DUALISTIC SIDE BY SIDE ENDORSEMENT OF MULTICAST PROTOCOL BY DYNAMIC CLUSTERING IN MANET

[1]P.MANJULA
[1]Asst.Professor, Department of Information Technology, Veltech Multitech Dr. Rangarajan Dr.Sakunthala Engineering College, Chennai
Email: [1]manjula.arunraj@gmail.com

ABSTRACT

Source authentication and message integrity become a fundamental requirement for ad-hoc network. Clustering is an effective technique to reduce overhead and ensure scalability which we are using in this paper. The proposed work is new Tiered [11] Authentication scheme for Multicast traffic (TAM), using dynamic clustering algorithm .The algorithm modifies Weighted Clustering Algorithm (WCA) with mobility prediction. The weighted Clustering Algorithm itself is enhanced with the use of mobility prediction in the Cluster Maintenance phase. Meanwhile the nodes are mobile in MANET maintenance is essential. Effective exploitation of power, minutest depletion of Bandwidth, Additional Stable Clusters by using WCA helps in improving the QOS in MANETS.

Keywords: *MANET, TAM, Clustering, Weighted Clustering Algorithm, Mobility Prediction.*

1. INTRODUCTION

Multicasting is an efficient communication mechanism for group-oriented applications. [11] Multicast traffic among the nodes has to be delivered in a secure and trusted manner. Network services need to achieve the following security goals:
(1) Confidentiality, (2) Message reliability and (3) Source Endorsement .In this paper we are achieving source authentication and message integrity [3].
TESLA is Timed Efficient Stream Loss-tolerant Authentication system. A stream S is divided into chunks called messages. Each message is sent in a packet along with additional authentication information [5].TESLA is based on time asymmetry [4].The main drawback is TESLA limits scalability. Hence we are going for TAM.
TAM thus [16] combines the advantages of the secret information asymmetry and the time asymmetry paradigms [3].TAM improves the scalability by using clusters and controlling the maximum size of the cluster within which time asymmetric schemes are employed [1]. Clustering is a best technique for managing nodes in a MANET. In this paper we are using dynamic clustering algorithm by modifying weighted clustering algorithm (WCA) with mobility prediction [6]. U The mobility prediction with WCA will reduce the power consumption and Increase the Stability of the Cluster. We are combining the advantages in [1] and [6].In our paper we are using dynamic clustering algorithm in TAM. Dynamic clustering algorithm uses WCA [8] for cluster formation and mobility prediction for maintenance.

2. TIERED AUTHENTICATION OF MULTICAST PROTOCOL USING DYNAMIC CLUSTERING IN MANET

Our proposed paper combines advantage of time asymmetry and secret information asymmetry. Asymmetry means a receiver verify the message by using MAC in a packet without knowing to generate MAC. A MAC algorithm, sometimes called a keyed hash [17] function (however, cryptographic hash function is only one of the possible ways to generate MACs), accepts as input a secret key and an arbitrary-length message to be authenticated, and outputs a MAC known as a tag. The MAC value protects both a message's data integrity as well as its authenticity, by allowing verifiers to detect any changes to the message content.

The deployment of MANET, [15] poses several challenging issues, due to the dynamic nature of the nodes, the arbitrary topology, the limited wireless range of nodes, and transmission errors. Since all the nodes in the network collaborate to forward the data, the wireless channel is prone to active and passive attacks by malicious nodes, such as Denial of Service (DoS), eavesdropping etc.

Implementing security is therefore of prime importance in such networks. The components of security mechanism are:

2.1 Data Reliability

Data reliability is assuring that data has not changed, destroyed or lost in an unauthorized manner. Cryptographic [12] hash function is used to assure data integrity. A hash function is mapping binary strings of arbitrary length to binary string of fixed length. A cryptographic hash function is a hash function; that is, an algorithm that takes an arbitrary block of data and returns a fixed-size bit string, the (cryptographic) hash value, such that any change to data will change the hash value. The data to be encoded are often called the "message," and the hash value is sometimes called the message digest or simply digests.

The ideal cryptographic hash function has four main properties:

- It is easy to compute the hash value for any given message
- It is infeasible to generate a message that has a given hash
- It is infeasible to modify a message without changing the hash.

