International journal on applications of graph theory in wireless ad hoc networks and sensor networks (GRAPH-HOC) Vol.2, No.3, September 2010

IMPACT OF MOBILITY FOR QOS BASED SECURE MANET

D. Suganya Devi[1] and Dr. G.Padmavathi[2]

[1]Department of Computer Applications, SNR SONS College, Coimbatore, TamilNadu, India
Sugan.devi1@gmail.com
[2]Department of Computer Science, Avinashilingam University, Coimbatore, TamilNadu, India
Ganapathi.padmavathi@gmail.com

ABSTRACT

Secure multicast communication in Mobile Adhoc Networks (MANETs) is challenging due to its inherent characteristics of infrastructure-less architecture with lack of central authority, limited resources such as bandwidth, energy and power. Several group oriented applications over MANETs create new challenges to routing protocols in terms of QOS requirements. In many multicast interactions, due to its frequent node mobility, new member can join and current members can leave at a time. It is necessary to choose a routing protocol which establishes true connectivity between the mobile nodes. The pattern of movement of members is classified into different mobility models and each one has its own distinct features. It is a crucial part in the performance of MANET. Hence key management is the fundamental challenge in achieving secure communication using multicast key distribution for mobile adhoc networks. This paper describes the impact of mobility models for the performance of a new cluster-based multicast tree algorithm with destination sequenced distance vector routing protocol in terms of QOS requirements such as end to end delay, energy consumption and key delivery ratio. For simulation purposes, three mobility models are considered. Simulation results illustrate the performance of routing protocol with different mobility models and different mobility speed under varying network conditions.

KEYWORDS

DSDV, MANET, Mobility models, Multicast Communication, Routing Protocol

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, 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].

These security services can be facilitated if group members share a common secret, which in turn makes key management a fundamental challenge in designing secure multicast and reliable group communication systems. Group confidentiality requires that 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.

Most of these security services rely generally on encryption using Traffic Encryption Keys (TEKs). The Key management [5] includes creating, distributing and updating the keys then it constitutes a basic block for secure multicast communication applications.

The process of updating the keys and distributing them to the group members is called rekeying operation. A critical problem with any rekey technique is scalability [6]. 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 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 characteristics.

Energy consumption: This induces minimization of number of transmissions for the forwarding messages to all the group members.

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.

Key Delivery Ratio: This induces number of successful key transmission to all group members without any loss of packet during multicast key distribution.

Thus a secure multicast key distribution in mobile ad hoc environment should focus on both security and Qos characteristics. To overcome these problems, several approaches propose a multicast group clustering. [7, 8, 9]. 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 and hence it overcomes 1-affects-n phenomenon.

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:

DSDV (Destination Sequenced Distance Vector) routing protocol to maintain routing table periodically. 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.

MAC 802.11 for providing communication between nodes.

Channel bandwidth for minimization of congestion that occurs during transmission.

Mobile Adhoc network have enormous secure group oriented applications, such as emergency and relief operations, military and disaster situations, and conference or class room meetings. In each of these applications, due to frequent node mobility, new member can join and current members can leave at a time, dependent on interactions among participants and the environment. The moving behavior of each member in MANET should be realistic.

The frequent mobility of members and limited communication resources make routing in MANET very difficult. Mobility causes frequent topology changes and may break existing paths. A routing protocol should quickly adapt to the topology changes and efficiently search for new paths. To overcome these above limitations, Destination Sequenced Distance Vector routing protocol is used. It allows fast reaction to topology changes and is specially designed for MANET.

The pattern of movement of members can be classified into different mobility models and each is characterized by their own distinct features. The traditional mobility models includes (i) Random Waypoint Model (ii) Random Walk Model and (iii) Group Mobility Model which are simple to implement and analyze. These are randomized model in which each member chooses their velocity and direction independently without any restrictions. Hence these models do not capture correlation between the member movements. Recent work on mobility models attempts to identify common mobility movement.

