Cluster Based Multicast Tree for Secure Multicast Key Distribution in Mobile Adhoc Networks

D.Suganya Devi † and Dr. G.Padmavathi††

†Sr.Lecturer, SNR SONS College, Coimbatore, Tamil Nadu, India.
††Prof and Head, Avinashilingan University for Women, Coimbatore, Tamil Nadu, India.

Summary

Secure multicast communication in mobile adhoc networks is challenging due to its inherent characteristics of infrastructure-less architecture with lack of central authority, high packet loss rates and limited resources such as bandwidth, time and power. Hence key management is the fundamental challenge in achieving secure communication using multicast key distribution in mobile adhoc networks. This paper proposes a new cluster based multicast tree (CBMT) algorithm for secure multicast key distribution, in which source node uses Multicast Destination Sequenced Distance Vector(MDSDV) routing protocol to collects its 1 hop neighbors to form cluster and each node which have child node is elected as the Local controllers of the created clusters. Simulation results shows the demonstration of CBMT using MDSDV have better system performance than using DSDV and I-DSDV in terms of end to end delay, key delivery ratio and packet drop rate under varying network conditions.

Key words:

Cluster based multicast tree, MDSDV, Mobile Adhoc Networks, Multicast Key Distribution.

1. Introduction

A MANET (Mobile AdHoc Network) is an autonomous collection of mobile users that offers infrastructure-free communication over a shared wireless medium. It is formed spontaneously without any preplanning. Multicasting is a fundamental communication paradigm for group-oriented communications such as video conferencing, discussion forums, frequent stock updates, video on demand (VoD), pay per view programs, and advertising.

The combination of an ad hoc environment with multicast services [1, 2, 3] induces new challenges towards the security infrastructure. In order to secure multicast communication, several security services such as authentication, data integrity, access control and group confidentiality are required. Among which 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] as follows:

N**on-group confidentiality**: Here users that are never part of the group should not have access to any key that can decrypt any multicast data sent to the group.

Forward secrecy: In this case, users left the group should not have access to any future key. This ensures that a member cannot decrypt data after it leaves the group.

Backward secrecy: A new user who joins the session should not have access to any old key. This ensures that a member cannot decrypt data sent before it joins the group.

Collusion freedom: Any set of fraudulent users should not be able to deduce the currently used key.

These security services can be facilitated if group members share a common secret, which in turn makes key management a fundamental challenge in achieving secure communication using multicast key distribution. The Key management includes creating, distributing and updating the keys then it constitutes a basic block for secure group communication applications [5, 6]. One of the primary objectives of any key management scheme is the secure distribution of keying material.

Most of the security services rely generally on encryption using Traffic Encryption Keys (TEKs) and re-encryption is using Key Encryption Keys (KEKs) [7]. Each 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 requirements. The process of updating the keys and distributing them to the group members is called rekeying operation [8]. Rekeying is required in secure multicast communication to ensure that a new member cannot decrypt the stored multicast data (before its joining) and prevents a leaving member from eavesdropping future multicast data.

A critical problem with any rekey technique in multicast key distribution is unreliability with high packet loss rates due to frequent node mobility. The rekey process should be done after each membership change, and if the membership changes are frequent, key management will require a large number of key exchanges per unit time in

Manuscript received September 5, 2009
Manuscript revised September 20, 2009

order to maintain both forward and backward secrecies. The number of TEK update messages in the case of frequent join and leave operations induces several QOS requirements as follows:

Low bandwidth overhead: The re-key of the group should not induce a high number of messages, especially for dynamic groups.

End to end delay: Many applications that are built over the multicast service are sensitive to average latency in key delivery. Therefore, any key distribution scheme should take this into consideration and hence minimizes the impact of key distribution on the latency of key delivery.

Packet Drop Rate and Key Delivery Ratio: The number of TEK update messages in the case of frequent join and leave operations induces high packet loss rates and reduces key delivery ratio which makes the system unreliable.

Thus a secure multicast key distribution in mobile ad hoc environment should focus on both security and Qos requirements.