Cryptographic hash functions have many information security applications, notably in digital signatures, message authentication codes (MACs), and other forms of authentication. They can also be used as ordinary hash functions, to index data in hash tables, for fingerprinting, to detect duplicate data or uniquely identify files, and as checksums to detect accidental data corruption. Indeed, in information security contexts, cryptographic hash values are sometimes called (digital) fingerprints, checksums, or just hash values, even though all these terms stand for functions with rather different properties and purposes.

2.2 Data Origin Authentication

Data origin authentication is the corroboration that the source of the data received is as claimed. Message authentication codes (MACs) is a cryptographic mechanism that assure data origin authentication and data integrity at the same time.

MACs differ [17] from digital signatures as MAC values are both generated and verified using the same secret key. This implies that the sender and receiver of a message must agree on the same key before initiating communications, as is the case with symmetric encryption. For the same reason, MACs do not provide the property of non-repudiation offered by signatures specifically in the case of a network-wide shared secret key: any user who can verify a MAC is also capable of generating MACs for other messages. In contrast, a digital signature is generated using the private key of a key pair, which is asymmetric encryption. Since this private key is only accessible to its holder, a digital signature proves that a document was signed by none other than that holder. Thus, digital signatures do offer non-repudiation. In our proposed model we are using MAC that provides both origin authentication and data integrity.

2.3 Non-Refutation With Evidence Of Cause

Non- refutation proves recipient with origin of data and also protect it from false sender. One of the main issues to consider in a [15] certificate-based scheme is the secure distribution of the public keys to all the nodes in the network. In wired network the centralized server handles creation, renewal and revocation of certificates. But in ad-hoc network the topology changes and its won't have fixed infrastructure hence reauthentication is required. To overcome this we are using several public key management mechanisms. In our proposed work we are using one way hash function as public key management mechanism.

2.4 Confidentiality

Confidentiality is that information is not disclosed to other individuals. [18] Encryption is the conversion of data into a form, called a cipher text that cannot be easily understood by unauthorized people. Decryption is the process of converting encrypted data back into its original form, so it can be understood. In our paper we are using one way hash function to provide confidentiality. Mobile ad hoc networks (MANETs) [14] are self-configuring infrastructure less networks comprised of mobile nodes that communicate over wireless links without any central control on a peer-to-peer basis. These individual nodes act as routers to forward both their own data and also their neighbor's data by sending and receiving packets to and from other nodes in the network infrastructure-less networks comprised of mobile nodes that communicate over wireless links without any central control on a peer-to-peer basis. These individual nodes act as routers to forward both their own data and also their neighbour's data by sending and receiving packets to and from other nodes in the network.

2.5 Time Irregularity

The main idea behind time [11] irregularity is to tie the validity of the MAC to a specific duration so that a forged packet can be discarded. One-way hash chains are usually employed to generate a series of keys so that a receiver can verify the current key based on an old key without being able to guess the future key. The source reveals the last key, in the chain to all receivers to serve as the baseline for verification. The key which is used to generate the MAC of a packet is revealed after some time period so that the key cannot be used to impersonate the source. TESLA is an example of this category.

2.6 Secret Information Asymmetry

In secret information asymmetry every node is assigned a share in a secret, e.g., a set of keys. A source appends MACs for the multicast keys so that a receiver verifies the authenticity of the message without being able to forge the MACs for the other nodes. The challenge in using this category of approaches is striking the balance between collusion resilience and performance impact. While the use of a distinct MAC per node imposes prohibitive bandwidth overhead, relying on the uniqueness of the key combinations risks susceptibility to node collusion.

2.7 Architectural Model

In ad-hoc network autonomous nodes that together set up a topology. It does not have any physical networking infrastructure. Based on the applications, an ad-hoc network can include up to a few hundreds or even thousand nodes. Communications among nodes are via multihop [16] routes using Omni directional wireless broadcasts with limited transmission range. In our model, nodes are grouped into clusters.

