1 we can say that proposed protocol consume less energy when compare to ordinary dsdv protocol.

B. End To End Delay (Latency)

The average latency or delay of keys transmission from the source to the receivers. This metrics allows evaluating the average latency to forward a key from a group head to its group members. By seeing the Fig.2 we can say that latency of the proposed protocol is less than the ordinary dsdv protocol.

C. Packet Loss Rate

It is obtained by subtracting number of packets received at the destination from number of packets send to destination. This metric allows to know the reliability of the protocol in terms of packet loss rate. By seeing the Fig.3 we can say that packet drop ratio for proposed protocol is less than the ordinary dsdv protocol.

D. Key Delivery Ratio

It is defined as the number of received keys divided by number of sent keys. This metrics allows evaluating the reliability of the protocol in term of key transmission. By seeing the fig.4 we can say that key delivery ratio for proposed protocol is more than the ordinary dsdv protocol.

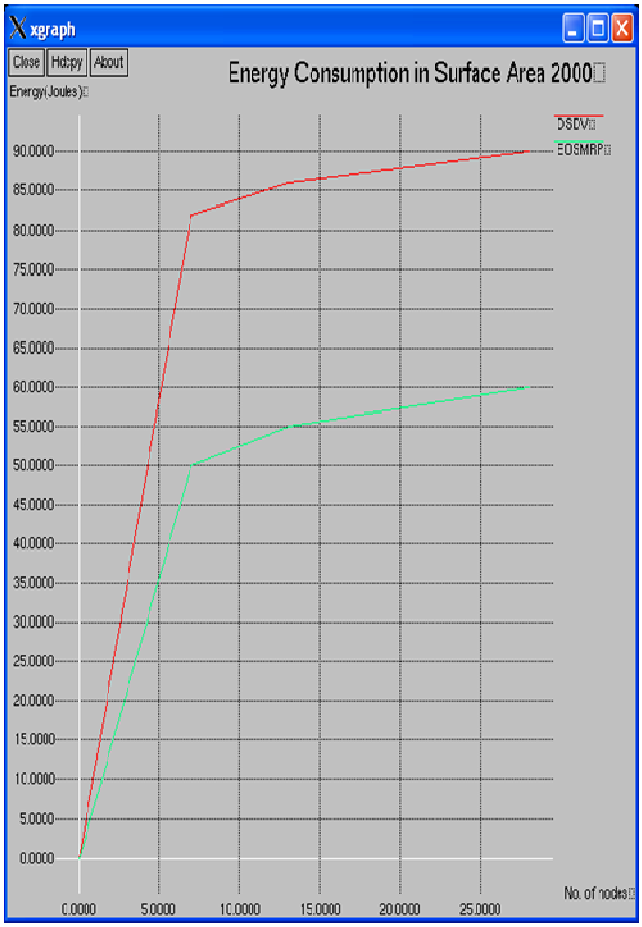

Figure..1Energy Consumption in multicast key distributions

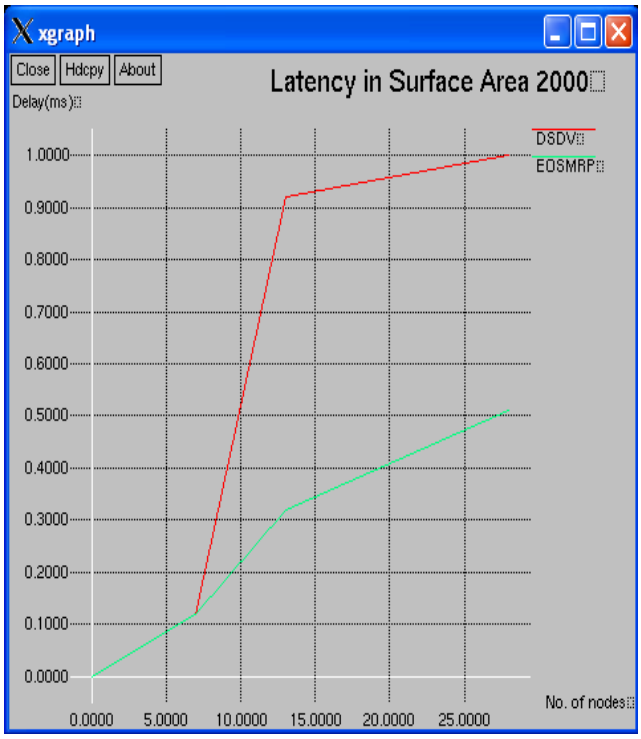

Fig.ure.2 Average Latency(end to end delay) in multicast key distributions

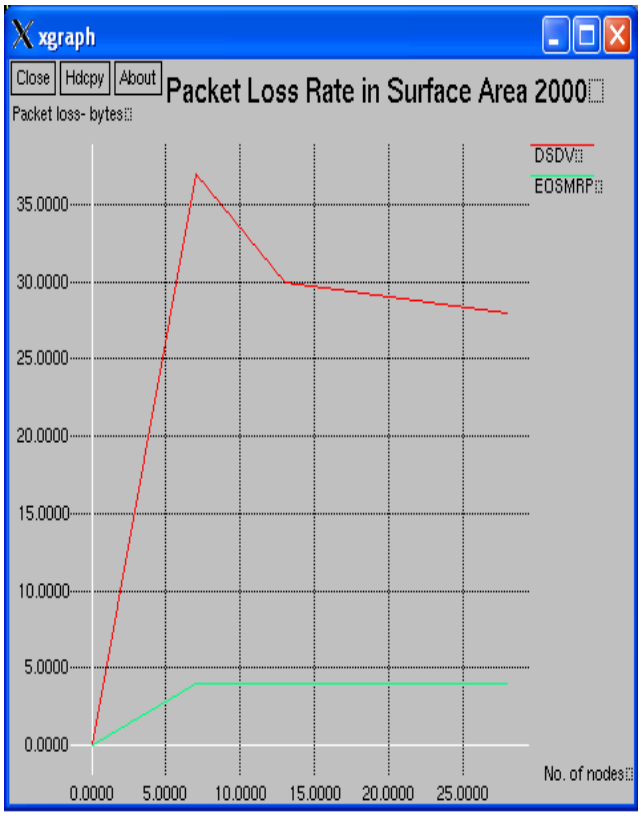

Fig.ure.3 Packet loss rate in multicast key distributions

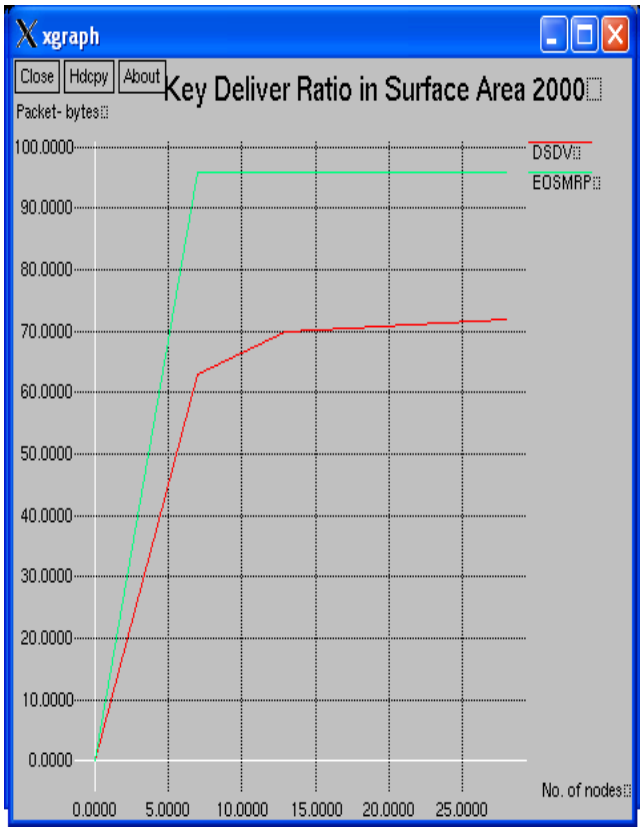

Figure..4 key delivery ratio in multicast key distributions

VI.CONCLUSION

Secure multicast communication is a significant requirement in emerging applications in adhoc environments like military or public emergency network applications. Some of the existing protocols like DSDV can't address the critical problems like 1-affects-n phenomenon, energy and latency issues. However the major challenges in mobile adhoc networks include high packet loss rate which is not attempted in ordinary DSDV protocol and hence results in unreliable key distribution. Therefore an attempt is made to reduce the energy and latency and improve the reliability by reducing packet loss rate and increasing key delivery ratio using an protocol called Optimal energy efficient and secure multicast routing protocol for multicast key distribution. This protocol uses DSDV routing protocol for electing group heads and to find group members. The proposed protocol is tested and the entire experiments are conducted in a simulation environment using network simulator NS2. The results are formed to be desirable and the proposed method is efficient, reliable and more suitable for secure multicast key distribution dedicated to operate in MANETs.