To overcome these problems, several approaches propose a multicast group clustering. [9, 10, 11]. Clustering is dividing the multicast group into several sub-groups. Local controller (LC) manages each subgroup, which is responsible for local key management within the cluster. Thus, after Join or Leave procedures, only members within the concerned cluster are affected by rekeying process, and the local dynamics of a cluster does not affect the other clusters of the group. Moreover, few solutions for multicast clustering such as dynamic clustering did consider the end to end delay to achieve an efficient key distribution process.

This paper proposes a cluster based multicast tree (CBMT) algorithm for secure multicast key distribution in mobile adhoc networks. Several methods applied in this paper are as follows:

1. MDSDV (Multicast Destination Sequenced Distance Vector) routing protocol to maintain routing table periodically and forms multicast tree among the group members. When event-triggered, exchanges the routing table for electing the cluster head and distributing the keys when a node joins and leaves. It sends acknowledgement for each transmission in order to reduce the retransmission.
2. MAC 802.11 for providing communication between nodes.
3. Channel bandwidth for minimization of congestion that occurs during transmission.
4. Multicast Congestion control mechanism to control flooding message.

Thus this new CBMT approach is an efficient dynamic clustering scheme using MDSDV routing protocol, which makes easy to elect the local controllers of the clusters and updates periodically as the node joins and leaves the cluster. The main objective of the paper is to present a new approach of clustering algorithm for efficient multicast key distribution in mobile adhoc network by overcoming issues of end to end delay, unreliability with high packet drop rate and low key delivery ratio.

Simulation results in NS2 shows that the demonstration of CBMT using MDSDV have better system performance than using DSDV and I-DSDV in terms of end to end delay, key delivery ratio and packet drop rate under varying network conditions.

The remainder of this paper is organized as follows. Section 2 focuses on the related work about multicast clustering approaches. Section 3 describes the proposed CBMT using MDSDV for Secure multicast key distribution. Section 4 presents the analysis of simulation results and performance comparison of the proposed approach. Section 5 concludes the paper.

2. Related Work

Several Clustering approaches [9, 10, and 11] for securing multicast key distribution in ad hoc networks have been proposed. They are basically classified into two main approaches. They are static clustering and dynamic clustering as shown in figure 1.

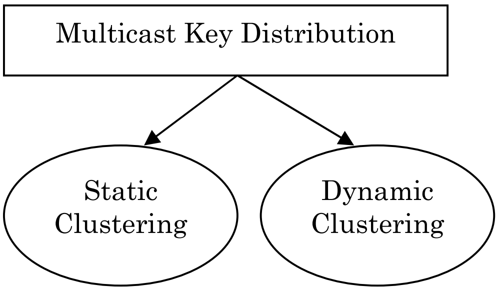

Figure 1. Classification of multicast key distribution Approaches

In Static clustering approach, the multicast group is initially divided into several subgroups. Each subgroup shares a local session key managed by LC. Example: IOLUS [12] and DEP [9] belong to the category that is more scalable.

Dynamic clustering approach aims to solve the “1 affect n” phenomenon. AKMP [10], SAKM [13] belong to this approach and are dedicated to wired networks. Enhanced BAAL [11] proposes dynamic clustering scheme for multicast key distribution in adhoc networks.

One approach to distribute group key on multicast environments based on clusters is the Optimized Multicast Cluster Tree (OMCT) [14, 15]. It is a dynamic clustering scheme for multicast key distribution dedicated to operate in ad hoc networks. Its main idea is to elect the LCs of the created clusters

OMCT needs the geographical location information of all group members in the construction of the key distribution tree, which does not reflect the true connectivity between nodes. Based on the literature reviewed, OMCT is the efficient dynamic clustering approach for secure multicast distribution in mobile adhoc networks. However knowing the true connectivity between the nodes in mobile adhoc networks simplifies the key distribution phenomenon due to the node mobility. Hence the true node connectivity is taken into consideration for the cluster formation.

To overcome the above limitations another method called Optimized Multicast Cluster Tree with Multipoint Relays (OMCT with MPR) [16] is introduced which uses the information of Optimized Link State Routing Protocol (OLSR) to elect the LCs of the created clusters. OMCT with MPRs assumes that routing control messages have been exchanged before the key distribution. It does not acknowledge the transmission and hence results in unreliable key distribution due to high packet loss rate in mobile adhoc networks.