Clustering is a popular architectural mechanism for providing scalability of network .clustered network topologies better support routing of multicast traffic and the performance gain dominates the overhead of creating and maintaining the clusters. Each cluster is controlled by a cluster-head, which is reachable to all nodes in its cluster, either directly or over multi-hop paths.

2.7.1 Intra-Cluster Source Authentication

Intra-cluster authentication in TAM is based on TESLA using the hash function, e.g. SHA-1.The receiver recursively applies the cryptographic hash function until reaching *kl* message can be authenticated only when the used key in the chain is revealed.

The approach has two distinct advantages, namely:

- The MAC overhead single MAC is used per every multicast packet for all receivers.
- A lost key in a lost packet would not obstruct authentication process since a receiver can refer back to *Kl.*

2.7.2 Inter-Cluster Authentication

Inter-cluster multicast traffic, TAM applies a strategy based on secret information asymmetry. The source "*s*" that belongs to Clustering will send the multicast packets to the heads of all clusters that have designated receivers. For example, if the members of the multicast group for s are residing in clusters g, h, j, and k, node s sends the message to CHg, CHh, CHj, and CHk. These cluster heads will then forward the message to the receivers in their respective clusters. The rationale is that the MAC will be associated with the cluster rather than the nodes and thus the overhead is reduced significantly. In other words, the multicast from s consists of multiple multicasts; (1) from *s* to all relevant cluster heads, (2) a distinct multicast within each of the target clusters to relay the message to designated receivers.

2.8 A Dynamic Clustering Algorithm For Manets Formation Of Cluster

Initially, each node broadcasts a [19] beacon message to notify its presence to the neighbors. A beacon message contains the state of the node. Each node builds its neighbor list based on the beacon messages received. Each node computes its weight value based on the following algorithm:

Step 1:

The coefficients used in weight calculation are assumed the following values w1=0.7, w2=0.2, w3=0.05,w4=0.05

Step 2:

Compute the difference between the optimal cluster's size 'α' and the real number of neighbors 'R (V)'as spreading degree,

$\Delta sp= 1-(| \alpha -R (V)| / \alpha)$

Step 3:

For every node the sum of the distances, Dv, with all its neighbors are calculated.

Dv= Σdist(v,v') where v'ϵN(v)

Step 4:

Calculate the average speed for every node until the current time T. This gives the measure of the mobility Mv based on the X co-ordinate and Y co-ordinate ie.,position of the node v at all previous time instance t.

Step 5:

Determine how much battery power has been consumed as Pv. This is assumed to be more for a Cluster-Head when compared to an ordinary node.

Step 6:

The weight Wv for each node is calculated based on $Wv = (w1\times \Delta sp) + (w2\times Dv) + (w3\times Mv) + (w4\times Pv)$

Where Δsp is the spreading degree, Dv is the distance with its

Neighbors, Mv is the mobility of the node, and power consumed is represented by, Pv

Step 7:

The node with the smallest Wv is elected as a cluster-head. All the neighbors of the chosen cluster-head are no more Allowed to participate in the election procedure.

Modified weighted clustering algorithm
For a particular node named 'v'

Action 1:
Broadcast [19] a beacon signal to all its neighbor nodes in the transmission range;
Process the beacon signals received from the neighbor nodes in the network and form the connection matrix
Action 2:
Calculate Weight of node V, as Wv;
Action 3:
Broadcast weight value Wv to all its neighbor nodes;
Process the signals received from the neighbor nodes in the network and identify the weights of the neighbors;
Action 4:
Find the [19] node with minimum weight in the neighborhood;
If (Wv is the least weight)
Declare itself as the Cluster-head;

Step 8:

All the above steps are repeated for remaining nodes which is not yet elected as a cluster-head or assigned to a cluster. In WCA the cluster-head is choosed based on weight of each node .For calculating weight four factors are considered they are number of neighbors, sum of distance to all its neighboring nodes, mobility and battery power.

The weight Wv for each node is calculated based on

$$Wv = (w1\times \Delta sp) + (w2\times Dv) + (w3\times Mv) + (w4\times Pv)$$

Where Δsp is the spreading degree, Dv is the distance with its Neighbors, Mv is the mobility of the node, and power Consumed is represented by, Pave. The actions carried out for cluster head selection is given below. If a cluster head battery power is less than a specified threshold then it will send a life down message to all its neighbors and based on weight again election is carried out. This can reduce the failure of cluster heads.