Thus this new CBMT approach is an efficient dynamic clustering scheme using DSDV routing protocol, which makes easy to elect the local controllers of the clusters and updates periodically as the node joins and leaves the cluster. This paper describes the impact of the three mobility models on the performance of CBMT approach with DSDV routing protocol for QOS based secure multicast communication in MANET. Simulations have been conducted under varying network conditions in terms of QOS requirements in two scenarios. The first scenario analyzes the different mobility models with varying number of nodes and speed and the second scenario analyzes with two different node mobility speeds.

The remainder of this paper is structured as follows. Section 2 presents the related works about different mobility models. Section 3 describes the impact of the three mobility models for CBMT used in this simulation. Section 4 describes the methodology used to evaluate the performance. Section 5 discusses QOS based performance analyzes of simulation results. Finally, Section 6 concludes the paper.

2. RELATED WORK

Several Clustering approaches [7, 8, and 9] 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. 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 [10] and DEP [7] belong to the category that is more scalable. Dynamic clustering approach aims to solve the “1 affect n” phenomenon. AKMP [8], SAKM [11] belong to this approach and are dedicated to wired networks. Enhanced BAAL [9] proposes dynamic clustering scheme for multicast key distribution in adhoc networks.

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) [17] 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 results in retransmission which consumes more energy and unreliable key distribution for mobile adhoc networks.

This section also describes a sampling of the mobility models that have been designed specifically for ad hoc networks. Classification and survey of existing mobility models are given in [18]. Since tactical network consist of mobile devices, the mobility models used has a decisive impact. A recent study show that the average speed of a node using Random Waypoint decreases with time, and hence the results obtained using this model becomes unreliable as the simulation advances [19]. In [20], the effect of mobility models on the performance of mobile ad hoc network using unicast routing protocol is discussed.

The IMPORTANT framework [21] characterizes movement based on spatial dependence, relative speed, and other factors and illustrates how these metrics impact unicast routing performance. In [22] the authors have shown that the mobility model used can significantly impact the performance of ad hoc routing protocols, including the packet delivery ratio, the control overhead and the data packet delay.

The performance of two multicast routing protocols ODMRP and ADMR for mobile adhoc networks with different mobility models are compared in [23]. The difference in the performance is analyzed widely across the different mobility models. The performance of AODV with effect of random mobility models patterns are compared in [24]. Here the performance is analyzed using varying network load, random based mobility model and network size.

In [25], the simulation done based on the performance of multicast tree algorithms for MANET. In [26], the simulation done based on the performance of multipath routing protocols for MANET. These both include performance metric as lifetime per multicast tree and multipath set respectively. Mobility framework called Dispersion mobility model [27] organized mobile nodes as group of clusters and evaluated performance under different mobility patterns and for different implementations.

The proposal of this paper is to present the impact of mobility models for this new Cluster Based Multicast Tree (CBMT) approach for multicast key distribution. The CBMT algorithm is simulated with different mobility models in network simulator NS-allinone-2.33 and the performance is studied using the QOS characteristics in multicast key distribution.

3. IMPACT OF MOBILITY MODELS

This section describes the impact of different mobility models for CBMT approach.

3.1 CBMT

The main idea of CBMT is to use DSDV routing protocol to elect the local controllers of the created clusters. The principles of the proposed clustering approach are described in steps as follows.

Step1: Initially, the list of LCs contains only the source of the group GC, which collects all its 1-hop neighbours by DSDV, and to elect LCs which are group members and which have child group members (the LC belongs to the unicast path between the source and the child group members). The list of the current LC is collected.

Step2: Traverse the list nodes, while there are group members not yet covered by LCs, and verify for each one if it is a group member and if it has child group members. In case of success, add the LC to the list of LCs, and withdraw from the list of group members. All the members reachable by this new LC will form a new cluster.

Step3: If group members that exist and do not belong to the formed clusters then choose the nodes that have the maximum reachability to the others nodes in one hop from the remaining members. This reachability information is collected through the MDSDV routing protocol.

However, the created clusters do not cover group members yet. Thus, nodes are selected as local controllers for the remaining group members.

3.2. Mobility model

A mobility model is used to capture the movement of objects in simulations. In MANET, a mobility model is used to define the movement of a mobile wireless node. There are two types of MANET mobility models: single-entity and group. In single-entity models, each mobile node moves independently of all the other nodes within the network area.