Destination Sequenced Distance Vector (DSDV) [17] is a table driven proactive routing protocol designed for mobile ad hoc networks. This protocol maintains routing table as a permanent storage. Routes are maintained through periodically and event triggered exchanges the routing table as the node join and leave. Route selection is based on optimization of distance vector. It avoids routing loops and each node has a unique sequence number which updates periodically. It is mainly used for intra cluster routing. It allows fast reaction to topology changes.

Improvement of DSDV (IDSDV) [18, 19], improves the delivery ratio of Destination-Sequenced Distance Vector (DSDV) routing protocol in mobile ad hoc networks with high mobility. It uses message exchange scheme for its invalid route reconstruction but does have multicast connectivity between nodes.

The proposal of this paper is to present a new Cluster Based Multicast Tree (CBMT) using Multicast DSDV for secure multicast key distribution. MDSDV have multicast connectivity between nodes. It sends acknowledgement for each transmission in order to reduce the retransmission. The LCs are elected easily with periodic updates of node join and leave information using multicast tree. This overcomes the issues of end to end delay, unreliability with high packet drop rate and low key delivery ratio.

3. CBMT using MDSDV

The main idea of CBMT is to use MDSDV routing protocol to elect the local controllers of the created clusters. The principle of this clustering scheme is to start with the group source Group Controller (GC), to collect its 1-hop neighbors by MDSDV, and to elect LCs which are group members have child nodes at the next level. The LC belongs to the unicast path between the source and the child group members.

At this step, the elected LCs covers the group members having 2-hops neighbors of the group source. This scheme iterates until LCs cover all the group members.

The cluster based multicast tree is thus constructed using CBMT using MDSDV is shown in figure 2.

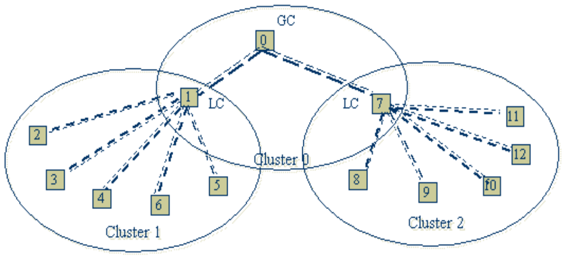

Figure. 2 CBMT using MDSDV

3.1 CBMT using MDSDV algorithm

The CBMT using MDSDV approach for multicast key distribution is described in algorithm 1 as follows:

Algorithm 1 CBMT-MDSDV (Cluster head)

```
//STEP 1
  ListLCs = Cluster Head
  Listnodes = {1, 2, 3... c} //c is the number of cluster members
//STEP 2
  for (i = 1 to List nodes) do
     if (Listnodes ≠ ϕ ) then
        if (i     multicast group) && (i has group members Childs) then
        ListLCs = ListLCs ∪ {i};
  // Add i to the local controllers     list
        Listnodes = Listnodes / {group members
                 covered by i};
  // Remove members covered by i of the members list
        CBMT-MDSDV (i);
// Execute recursively the algorithm applied to i
      end if
    end if
  end for
//STEP 3
   if (Listnodes ≠ ϕ ) then
      for (    j = 1 to Listnodesnumber)
//Compute the reachability factor of j: number of members in List nodes, in 1-hop from the node
      end for
      while (List nodes = i) do
// Group of child nodes provide reachability factor
         ListLCs = Listnodes {i};
// LC joins the new member     lists
          ListLCs ≠ Listnodes {i};
// Remove from the members list
      end while
  end if
```

3.2 Key Distribution

The proposed approach is to achieve secure multicast key distribution for mobile adhoc networks. In this proposed approach, the source encrypts multicast data with the TEK, and then sends it to all the members of the group following the multicast tree. The TEK distribution is achieved in parallel, according to the following steps.

Initially, the entire group members receive from the source by unicast the session key *KEKcsg-0* (key encryption key of the sub-group 0), encrypted with their respective public keys. New clusters will then be created dynamically.