2.9 Cluster Head:

Cluster Head selection is the important strategy in this dynamic clustering. Many authors give many effective solutions for selecting the cluster head in cluster architecture. In our proposed scheme we are using the scheme for selecting the cluster head is given below.

Cluster Head is responsible for sending and receiving data packets for that cluster. If the cluster moved then the packet get loosed, So the delay ratio, drop rate Overhead collision get increased.

So in our proposed model we also perform the checking for the battery life of the cluster head. If the battery life of the cluster head is less than some particular threshold value then that node not selected as cluster head in the election part. Mainly our proposed system focused on the weight factor based on the energy level of the nodes, if the nodes energy level is less than some threshold value then signal is sent for taking another node with highest energy level.

In our paper we are using dynamic clustering for TA. Since for dynamic clustering we are computing weight based on distance from neighbor power consumed and spreading degree. Node with less weight is chosen as head for cluster. Thus when a cluster head node battery power falls other node is elected as cluster. Mobility prediction is also done in dynamic clustering hence it reduce bandwidth for communication.

CLUSTER-HEAD
Action
Verify the threshold on the Cluster -Head's Battery power;
If (Battery power < Threshold)
Cluster-Head sends aLIFE_DOWN message to all its Neighbors;
All the Member nodes participate in the Re-Election Procedure using Modified Weighted Clustering Algorithm and the Node with least weight is selected as the New Cluster-Head;
Else
Re-election is not needed;

When a new node enters our system it will broad cast beacon signal to all its neighbors. Then neighbor nodes will form a connection matrix based on the received signal. Then the newly entered node will calculate the weight based on the power, distance between neighbors, spreading degree and power consumption. If in the cluster head is already there this node will send cluster head to join in the cluster. Otherwise new node will form a new cluster and declare itself as a cluster head.

Thus cluster head selection made dynamic and increase the performance. When cluster head energy reduces it can be changed and new node is choosed. In dynamic clustering weighted clustering algorithm is used and mobility prediction is used for cluster maintenance. Mobility prediction reduces communication overhead. Spreading degree calculation and weight calculation formulae are used for calculation. Since we are using mobility prediction with weighted clustering that reduce bandwidth, power and increase stability of cluster.

3. SIMULATION CONSEQUENCE

3.1 Performance Analysis

TESLA has less scalability because the communication .In our existing system TAM cluster head is static. Even if energy is less cluster head is not changed. This reduces entire performance of system. Hence we are going for dynamic clustering. Dynamic clustering uses weighted clustering algorithm for cluster formation and mobility prediction for cluster maintenance.

Algorithm for newly arriving node 'U'

Action 1:
Node u will broadcast a beacon signal to all its neighbor nodes in the transmission range;
Process the signals received from the neighbor nodes in the network and form the connection matrix.

Action 2:
Calculate the Degree R (U) using Spreading degree, Δsp, Sum of the distances with all its neighbors, Average Speed, Amount of battery power that has been consumed, and Weight of node U.

degree, mobility, power consumption and distance of neighbours for calculating weight. Based on the weight cluster head is choose. Node with least weight is chosen as cluster head. If the energy of the cluster head reduces it sends message to all other nodes .Then again reclustering is chosen based on weight. Node removed from cluster head won't participate again. TAM uses time asymmetry for intra clustering. Here message is divided in to chunk's and they are sending in packet. MAC is attached to each packet and is valid only for specific time. If the packet is reached after that it is discarded. Inter clustering uses secret information asymmetry. Node will send information to all member of multicast group. That is will send to all cluster head of that group. The main advantage is MAC is associated with cluster than nodes. The performance of TAM with dynamic clustering is shown in graphs .The parameters used for measuring performance are node and rate. Node and rate are varied and performance is analyzed. The metrics used are delay, delay ratio and overhead. From the graph it is know that delay and overhead is and delay ratio is more for dynamic TAM than static with node and rate as parameter. In our proposed system mobility prediction with weighted clustering that reduces bandwidth, power and increase stability of cluster. The performance is shown with simulation result.