For simplicity, most of the mobility models are defined for a rectangular network area enclosed by (0, 0), (0, ymax), (xmax, ymax), and (xmax, 0). A characteristic feature of every mobility model is to ensure that a mobile node will not travel outside the network area. In group mobility models, nodes are assumed to be organized in groups and the mobility of a node is often reflective of the movement pattern of the entire group.

In this section, three mobility models are used which are designed to capture a wide range of mobility patterns for adhoc applications. Mobility models are chosen for simulation based on their different classes of motion as random based and group based movements.

3.2.1 Random based Mobility Models:

In random based mobility models, the mobile nodes move randomly and freely without restrictions. The destination, speed and direction are all chosen randomly and independently of other nodes. The different types are discussed below:

(a) Random Waypoint Mobility model: The random way point mobility model is simple and is widely used to evaluate the performance of MANETs. The random way point mobility model contains pause time between changes in direction and/or speed. Once a Mobile Node begins to move, it stays in one location for certain period of time called pause time. After the specified pause time is elapsed, the mobile node randomly selects the next destination in the simulation area and chooses a speed uniformly distributed between the minimum speed and maximum speed and travels with a speed v whose value is uniformly chosen in the interval $(0, Vmax)$. V*max* is some parameter that can be set to reflect the degree of mobility. Then, the MN continues its journey toward the newly selected destination at the chosen speed. As soon as the MN arrives at the destination, it stays again for the indicated pause time before repeating the process. Figure 1 shows the travelling pattern of mobile nodes using random way point mobility model.

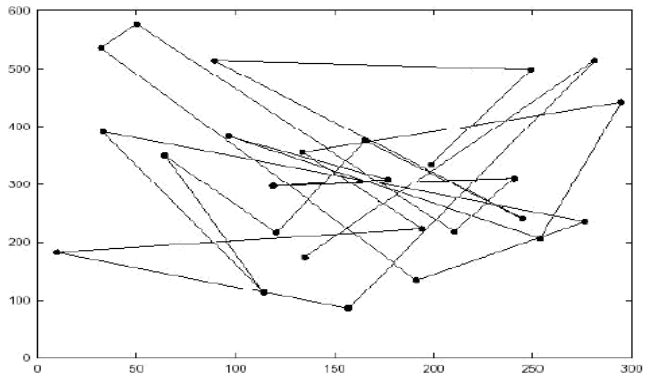

Figure 1 Traveling pattern of mobile nodes using Random way point mobility model

(b) Random Walk Mobility Model: This model is similar to the random waypoint, but at a trip transition instant, a node picks direction, trip duration and numeric speed. The node moves in the given direction with the given numeric speed for the given trip duration. Each movement in the Random Walk mobility model occurs in either a constant time interval t or a constant distance travelled d, at the end of which a new direction and speed are calculated. If a mobile node moving according to this model reaches a boundary area, it bounces off the boundary border with an angle determined by the incoming direction. The mobile node then continues along this new path. The Random Walk mobility model is a memory less mobility pattern because it does not retain knowledge concerning its past locations and speed values. Figure 2 shows the travelling pattern of mobile nodes using random way point mobility model.

