

Secured and Scalable Multicasting through New SCDMP Protocol in MANET

Govind V Haldankar
Department of Computer Engg.
Mumbai University,
PIIT, New Panvel, India.

Manjusha Deshmukh
Department of Computer Engg.
Mumbai University,
PIIT, New Panvel, India.

ABSTRACT

In MANET, multicast routing can take full advantage of the shared wireless channel. Wireless communication is defined as sharing of information between one or more systems through wireless links. We propose Secure Core Defined Mesh based protocol (SCDMP) which can scale to a large group size and large network size. The protocol is designed to be complete and collected, and efficient for more reliable operation. Security of the network infrastructure is obtained using standard encryption techniques that permit to achieve both confidentiality and integrity of the exchanged traffic. A hop-by-hop encryption scheme based on the cryptographic functions operating at the data link layer is used in order to secure both data and signaling communications against external attacks. Simulations based on NS2 and glomosim shows that proposed protocol having better performance metrics such as, average End to end Delay, Packet delivery ratio, by varying group size, node density, moving speed, for network range.

Keywords

Mesh, Core, Ad-Hoc, MANET, Multicasting,

1. INTRODUCTION

Mobile Ad-Hoc Network (MANET) is a self-organized network of mobile devices without having any intended infrastructure to connect those devices to wired networks. Because there is no infrastructure, all important network operations such as routing and forwarding must be handled by the mobile nodes that is each node behaves both as a router and as an end host at the same time [2]. MANETs have many applications in battlefields of military, critical search, rescue operations, fire-fighting, temporary networks in conferences and etc. MANETs are very flexible and can be established quickly and easily using low cost equipment's. Due to limited radio range of wireless nodes, the path between a pair of nodes may consists of many mobile nodes. Generally, there are two models for multicast "one-to-many" and "many-to-many". Multicasting techniques can be considered as an efficient way to deliver packets from the source to any number of client nodes. The applications in MANET include military, emergency applications, and small sensor devices located in animals and other strategic locations that collectively monitor habitats and environmental conditions there is a crucial challenge in enabling effective multicasting over a MANET whose topology change constantly [3].

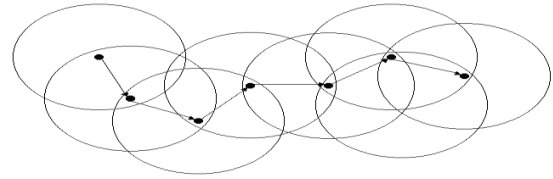


Figure 1. Basic Structure for Ad-Hoc Network.

Wireless technologies such as Bluetooth or the 802.11 Standards enable mobile devices to establish a Mobile Ad-hoc Network (MANET) by connecting dynamically through the wireless medium without any centralized structure [9]. MANET offer several advantages over traditional networks including reduced infrastructure costs, ease of establishment and fault tolerance, as routing is performed individually by nodes using other intermediate network nodes to forward packets [10]. This multi-hopping reduces the chance of bottlenecks, however the key MANET attraction is greater mobility compared with wired solutions. There are a number of issues which affect the reliability of Ad-hoc networks and limit their viability for different scenarios; lack of centralized structure within MANET requires that each individual node must act as a router and is responsible for performing packet routing tasks; this is done using one or more common routing protocols across the MANET [11]. However mobile devices feature physical size and weight limitations essential for their mobility, this reduces the available memory and computational resources as well as limiting battery power. MANETs containing more nodes require greater processing power, memory and bandwidth to maintain accurate routing information; this introduces traffic overhead into the network as nodes communicate routing information, this in turn uses more battery power. Wireless technologies use a shared communication medium; this causes interference which degrades network performance when multiple nodes attempt to transmit simultaneously.

2. RELATED WORK

When the number of nodes in the same area of a MANET increases, multicast routing is considered a key measure to boost system performance [4]. Multicast routing in MANETs can be achieved by the following mechanisms: flooding (a node receives a message and flood it to nodes in its neighbor table), routing tables (a node will send data by the path in its routing table) or on-demand paths (when a source sends a request, it first searches and builds a path to the destination, and then sends data by the path after getting responses from the destination).