3.2 Simulation Model And Parameters

We use NS2 to simulate our proposed dynamic clustering for TAM t. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol.

No. of Nodes	100
Area Size	1500 X 300
Mac	802.11
Radio Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Mobility Model	Random Way Point
Speed	5m/s
Pause time	0,10,20,30 and 40 s
Rate	250Kb

Table 1: Simulation settings and parameters

TAM performance can be viewed simulation experiments pursued using NS2. TAM with dynamic clustering performance is better than static. The performance of TAM is compared with two parameters node and rate.

Figure 1 show that delay is less for TAM using dynamic clustering with varying node.
Figure 2 shows that delay ratio is greater for TAM using dynamic clustering with varying node.
Figure 3 shows that overhead is less for TAM using dynamic clustering with varying node
Figure 4 shows that delay is less for TAM using dynamic clustering with varying rate.
Figure 5 shows that delay ratio is greater for TAM using dynamic clustering with varying rate. Figure 6 shows that overhead is less for TAM using dynamic clustering with varying rate.

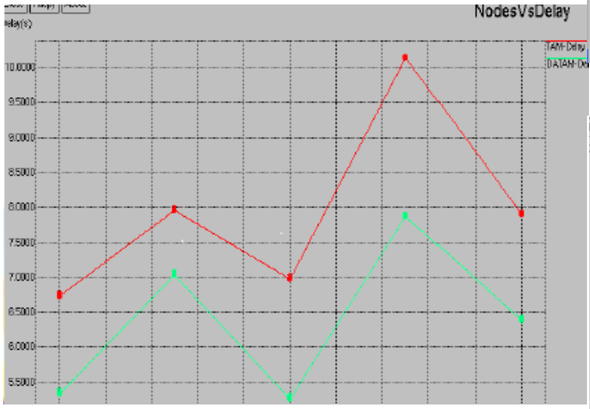

Fig 1 Node vs. Delay for TAM and Dynamic TAM

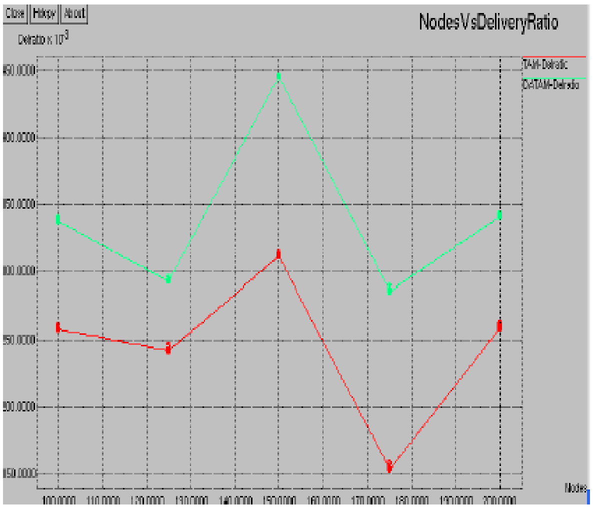

Fig 2 Node vs. Delay Ratio for TAM and Dynamic TAM