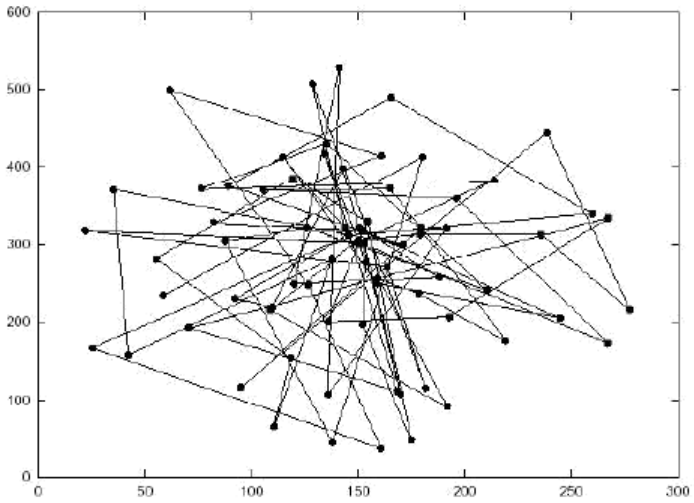

Figure 2 Traveling patterns of mobile nodes using Random walk mobility model

3.2.2 Group Mobility Model:

Group mobility model represents multiple mobile nodes whose actions are completely independent of each other. For example, a group of soldiers in a military scenario may be assigned the task of searching a particular plot of land in order to destroy land mines. In order to model such situations, a group mobility model is needed to simulate this kind of characteristic. Here each group has a logical centre (group leader) that determines the group's motion behavior. Initially each member of the group is uniformly distributed in the neighbourhood of the group leader. Subsequently, at each instant, every node has speed and direction that is derived by randomly deviating from that of the group leader. Each node deviates from its velocity (both speed and direction) randomly from that of the leader.

4 EVALUATION METHODOLOGY

The simulation methodology is used to evaluate the performance of secure mobile adhoc network. The network simulation is done for CBMT approach with different mobility models under Linux Fedora, using the network simulator [28] NS2 version ns-allinone-2.33.

4.1 Performance Metrics

The performance is evaluated in terms of QOS requirements such as end to end delay, energy consumption, packet delivery ratio and routing overhead.

Average End to end delay or Average Latency: The average end to end delay is a measure of average delay of transmissions from source to the receivers.

Energy Consumption (E): is defined as the sum of units required to the keys transmission throughout the duration of simulation.

Key Delivery Ratio (KDR) or packet delivery ratio (PDR): 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.

Routing Overhead: It is an important metric for measuring scalability of a protocol. The number of routing packet transmitted per data packet delivered at destination.

4.2 Simulation Setup

This simulation setup is defined by the following parameters.

- The density of group members within the ad hoc network: group members number (7 - 13 - 28)
- Network surface (1000m*1000m, 1500m*1500m, 2000m *2000m).
- The mobility scenarios are generated by the automatic generator setdest provided by NS2
- The pause time is 20 seconds
- The simulation duration is 200 seconds.
- Physical/Mac layer: IEEE 802.11.
- Routing protocol: DSDV

The simulation will be conducted in two different scenarios to obtain a good result in terms of QOS performance metrics.

1. Scenario 1 compares the different mobility models in varying number of nodes and speed.
2. Scenario 2 evaluates the mobility models in varying number of nodes and compares with two different mobility speeds as 5m/s and 10 m/s.

5 SIMULATION RESULTS

This section presents simulation results to compare and analyze the performance of CBMT approach with different mobility models for QOS based secure MANETs. The simulation results are based on two scenarios which illustrates the performance.

5.1. Different Mobility Models

In this scenario, all the three mobility models are evaluated on CBMT approach based on QOS requirements with number of nodes and speed.

Figure 3 compares three mobility models as Random waypoint mobility model, Random walk mobility model and Group mobility model in term of average end to end delay in multicast communication. Results illustrates as Random waypoint mobility model gives less delay than the other two mobility models for CBMT with DSDV routing protocol in multicast communication.

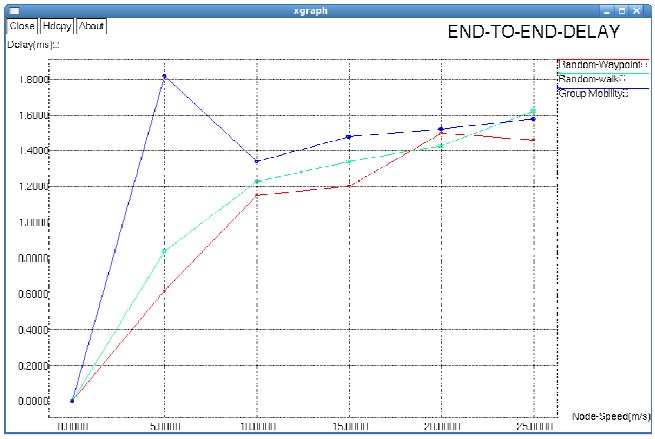

Figure 3 Average end to end delay

Figure 4 shows the comparison of mobility models in term of energy consumption.