VII. REFERENCES

[1] T. Chiang and Y. Huang, "Group keys and the multicast security in ad hoc networks", Proc. IEEE International Conference on Parallel Processing, IEEE press, pp 385-390, Oct 2003.

[2] T. Kaya, G. Lin, G. Noubir, and A. Yilmaz, "Secure multicast groups on ad hoc networks". Proc. 1st ACM workshop on security of ad hoc and sensor networks, ACM Press, pp 94-102.2003.

[3] L. Lazos and R. Poovendram, "Energy-Aware Secure Multicast Communication in Ad Hoc Networks Using Geographical Location Information". Proc.IEEE International Conference on Acoustics Speech and

[4] H. Bettahar, A. Bouabdallah, and M. Alkubeily, Efficient Key Management Scheme for Secure Application level", IEEE sym. On Computers and Communications, pp 489-497, July 2007.

[5] G.Valle, R.Cardenas, "Overview the Key Management in Adhoc Networks", LCNS 3563, pp 397-406, Aug 2005.

[6] D.Huang, D.Medhi, "A Secure Group Key Management scheme for Hierarchical Mobile Adhoc Networks", Adhoc Networks, pp 560-577, June 2008.

[7] Perkins,C.E., and Bhagwat.P. (1994). Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers. ACM, pp.234 – 244.

[8] Y. Challal, H. Seba, "Group Key Management Protocols: novel Taxonomy", International Journal of Information Technology pp 105-118, 2005.

[9] Frank, A. J., Wittie, L. D., and Bernstein, A. J. Multicast communication on network computers. IEEE Softw. 2,3(May 1985), 49-61.

[10] J. Blömer, M. Otto, J.-P. Seifert, "A new CRT-*RSA algorithm* secure against Bellcore attacks," acm ccs. 2003, acm press, pp.311–320, 2003

[11] L. Dondeti, S. Mukherjee, and A. Samal, "Secure one-to many group communication sing dual encryption", IEEE sym. On Computers and Communications, pp 1-25, Jul 1999.

[12] D.Suganya Devi, Dr.G.Padmavathi. "Performance Characteristics of Cluster –Based Multicast Key Distribution Scheme for Mobile ADHOC Networks ," IJCA

On computer application volume 1 – no. 23, 2010.

[13] L. Dondeti, S. Mukherjee, and A. Samal, "Secure one-to many group communication sing dual encryption", IEEE sym. On Computers and Communications, pp 1-25, Jul 1999.