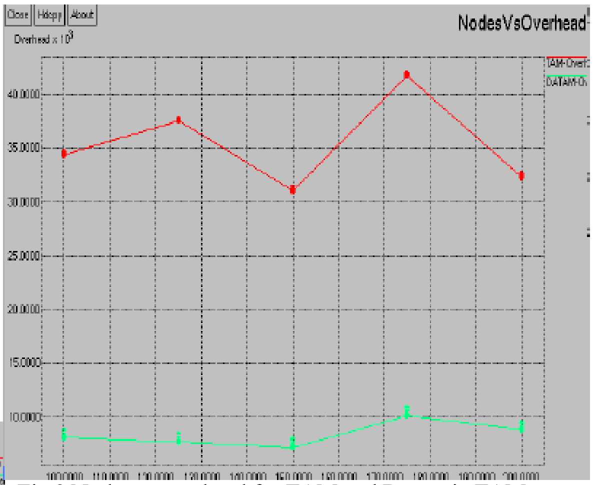

Fig 3 Node vs. overhead for TAM and Dynamic TAM

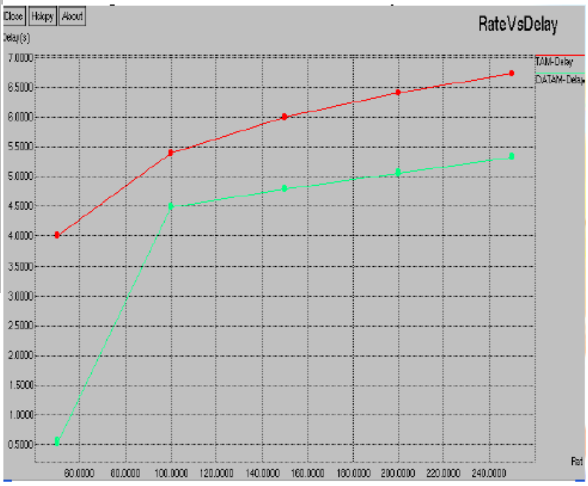

Fig 4 Rate vs. Delay for TAM and Dynamic TAM

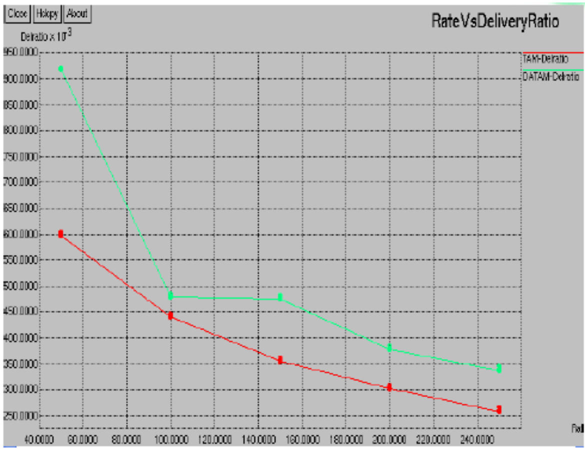

Fig 5 Rate vs. Delay Ratio with TAM and Dynamic TAM

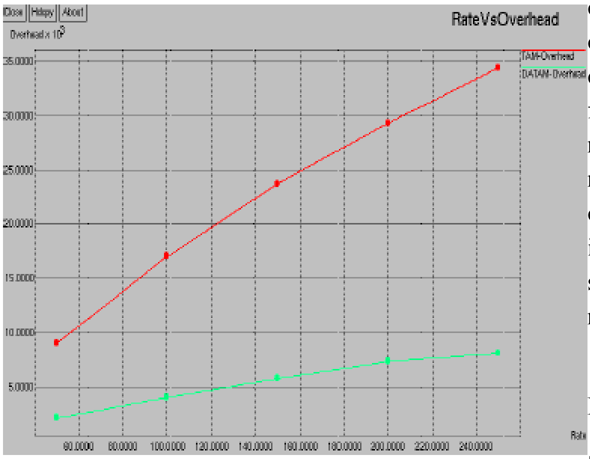

Fig 6 Rate vs. Overhead for TAM and Dynamic TAM

These graphs show the performance of our proposed system increases when using dynamic clustering. The graphs show that delay and overhead is highly reduced and delay ratio is comparatively higher for dynamic clustering algorithm in TAM than static.

4. DISCUSSION

In our paper dynamic clustering is used in TAM.TAM uses clustering to increase scalability. Intra clustering is based on time asymmetry. This is similar to TESLA. Inter clustering uses secret information asymmetry; hence clock synchronization is not needed. By using dynamic clustering it uses battery power and distance of neighbours to calculate weight. Based on the weight it will select the cluster head i.e. node with less weight is chosen as cluster head. If battery power of cluster head is less than a specified threshold then reclustering is done. Mobility predication in dynamic clustering reduces bandwidth for communication. Hence dynamic clustering with TAM can increase the performance.