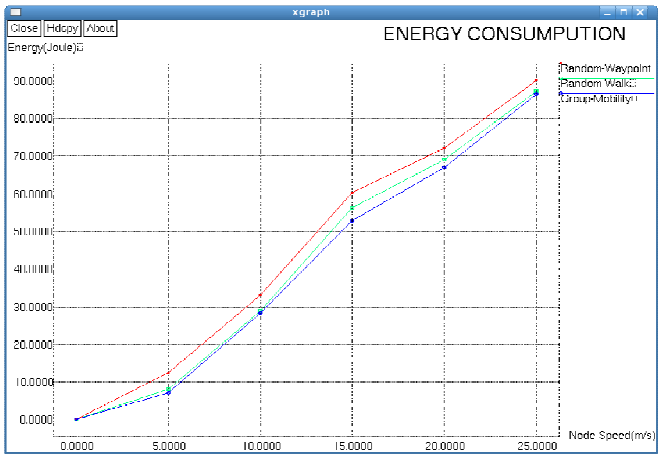

Figure 4 Energy consumption

Figure 5 shows the comparison of mobility models in term of packet delivery ratio. Results illustrates as Random waypoint mobility model gives increased delivery ratio than the other two mobility models for secure multicast communication.

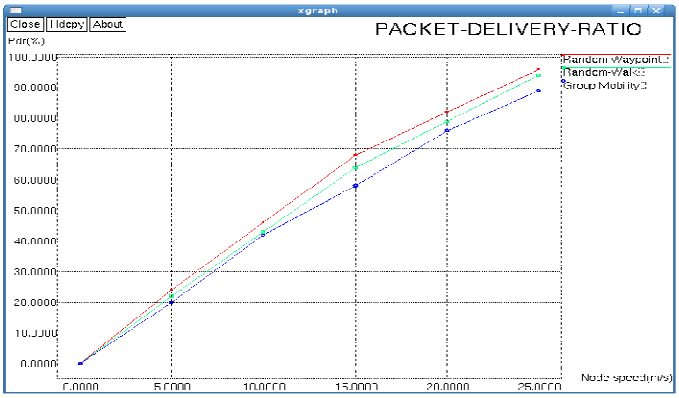

Figure 5 Packet delivery ratio

Figure 6 shows the comparison of mobility models in term of routing overhead. Results illustrates as all the mobility models show that the routing overhead is increased when the number of nodes and node speed is increased.

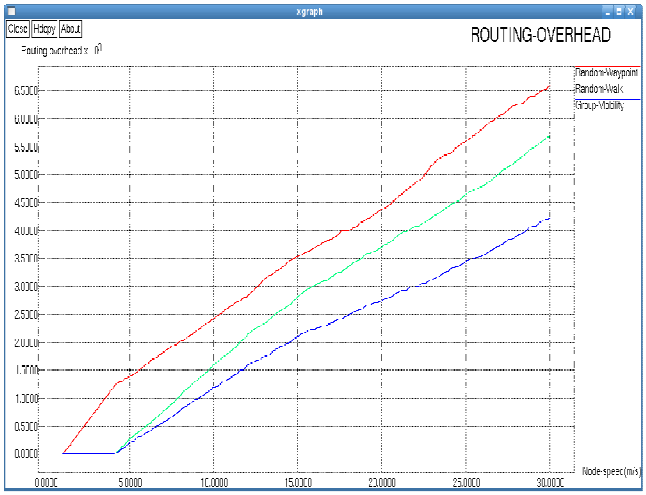

Figure 6 Routing overhead

The above simulation results illustrates that the performance of CBMT approach with different mobility models at varying number of nodes and node speed in terms of QOS metrics.

5.2. Different Node Mobility Speed

This section presents simulation results to compare the impact of nodes mobility speed on the performance of CBMT with different randomized mobility models for multicast communications in terms of key delivery ratio, latency and energy consumption in varying density of nodes and network surface. The simulation results are shown in table I.