The local controllers form a multicast group GLC (Group of Local Controllers), and share a key called KEK_{ccl}. Each local controller should join this group. The local controllers decrypt this message, extract the TEK, re encrypt it with their respective clusters keys and send it to all their local members. To send the TEK to all the group members, the source encrypts it with *KEKcsg-0* and sends it to all the members of its sub-group as shown in figure 3.

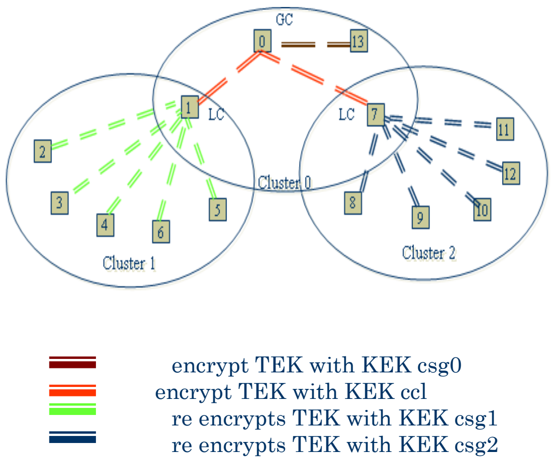
GC
0
13
1
LC
LC
7
2
3
4
6
5
Cluster 0
8
9
10
11
12
Cluster 1
Cluster 2
encrypt TEK with KEK csg0
encrypt TEK with KEK ccl
re encrypts TEK with KEK csg1
re encrypts TEK with KEK csg2

Figure. 3 Multicast key distributions

In the example shown in figure 3, the group source GC 0 collects its 1-hop neighbors by MDSDV, and elects LCs node 1 and 7, which are group members and which have child group members as 2, 3,4,5,6 and 8, 9,10,11,12 respectively. The selected nodes will be elected as local controllers. According to the step 3 in the algorithm, if a new member 13 joins the group, this approach chooses the nodes from these remaining group members that have the maximum reachability to the others nodes in one hop. This reachability information is collected through the MDSDV routing protocol, and attached the created cluster. If the created clusters do not cover group members then the node is selected as local controller for the remaining group members.

The major advantage of this solution is to minimize the overhead of decryption and re-encryption process for the local controllers. Hence local controller should only to decrypt and re-encrypt the TEK and not all the multicast flow which in turn makes the multicast key distribution as reliable one.

4. Simulation Results

The proposed CBMT using MDSDV is simulated under Linux Fedora, using the network simulator NS2 version ns-allinone-2.33[20]. The following are the parameters considered in the simulation as shown in the table1.

Table 1: Simulation Parameters

The density of group members	Group members number (7 - 13 - 28)
Network surface	1000m*1000m, 1500m*1500m, 2000m *2000m
The mobility scenario	*setdest* provided by NS2
The maximal speed of members	10km/h (2.77m/sec)
The pause time	20 seconds
The simulation duration	200 seconds
Physical/Mac layer	IEEE 802.11
Mobility model	Random waypoint model
Routing protocol	MDSDV
Traffic	Only unicast distribution keys traffic exists in the simulation. The source of the group sends the TEK to the LCs, which is forwarded to the local members

This scheme focuses on the cluster based multicast tree using MDSDV for secure multicast key distribution. It evaluates its performance in terms of end to end delay, packet drop rate and key delivery ratio under varying network conditions.

The evaluation of the metrics is as follows.

1. End to End Delay (TD**)**: The average delay of key transmission from the source to the receivers. This metrics allows evaluating the average delay to forward a key from a LC to its cluster members. Transmission delay is calculated as follows,

$$TD(N) = t_s + t_k + \sum_{i=1}^{n} ((1 - p_i)N_i)$$

N--> No. of packets from source to destination

Ni-->.No. of packets transmitted to path

Pi--> packet drop TD--> Transfer delay

ts--> transmitting setup tk-->transmitting key size

2. Packet Loss Rate (PDR): is obtained as subtracting number of packets received at the destination from number of packets send to destination. This metrics allows in evaluating the reliability of the protocol in term of packet loss rate in key transmission from the source to the group members.

$$PDR = \text{No. of packets sent to destination} - \text{No. of packets received at the destination}$$

3. Key Delivery Ratio (KDR): 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 from the source to the group members.

$$\text{KDR} = \frac{\text{Number of received keys}}{\text{Number of sent keys}} .$$

The simulations are conducted and the performance is compared for CBMT using DSDV, IDSDV and MDSDV with varying density of cluster and network surface. This comparison is done in terms of end to end delay, packet drop ratio and key delivery ratio. The simulation results of the metrics in 2000m network surface area are shown in figure 4a, 4b and 4c.