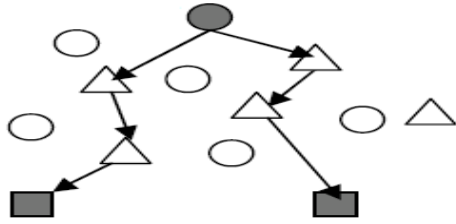


Figure 2. Multicasting in MANET.

According to network topology MANET multicast routing protocols are divided into two general categories: tree-based, mesh-based. For tree-based multicast routing protocol, there is only one path between source and destination node; several available paths in mesh-based protocol, Tree-based topology has a better efficiency; as multiple paths is available, mesh based topology has better robust and reliability. ODMRP [1] (On-Demand Multicast Routing Protocol) is a mesh-based multicast routing protocol using Forwarding Group, which adopts Soft State to maintain multicast membership. Forwarding Group is the set of leader nodes sending multicast data to member nodes along minimum path; such leader nodes constitute mesh forwarding structure of each multicast group. When node needs to send multicast data it begin to establish a multicast network composing of forwarding nodes, different sending node should constitute different multicast network a shared tree is one in which each connected node is able to send packets to all other nodes using the same tree. Shared trees are built among others E.g. MAODV [6]. It is very difficult to maintain the tree structure in mobile ad hoc networks; Tree-based approaches often use local repair mechanisms to shield the distribution structure from link failures caused by mobility.

3. PROPOSED PROTOCOL

Our proposed protocol supports data send from any source to a given multicast group. The protocol is executed as a dispersed algorithm to elect one of the receivers of a group as core of the group. The election of the core is done using spanning tree algorithm. All nodes on shortest paths between any one receiver and the core entirely form the mesh. A sender sends a data packet to the group along any of the shortest paths between the sender and the core. The data packet when reaches to the mesh member, it is trying to flooded within the mesh, and nodes maintain a packet ID which stores in cache memory to drop duplicate packets. The protocol applies head control message for all its functions. Each head control message has a Core ID, Group ID, Single sequence number, distance between the core, mesh member flag, and a parent member that describes the preferred neighbor to reach the core of the protocol. With the help of information or knowledge contained in this control announcement nodes will be able to elect cores, now need to determine the routes for single sources outside a multicast group, also need to notify about joining or leaving the mesh of the group and handled the mesh. The mesh is formed and data passing is done within the multicast group. For example the parent of nodes O and Q is node N. also for the same case is for node P, it is validated in its multicast announcement that its parent is node K. Now by considering nodes O and P are senders. Node N starts sending a data packet from node O, not from node P, because there is only one parent for node O and it is node N. Although node J is not the parent of node P, it forwards the packet when it receives it from P, members of the mesh do not confirm their connectivity list before forwarding a packet. As a result, receiver node I will get the

packet early. Node J does not resend same the packet when it receives exactly equivalent packet from K due to duplicate packet confirmation. Following are steps which are performed for the protocol.

3.1 Announcement of the Multicast Members

Core of the group is one of the nodes which is able to transmit the announcement of the multicast members periodically for that group. As the multicast declaration travels through the network, as it forms connectivity in the list at every node in the network. By using connectivity lists, nodes will be able to form a mesh, and routing of data packets from senders to receivers. A node stores the data from all the multicast declaration it receives from its neighbors in the connectivity list. Fresh multicast declarations overwrite entries with lower sequence numbers for the same group. Now in the given group, a node has remaining only one entry in its connectivity list from a particular neighbor and it tries to keeps only that information with the new sequence number for a given core. Each entry in the connectivity list, it stores the multicast declaration, stores the time when it was received, and the nearest from which it was received. Then the node generates its own multicast declaration based on the best entry in the connectivity list. For the same core ID and sequence number, multicast declarations with smaller distances to the core are considered. When all those fields are the same, the multicast declaration that arrived earlier is considered. After selecting the best multicast declaration, the node generates the fields of its own multicast announcement i.e. Core ID, Group ID, Sequence number, Distance to core, for the Parent Mesh member. The connectivity list holds information about all the routes that exist to the core. When a core change occurs for a group then the node clears the entries of its old connectivity list and builds a new list, specific to the new core.