TABLE I. COMPARISON TABLE

Nodes Vs Mobility	Key delivery ratio		Latency		Energy	
	5m/s	10m/s	5m/s	10m/s	5m/s	10m/s
5	851	827	0.84	1.82	8.1	7.1
10	1387	1161	1.23	1.34	29.04	28.34
15	2310	2174	1.34	1.48	56.23	52.94
20	2523	2374	1.43	1.52	69.17	66.92
25	2790	2547	1.62	1.58	87.22	86.53

The movement of groups is characterized by several parameters, such as its speed. Within the same group, the speed of its member are not identical, they take their values within an interval

around the speed of the group. This simulation illustrate the multicast communication among the group with varying number of nodes and for the two nodes mobility speed as 5m/s and 10m/s for random based model. The figure 7 shows the impact of nodes mobility speed on the key delivery ratio in multicast communication. The key delivery ratio decreases as the nodes mobility speed increases.

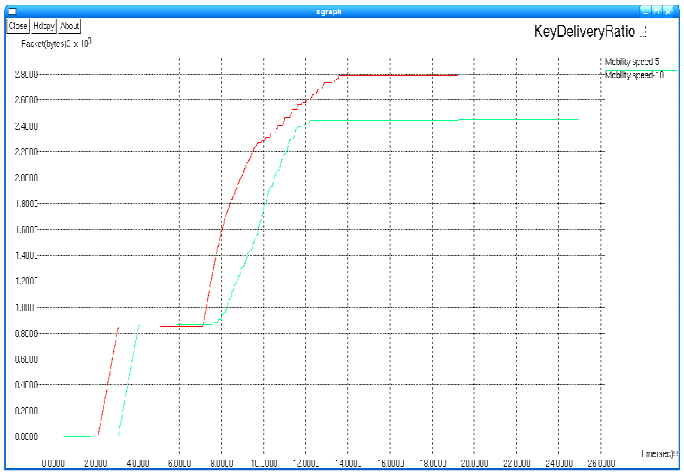

Figure 7 Impact of Nodes mobility on key delivery ratio

The figure 8 shows the impact of nodes mobility speed on the average latency of multicast communication. The average latency decreases as the nodes mobility speed decreases.

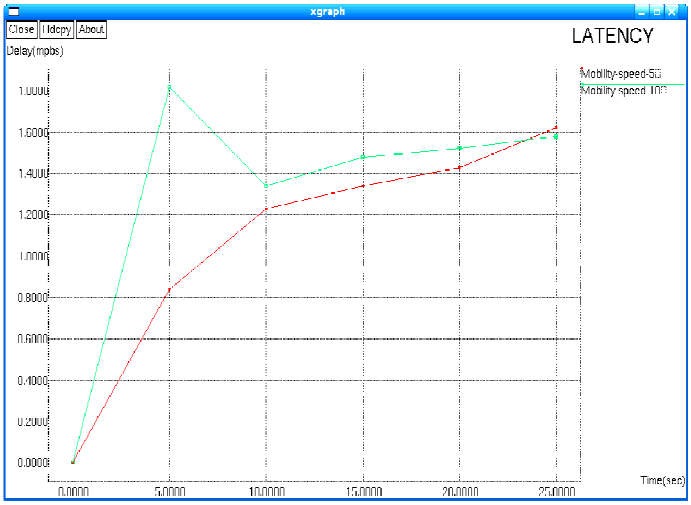

Figure 8 Impact of Nodes mobility on Latency

The figure 9 shows the impact of nodes mobility speed on the energy consumption during simulation period of multicast communication. It consumes less energy as the nodes mobility speed increases.