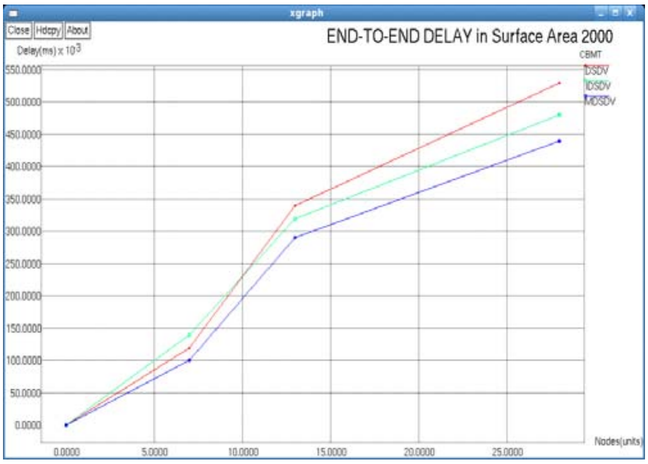

Figure. 4a. End to End Delay in multicast key distributions

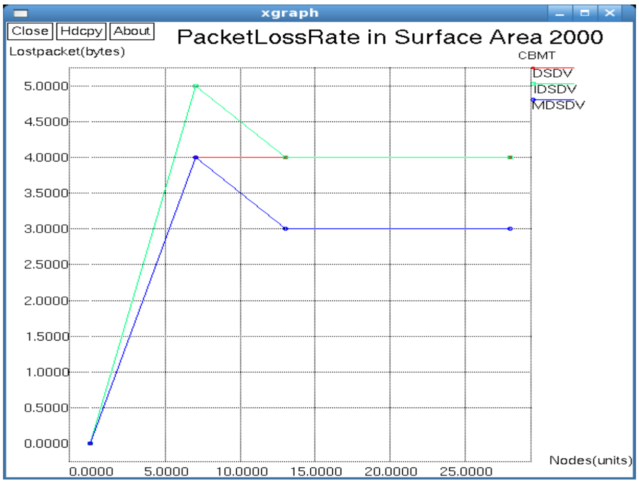

Figure. 4b. Packet loss rate in multicast key distributions

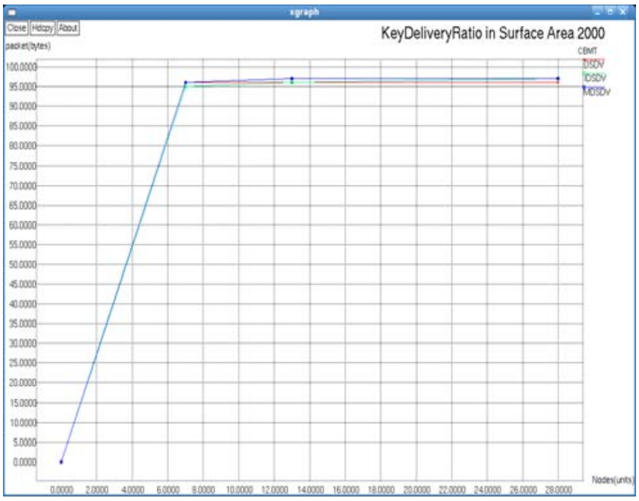

Figure. 4c. Key delivery ratio in multicast key distributions

From the simulation results, it can be observed that CBMT using MDSDV divides the group with the effective multicast connectivity between nodes. It allows fast reaction to topology changes. This approach minimizes the end to end delay of key delivery for multicast key distribution. This is due to the fact that it sends acknowledgement for each transmission in order to reduce the retransmission. It also gives better performance and achieves reliability in terms of packet drop rate and key delivery ratio and in CBMT using MDSDV compared to DSDV and IDSDV in varying network conditions.