3.2 Establishment of the Mesh and its Preservation:

At the initial stage only receivers are considered as mesh members and their mesh member flag is set to TRUE in the multicast announcement. Non receivers consider themselves as mesh members if and only if they have at least one mesh child in their connectivity list. Now if neighbor in the connectivity list is a mesh child if Case (1):Its mesh member flag is set, Case(2):The distance to core of the neighbor is larger than the node's distance to core, Case(3) The multicast announcement corresponding to this entry was received in within a time period equal to two multicast announcement intervals. If a node has a mesh child and is hence a mesh member, then it means that it remain on the shortest path from the receiver to the core.

3.3 Define the Core for the Election

When a new receiver wants to join a multicast group, it first finds whether it has received a multicast announcement from core of that group. If the node has received it earlier, it adopts the core specified in the announcement it has received, and it starts transmitting that specify the core for that group. It considers itself as the core of the group and starts transmitting multicast announcement periodically to its neighbor stating itself as the core of the group and no distances to itself. Nodes propagate multicast announcement based on the best multicast announcements they have received from their neighbors. A multicast announcement with higher core ID is considered better than a multicast announcement with a lower core ID.Each connected component has only one core. If a receiver

joins the group before any other receivers, it declares itself as the core of the group. If several receivers join the group concurrently, then the one with the highest ID is declared as core of the group. The election is held in the partition which does not have the old core.

3.4 Multicasting or Propagation of the Packets:

The parent field of connectivity list entry corresponds to the node from which the neighbor received its best multicast announcement. This field allows nonmembers to forward multicast packets towards the mesh of the group. A node forwards a multicast data packet it receives from its neighbor. The packets are then flooded within the mesh and group of its member's uses a packet ID cache to detect and discard packet which duplicates. The routing of data packets from senders to receivers is also used to update the connectivity list. When a nonmember transmits a packet, it expects its parent to forward the packet. This serves as an implicit acknowledgment of the packet transmission. If the node does not receive an implicit acknowledgment within ACK-TIMEOUT then it deletes the parent from its respective connectivity list.

3.5 Core Authentication of the protocol

Each new node that needs to connect to the mesh network first authenticates to the nearest mesh router (Core) exactly like a Sub-ordinate node, gaining access to the mesh network. After it performs a second authentication connecting to a Key Server. Finally, the Key Server distributes the information needed to create the temporary key that all mesh routers (Core) use to encrypt the traffic transmitted over the wireless backbone. The authentication process leaves two considerations: 1) The access point (AP) still needs to authenticate itself to the client station (STA) and 2) keys to encrypt the traffic need to be derived. Therefore the four-way handshake is used to establish another key called the PTK (Pairwise Transient Key). The PTK is created by concatenating the following attributes: PMK, AP nonce (ANonce), STA nonce (SNonce), AP MAC address, and STA MAC address. The product is further put through (PBKDF2-SHA) as the cryptographic hash function. The handshake also yields the GTK (Group Temporal Key), which is used to decrypt multicast and broadcast traffic. The actual messages also exchanged during the handshake are explained in the figure.

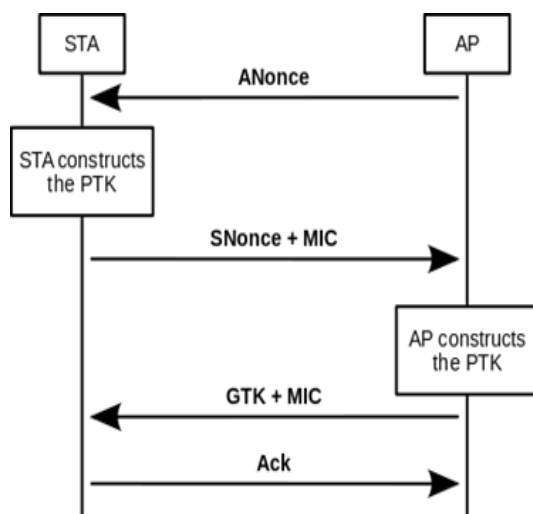


Figure 3. Encryption/Decryption of keys .

This protocol provides a reactive method to deliver the keys used by all mesh routers (Core) to protect the integrity and confidentiality of the traffic exchanged during a specific interval. In this protocol, each node maintains a list of n keys, which we refer to as the key list figure shows in detail the message exchanges that occur between the mesh router and the Key Server.