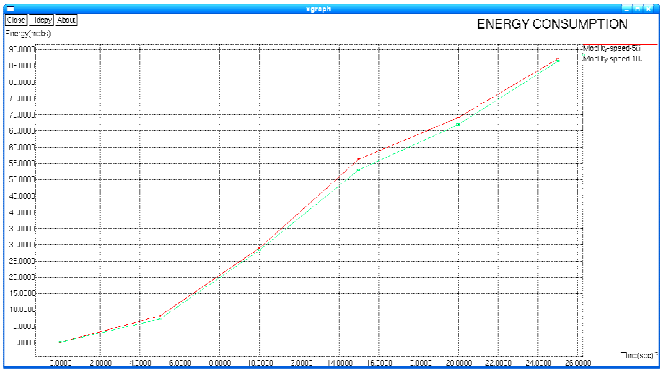

Figure 9 Impact of Nodes mobility on energy consumption

5. CONCLUSION

Secure multicast communication is a significant requirement in emerging applications in adhoc environments like military or public emergency network applications. Membership dynamism is a major challenge in mobile adhoc networks for multicast communications. Importance of mobility patterns on routing protocols of mobile adhoc network is studied. Simulation results illustrate that the impact of different mobility models on the performance of CBMT approach with DSDV routing protocol varies widely across different number of nodes and node mobility speed in terms of QOS performance metrics as average end to end delay, energy consumption key delivery ratio and routing overhead for secure MANETs. It is observed that the movement of nodes is characterized based on mobility speed. It is observed that the Random waypoint produces better results in suitable conditions than the other two mobility models in such adhoc environment.

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] K.Rahman, R.Zaman, A.Reddy, " An Efficient DSDV routing Protocol for Wireless Mobile Adhoc Networks and its Performance Comparison", Proc. European Sym. On Computer Modeling and Simulation, pp 508-511, Nov 2008.
[13] S. Mittra, "Iolus: A framework for scalable secure multicasting", SIGCOMM, pages 277–288, 1997.
[14] 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.
[15] M. Bouassida, I. Chrisment, and O. Festor, "Efficient Clustering for Multicast Key Distribution in MANETs", LCNS 3462, pp 138-153, May 2005.
[16] M. Bouassida, I. Chrisment, and O. Festor, "Group Key Management in Manets", International Journal of Network Security, pp 67-79, Jan 2008.
[17] 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.
[18] N.Aschenbruck,E.Gerhands-Padilla ,P.Martini,"A Survey on mobility models for Performance analysis in Tactical Mobile networks," Journal of Telecommunication and Information Technology,Vol.2 pp.54-61,2008.
[19] J. Yoon, M. Liu, and B. Noble. Random waypoint considered harmful, 2003.
[20] Geetha jayakumar, Gopinath Ganapathi,"Reference point group mobility and random waypoint models in performance evaluation of MANET routing protocols," Hindwi publication corporation, Journal of Computer systems, Networks, Communication Vol.2008 (2008).
[21] F. Bai, N. Sadagopan, and A. Helmy. IMPORTANT: A framework to systematically analyze the Impact of Mobility on Performance of RouTing protocols for Adhoc Networks. In IEEE INFOCOM, 2003.
[22] A. P. Jardosh, E. M. Belding-Royer, K. C. Almeroth, and S. Suri, "Toward realistic mobility models for mobile ad hoc networks," in Proc ACM MOBICOM, San Diego, CA, Sep. 2003, pp. 217–229.
[23] Malarkodi, Gopal, and Venkataramani, "Performance evaluation of adhoc networks with different multicast routing protocols and mobility models," In IEEE Computer Society, 2009.
[24] Gowrishankar, Basavaraju and Subir Kumar,"Effect of Random Mobility Models Pattern in Mobile Adhoc Networks," IJCSNS Vol. 7 No. 6, June 2007.
[25] Nicholas Cooper and Natarajan Maghanathan, " Impact of Mobility Models on Multicast Routing in Mobile Adhoc Networks", 2007.
[26] Nicholas Cooper and Natarajan Maghanathan, " Impact of Mobility Models on Multipath Routing in Mobile Adhoc Networks", 2007.
[27] Rajini Girinath and Selvam,"Performance Analysis of Dispersion Mobility Model in Mobile Adhoc Networks," IJCSNS Vol. 8 No. 3, March 2008.
[28] "The network simulator ns-2. http://www.isi.edu/nsnam/ns2,"

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 an Assistant Professor in the Department of computer Applications, SNR Sons College, Coimbatore. She has 11 years of teaching experience. She has presented 15 papers in various national and international conferences. She also published 5 papers in international level journals. 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 120 publications at national and International level. She is a life member of many professional organizations like CSI, ISTE, AACE, WSEAS, ISCA, and UWA.