5. CONCLUSION

TAM with inert clustering uses identical cluster head fully. Even if energy is less it is not change. In our proposed system we are overcoming this drawback. Based on mobility, spreading speed, power and distance of neighbor weight is calculated. Node with less weight is chosen as head. If the energy becomes less for cluster head then it will send a message to all neighbours. Then reclustering is done and then new cluster head is choosed. Dynamic clustering uses weighted clustering algorithm for calculating weight and choosing cluster head. It uses mobility prediction for cluster maintenance. Since we are using mobility prediction with weighted clustering that reduce bandwidth, power and increase stability of cluster. Our simulation results show the significant improvement in Performance. The performance is shown with node and rate as parameter. The metrics used are delay, delay ratio and overhead.

REFERENCES

[1] Mohamed Younis, Osama Farrag, Bryan Althouse," TAM: A Tiered Authentication of Multicast Protocol for Ad-Hoc Networks" IEEE Transactions on network and service management vol. 9, NO.1,March 2012.

[2] H. Yang, et al., "Security in mobile ad-hoc wireless networks: challenges and solutions," IEEE Wireless Commun. Mag., vol. 11, no. 1, pp. 1536–1284, Feb. 2004.

[3] Y. Challal, H. Bettahar, and A. Bouabdallah, "A taxonomy of multicast data origin authentication, issues and solutions," IEEE Commun. Surveys & Tutorials, vol. 6, no. 3, pp. 34–57, 2004.

[4] Perrig, et al., "Efficient and secure source authentication for multicast," in Proc. 2001 Network Distributed System Security Symposium.

[5] A. Perrig, R. Canetti, D. Song, and D. Tygar, "Efficient authentication and signing of multicast streams over lossy channels," in Proc. 2000 IEEE Symposium Security Privacy.

[6] Muthuramalingam, R.RajaRam, Kothai Pethaperumal and V.Karthiga Devi ”A Dynamic Clustering Algorithm for MANETs by modifying Weighted Clustering Algorithm with Mobility Prediction” International Journal of Computer and Electrical Engineering, Vol. 2, No. 4, August, 2010 1793-8163

[7] Puneet Sethi, Gautam Barua” Dynamic Cluster Management in Ad hoc Networks” Guwahati.

[8] D. Sivaganesan, R. Venkatesan ” Dynamic Cluster Routing Protocol for Broadcasting in Clustered Mobile Ad Hoc Networks” European Journal of Scientific Research ISSN 1450-216X Vol.73 No.1,2012, pp.111-118

[9] Dang Nguyen1, Pascale Minet2, Thomas Kunz3 and Louise Lamont “On the Selection of Cluster Heads in MANETs” IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 2, March 2011 ISSN (Online): 1694-0814.

[10]http://bangnew.blogspot.com/2009/04/message-authentication-code.html

[11]http://www.modainnovations.com/softwarepdf/java2012/A%20Tiered%20Authentication%20of%20Multicast%20Protocol%20for%20Ad-Hoc%20Networks.doc

[12]http://en.wikipedia.org/wiki/Cryptographic_hash_functin.

[13]S.Muthuramalingam, R.RajaRam, Kothai Pethaperumal and V.Karthiga Devi, "A Dynamic Clustering Algorithm for MANETs by modifying Weighted Clustering Algorithm with Mobility Predictions," International Journal of Computer and Electrical Engineering vol. 2, no. 4, pp. 709-714, 2010.

[14] Data Confidentiality in Mobile Ad hoc Networks by Hamza AldabbasPublisher: Arxiv.org Publication Date: Mar 8, 2012.

[15]Evaluation Of Certificate-Based Authentication In Mobile Ad Hoc Networks by Karthik Sadasivam T. Andrew Yang University of Houston-Clearlake Houston, TX, USA.

[16]IEEE Transactions On Network And Service Management, Vol. 9, No. 1, March 2012TAM: A Tiered Authentication ofMulticast Protocol for AdHoc NetworksMohamed Younis, *Senior Member, IEEE*, Osama Farrag, *Senior Member, IEEE*, and Bryan Althouse.

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

[18]http://balanagaraj.wordpress.com/2007/05/23/encryption-and-decryption-in-vbnet-2/

[19]http://www.ukessays.com/essays/computerscience/throughput-enhancement-using-cluster-based-approach-computer-science-essay.php.