5. Conclusion

Secure multicast Key distribution is a significant requirement in emerging applications of mobile adhoc environments like military or public emergency network applications. This paper proposes a new cluster based multicast tree for secure multicast key distribution in mobile adhoc networks. According to CBMT, for secure multicast communication, source node uses MDSDV to collects its 1 hop neighbors to form cluster and each node which have child node is elected as the Local controllers of the created clusters. MDSDV have multicast connectivity between nodes. It sends acknowledgement for each transmission in order to reduce the retransmission. So the LCs can be elected easily with periodic updates of node join and leave information. This overcomes the issues of end to end delay and unreliability with high packet drop rate and low key delivery ratio. Furthermore, the simulations of CBMT with DSDV, IDSDV and MDSDV with varying density of cluster and network surface are conducted in a simulation environment using network simulator NS2. In this, CBMT using MDSDV shows better performance than using DSDV and

IDSDV in terms of end to end delay, packet drop rate and key delivery ratio.

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 Signal Processing, pp 201-204, Apr 2003.

[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] B.Kim, H.Cho, J. Lee, "Efficient Key Distribution Protocol for secure Multicast Communication", LCNS 3043, pp 1007-1016, Apr 2004.

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

[9] 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.

[10] H. Bettahar, A. Bouabdallah, and Y. Challal, "An adaptive key management protocol for secure multicast", Proc.IEEE International Conference on Computer Communications and Networks, pp 190-195, Oct 2002.

[11] M. Bouassida, I. Chrisment, and O. Festor, "An Enhanced Hybrid Key Management Protocol for Secure Multicast in Ad Hoc Networks". LCNS 3042, pp 725-742, Apr 2004.

[12] S. Mittra, "Iolus: A framework for scalable secure multicasting", SIGCOMM, pages 277–288, 1997.

[13] Y. Challal, H. Bettahar, and A. Bouabdallah, "SAKM: A Scalable and Adaptive Key Management Approach for Multicast Communications", ACM SIGCOMM Computer Communication Review, pp 55-70, April 2004.

[14] M. Bouassida, I. Chrisment, and O. Festor, "Efficient Clustering for Multicast Key Distribution in MANETs", LCNS 3462, pp 138-153, May 2005.

[15] M. Bouassida, I. Chrisment, and O. Festor, "Group Key Management in Manets", International Journal of Network Security, pp 67-79, Jan 2008.

[16] M. Bouassida, I. Chrisment, and O. Festor "Efficient group key management protocol in MANETs using multipoint relaying technique", Proc.IEEE International Conference on Networking, pp 64, Apr. 2006.

[17] http://en.wikipedia.org/wiki/ DestinationSequenced_Distance_Vector_routing.

[18] T. Liu & K. Liu, Improvement on DSDV in Mobile Ad Hoc Networks, IEEE, China, 2007, pp.1637-1640

[19] A H A Rahman, Z A Zukarnain, " Performance Comparison of AODV, DSDV and I-DSDV routing protocols in Mobile Adhoc Networks", European Journal of scientific Research, pp 566-576, 2009.

[20] The Network Simulator NS-2 tutorial homepage, http://www.isi.edu/nsnam/ns/tutorial/index.html

D. Suganya Devi received her B.Sc (Chemistry) and MCA from PSGR Krishnammal College for Women, Coimbatore in 1996 and 1999 respectively. And, she received her M.Phil degree in Computer Science in the year of 2003 from Manonmaniam Sundaranar University, Thirunelveli. She is pursuing her PhD at Avinashilingam University for Women. She is currently working as a Senior Lecturer in the Department of computer Applications, SNR Sons College, Coimbatore. She has 10 years of teaching experience. She has presented 12 papers in various national and international conferences. Her research interests Multicast Communication, MANET and Network Security.

Dr. Padmavathi Ganapathi is the professor and head of Department of Computer Science, Avinashilingam University for Women, Coimbatore. She has 21 years of teaching experience and one year Industrial experience. Her areas of interest include Network security and Cryptography and real time communication. She has more than 60 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.