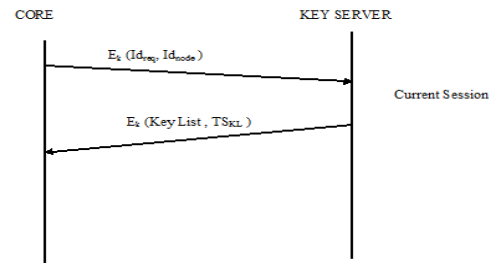


Figure 4. Communication between Core and Key server.

4. PERFORMANCE OF PROPOSED PROTOCOL

We implemented the SCDMP protocol using Network Simulator and they are compared with ODMRP and MADOV. The nodes followed the modified random waypoint mobility model. The result is calculated for with the no of sender one, two, five, and ten respectively senders with increasing receivers that is ten, twenty, thirty and forty receivers. The moving speed of sender nodes are uniformly set between the minimum and maximum speed values which are set as 1m/s (with pause time as 100 seconds) and 20 m/s respectively except when studying the effect of mobility.

4.1 Performance Metrics:

The metrics used to evaluate the protocol performance are packet delivery ratio, and end to end delay.

4.1.1 The packet delivery ratio (PDR):

It is defined as the sum of all unique data packets received divided by the sum of all data packets that should have been delivered (sum of sent packets multiplied by the number of receivers).

$$PDR = \text{Packets delivered} / \text{Packets sent}.$$

4.1.2 Average End-to-End Delay

It is the average time taken by a data packet to move from the source to the receivers.

$$\text{Avg. EED} = \text{Total EED} / \text{No. of packets sent}$$

4.2 Performance Evaluation:

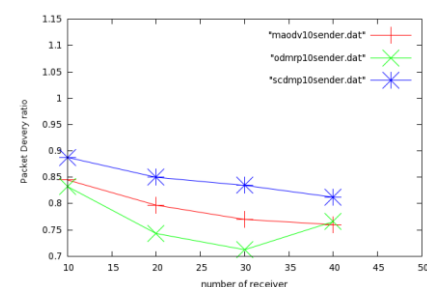


Figure 5. Comparison between protocols for PDR for 10 senders with multiple receivers for 1 ms.

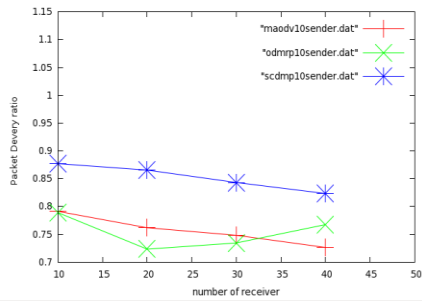


Figure 6. Comparison between protocols for PDR for 20 senders with multiple receivers for no movement.

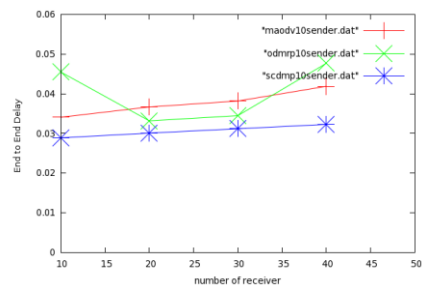


Figure 7. Comparison between protocols for End to End Delay for 10 senders with multiple receivers for no movement.

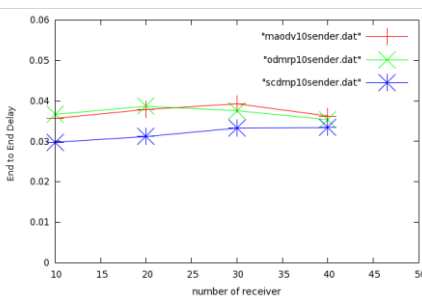


Figure 8. Comparison between protocols for End to End Delay for 10 senders with multiple receivers for 1 ms movement.

Table: 1 Information of the PDR and End to End delay for the Proposed Protocol

No of Nodes	No of Senders	No of Receivers	PDR	End To End Delay
10	10	10	0.9	0.03
20	10	20	0.87	0.032
30	20	30	0.86	0.31
40	20	40	0.85	0.315

5. CONCLUSION & FUTURE WORK

In MANET, unicasting as well as multicasting both can be done but according to the performance analysis, for group communications, multicast routing increases the efficiency and provides better efficiency when compared to unicast routing. In our approach core is defined for creation and maintenance of mesh. It forwards the data packets. If one of the core node get fails, core election need to takes place among the receivers. We can bring an energy field in the Message Announcement packet, which can be preferred for electing a core node. Electing a node which has higher energy as core will perform better, WMNs have been hugely accepted in the professional application sectors of ad hoc network. With increasing demand for real-time services in the wireless networks, quality-of-service (QoS)-based routing offers major challenges in Wireless-Mesh Networks.

6. REFERENCES

- [1] M.Gerla,S.J.Lee, and W.Su,“On-demand multicast routing protocol (ODMRP) for ad-hoc networks,” Internet draft, draft-ietf-manet-odmrp-02.txt,2000.
- [2] Olimpjon Shurdi, Rozeta Miho, Bexhet Kamo, Vladi Koliyi, Alban Rakipi, "Performance Analysis of Multicast Routing Protocols MAODV, ODMRP and ADMR for MANETs",2011.
- [3] L. Ji and M. S. Corson,“A lightweight adaptive multicast algorithm,”Proc.IEEE GLOBECOM, 1998, pp.1036–1042.
- [4] J.J.Garcia-Luna-Aceves and E.L.Madruga,“Core-assisted mesh protocol,” IEEE J.Select.Areas Commun.vol. 17, no.8, 1999, pp. 1380–1394.
- [5] J.J.Garcia-Luna-Acevesand D.Sampath, “Efficient multicast routing in MANETs using prefix labels”, Proc. IEEE Int.Conf. Computer Commun and Networks, Aug.2009, pp. 1–8.
- [6] X. Xiang, X. Wang, and Y. Yang, "Supporting Efficient and Scalable Multicasting over Mobile Ad Hoc Networks", IEEE Transactions On Mobile Computing, VOL. 10, NO. 4, April 2011.
- [7] Luo Junhai, Ye Danxia, Xue Liu, and Fan Mingyu "A Survey of Multicast Routing Protocols for Mobile Ad-Hoc Networks", In IEEE Communications Surveys & Tutorials, VOL. 11, NO. 1, FIRST QUARTER 2009.
- [8] S. Lee, W. Su, J. Hsu, M. Gerla, and R. Bagrodia,“A performance comparison study of ad hoc wireless multicast protocols”, In IEEE INFOCOM, 2000.
- [9] E. Alotaibi and B. Mukherjee, “A survey on routing algorithms forwireless Ad-Hoc and mesh networks,” Computer Networks: The International Journal of Computer and Telecommunications Networking, vol. 56, no. 2, pp. 940–965, October 2011.
- [10] M. Zhang and P. H. J. Chong, “Performance Comparison of Flat and Cluster-Based Hierarchical Ad Hoc Routing with Entity and Group Mobility,” in Proc. of IEEE Communications Society conference on Wireless Communications & Networking, Budapest, Hungary, 2009, pp. 2450-2455.

- [11] R. O. Schmidt and M. A. S. Trentin, "MANETs Routing Protocols Evaluation in a Scenario with High Mobility: MANET Routing Protocols Performance and Behaviour," Network Operations and Management Symposium, 2008. NOMS 2008. IEEE, Salvador, Bahia, pp.883-886, 2008.
- [12] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi "A Review of Routing Protocols for Mobile Ad-Hoc Networks (MANET) "International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013.
- [13] Fabio Martignon, Stefano Paris, Antonio Capone Design and implementation of MobiSEC:"A complete security architecture for wireless mesh networks", Computer Networks 53 (2009) 2192–2207.
- [14] Aiswarya Antony, Swarna Parvathi, Akshaya Venkatesan,"Experimental Analysis of Streaming over Mobile Ad hoc Networks using PUMA",Indian Journal of Engineering, Volume 2, Number 3, January 2013.
- [15] M. Nagaratna, V. Kamakshi Prasad, Raghavendra Rao,"Performance Evaluation of Mesh - Based Multicast, Routing Protocols in MANET's", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 2, No. 7, 2011.
- [16] Ravindra Vaishampayan, J.J. Garcia-Luna-Aceves,"Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks".