Asian Journal of Information Technology 15 (5): 978-988, 2016
ISSN: 1682-3915

Secure and Energy Efficient Dynamic Clustering Scheme in Mobile Adhoc Networks

A.D. Khamala Khannen and Suthanthira Vanitha
Anna University, Chennai, Tamil Nadu, India

Abstract: In Mobile Adhoc network, the secure key management and energy efficient route discovery is difficult and challenging due to the nature of dynamic infrastructure less network. In this study we propose a new secure and energy efficient clustering scheme to form zone based secret key management clustering. This is used to provide secure communication in Adhoc networks with quality of service. The mobile nodes lose their maximum energy by discovering the efficient route to reach its destination. We propose an efficient mechanism for key update, key revocation schemes and key management for Mobile Adhoc networks using Mobile Adhoc Energy Efficient Secure Cluster scheme (MAEESC). The main objective of this study is to improve energy and reduce overhead in wireless network with secure manner.

Key words: Security, route discovery, secret key management scheme, Adhoc network, India

INTRODUCTION

Adhoc networks are decentralized wireless network. It does not rely on any preexisting infrastructure such as routers in wired network or access point in the wireless network which are having preexisting infrastructure. The Adhoc networks consist of mobile nodes that can communicate with each other without any preexisting infrastructure and continuously self-configuring is called as Mobile Adhoc network. The mobile node in MANET can move independently in any direction cause the mobile node changes the link between them frequently. The communication throughout the network is enabled by cooperative communication. The mobile nodes in MANET communicate the multihop fashion. So, each node in MANET should forward other node's information towards the destination which is called as forwarder node. The selection of best forwarder node in MANET is a challenging task because the link between the nodes changes dynamically. To solve this issue, many routing protocols have been proposed.

Since, the mobile nodes are having very limited energy and limited computation power, we need to provide the energy efficient routing protocol for MANET. The routing protocols are classified into three: proactive, reactive and hybrid routing protocol. Proactive routing protocols maintain constantly updated routing topology. An example of proactive routing protocol is DSDV (Perkins and Bhagwat, 1994). Reactive routing protocols are discovering the route only on demand by flooding Route Request packets to the whole network. An example is DSR (Broch *et al*., 1999). Hybrid routing protocols comprise the advantages of both proactive and reactive routing protocols. An example of hybrid routing protocols is ZRP (Haas and Pearlman, 1998). For MANETs we mostly prefer reactive routing protocols. If a node wants to communicate with another node which does not have any route, the reactive routing protocol discovers the route. The reactive routing protocols can provide best route for highly dynamic environment too. The main disadvantage of reactive routing is, it may take long time to find the route and it may leads to excessive flooding. So, now we are in the need to discover the best route with minimum energy consumption and minimum delay.

Security is the major concern in Mobile Adhoc networks where any node can join in the network and leave from the network without authentication. Key management is proposed by various schemes like certificate based cryptography and ID based cryptography. To achieve more efficiency and suitability ID-based systems are influential scheme than CA-based systems. As the MANET is an infrastructure less network, any node can act as router to forward the traffic to the intended destination. So, we need to provide the security to the routing path and we need to detect the misbehavior node present in the network. To solve these issues, this study proposes secure and energy efficient clustering scheme with efficient route discovery method.

Corresponding Author: A.D. Khamala Khannen, Anna University, Chennai, Tamil Nadu, India

The zone based clustering scheme is used to cluster the mobile nodes. The ID based secure key management scheme is used to provide the authentication among the mobile nodes. By this scheme, we can detect the misbehave nodes in the network. The energy efficient route discovery is enabled by limiting the route discovery area.

Literature review

Related work: In this study, we present some of the existing work on security scheme and efficient routing for Mobile Adhoc Networks. In our proposed scheme, we are going to use ID based public key system. Shamir (1985) was introduced the concept of ID based authentication scheme. In this scheme, the users use their identity as the public key for securing information. ID based scheme facilitates the secure communication between any two nodes without exchanging public key certificates and without keeping public key storage. This is enabled by private key generator which issues a private key to each user corresponding to the identity. But it has one major disadvantage that, if the private key of the private key generator is compromised, the entire system is compromised.

The solution for this private key compromise is provided by Boneh and Franklin (2001) by broadens the private key of the PKG by threshold cryptography. The centralized public key infrastructure or a centralized certification authority is not possible in MANET. This can be solved by distributing of signing key and threshold cryptography. But, if the threshold number of key shareholder has compromised, the security of the entire network has broken.

The MANET has another challenge (Shin and Kwon, 2007) to maintain the group key. The group key should be agreed by group of nodes for secure communication. The group key agreement enables group of users to communicate among themselves by consent on the common group key (Shin and Kwon, 2007). This leads to the communication over insecure channel.

Two mobile nodes in MANET establish secure communication by using session keys for pair-wise key agreement protocol which uses that session key for encrypting the information exchanged between them. McCullah and Barreto (2005) proposed a pairwise key agreement protocol using bilinear pairings. They provide the implicit key authentication, session key security, No key compromise impersonation and perfect forward secrecy in Adhoc networks.

A fully distributed threshold centralized authority scheme is proposed (Luo *et al*., 2004). In this scheme, all nodes act as servers and which enables share refreshing. The drawback of this scheme is that it does not provide verifiability (Narasimha *et al*., 2003) and it is vulnerable to Sybil attack (Douceur, 2002). Many ID based key management scheme has been proposed for MANETs. Khalili and Arbaugh (2003) has proposed an ID-based and threshold cryptography scheme. In this scheme, the private key of the Private Key Generator (PKG) is shared among the in set of threshold number of nodes.

The route discovery and the route maintenance are working together to permit the nodes to discover the source routes (Broch *et al*., 1999) to all other nodes in Adhoc networks. If a node wants to communicate with a particular destination node, it first checks its cache for whether the path to the destination is already known or not. If it is not known, the source node initiates the route discovery in the network. The route maintenance phase monitors the operation of the route and inform to the source node if any route failure occurs. If the routing protocol uses the position information of the mobile nodes to discover the route, it is called as position based routing protocol (Liao and Lin, 2007, 2008). The data packets are forwarded to the destination in two types: Greedy forwarding and directional forwarding. If the next hop node is closest to the destination in distance, then it is called greedy forwarding. In directional flooding (Ko and Vaidya, 1998) the source node send the data packet to the geographical area towards the direction of destination node. Location Aided Routing (LAR) (Camp *et al*., 2002) is the best example for directional forwarding.

METERIALS AND METHODS

This study presents our proposed scheme for secure and efficient communication in Mobile Adhoc networks. It consists of three phases. Zone based dynamic clustering; ID based secret key management scheme and efficient route discovery.

Zone based dynamic clustering: Grouping the mobile nodes in Adhoc network is a challenging task because of its dynamic nature. But clustering in Adhoc networks reduces the no. of hops for data transmission as well as communication overhead. Initially, the network area is equally divided into six zones. Each node has zone ID to identify in which zone the mobile node is currently available. The mobile node changes its zone ID when it is moving from one zone to another zone.

The cluster head is chosen by calculating the centroid point of each zone. The node which is very closer to the centroid point is cluster head. The cluster head node should have the capability to reach all its members. The cluster head broadcasts advertisement message to all other nodes having same zone ID. Subsequently other nodes in the same zone send the join request along with its ID to the cluster head. The cluster head adds its ID into the member table. Each and every mobile node maintains a neighbor table by broadcasting HELLO messages. All the nodes send the reply to HELLO message along with its position. The mobile node adds the position of each node for corresponding node ID. This neighbor table is very much helpful to discover the route.

ID based secret key management scheme: Secure communication in Mobile Adhoc Network is a challenging task as it is a dynamic and infrastructure less network. In this study, we are using ID based key management scheme for efficient secure communication in Adhoc networks. This scheme consists of four phases: key Initiation, key Exchange, Subshare verification, Key Updation and key revocation.

Key initiation: Fundamental execution of network where there is an offline Private Key Generation (PKG) center. It consists of initial setup and private key extraction.

The PKG select a random number, s $\in$ $_{Zp}$as its private key. Ppub = s×P0 is the PKG's public key. The PKG predefines the number of the key update phase index, ∪ and selects a set of generators, Pm(1≤m≤U) of G1, for the purposes of regular periodic key updates. The system parameters of PKG are as follows:

<p,q,G1,G2,P0,Ppub,Pm,H1,H2,H3>

Key extraction: The PKG generates prime numbers m_i for each cluster head which is distributed to every other CHs. PKG also computes public-private key pair: Qi=(mi+s)P0 and Si = $(mi+s)^{-1}$ P0. The PKG then preloads the key pair and system parameters onto CH_i (1≤i≤n), securely.

Key exchange: A pair-wise key agreement protocol allows two parties to establish their session keys and use the keys to encrypt the communications between them. In order to provide perfect forward secrecy, we modified the scheme presented by McCullagh and Barreto (2005) to generate our pair-wise keys as follows: each CH_i (1≤i≤n) randomly chooses its ephemeral key, xi $\in$ $_{Zp}$, computes Xi,j=xi (mjP0+Ppub). (1≤i,j≤n,i≠j) and sends Xi, j to Chj(1≤j≤n, I≠j). After exchanging the ephemeral values, all CHs can compute their pairwise keys: Ki,j = ^e(P0, P0)xi ^e(xj,i,Si)+^e(Xj,i,Si)xi = ^e(po, po) xi+xj+^e(po, po) xixj(1≤i,j≤n,i/=j) ki,j = H3(ki,j).

The above pair wise key agreement protocol satisfies the security properties (McCullagh and Barreto, 2005). Therefore, it can be securely employed in MANETs.

This method of key computation satisfies the security properties such as key authentication, No key compromise impersonation and perfect forward secrecy. So it ensures secure communication in Mobile Adhoc Networks.

Subshare verification: A Master secret D∈$_{Z}$m0 is jointly shared between the clusterheads by:

- Each CH chooses a secret di∈Zm0 and shares it by using the VSS scheme as follows: He first computes yi=di+Aim0 where yi<M= (i=1tmi)/n. Then, the secret for the jth user is computed as yj (i) =y (i) mod mj. He sends yj (i) to user j secretly for all 1=i=n and broadcasts Eyi, Rngprf (Eyi, M)
- After receiving shares the jth user verifies them by using, to prove :gjyj(i)=Eyi mod pj

If the above equation is valid then the received share is valid else the CH is considered as misbehaving.

Correctness: To prove, Ey mod pi = giyi mod pi Ey = gymod PN. Ey mod pi=gymod PN mod pi. = gymod pi = giyimod pi

Thus, the received share is considered as valid. Where P = i = 1npi and N is a RSA composite whose factorization is secret. Note that even if φ (P) is known, φ (PN) cannot be computed since φ (N) is secret. The RngPrf (E(y), M) denotes the range proof that a secret integer y committed with E(y) is in the interval [0, M).Let gi∈Zpi be an element of order mi. The dealer sends yi to the ith CH privately and makes the values pi, gi and zi=giymod pi public for 1 = I = n. The ith CH can find whether his share is valid or not by checking zi = giyimod pi.

Let B be the set of CHs whose shares are verified correctly. The jth CH computes his overall share yj=i∈. Byj(i) mod mj by using the verified shares.

Let S be a coalition of t Clusterheads gathered to construct the secret. The share yi of user i∈S can be verified by the other users in S with the verification equation:

gyi= j∈BEyj mod pi

If all shares are valid, the participants obtain the secret D by, Let MS denote i∈Smi and Let MS\{i}denote j∈S,j∈imj and MS,i'be the multiplicative inverse of MS\{i} in Zmi, i.e., MS\{i}MS,i'=1 mod mi. First, the ith CH computes ui=yiMS\{i}MS,i' mod MS. The CHs first compute y=i∈Sui mod MS and then obtain the master secret D by computing D=y mod m0=i∈Bdimod m0.

After the above distributed key generation steps have been performed, each CH holds a subshare, yj, of the master secret key, D and broadcasts public key yjpub=H2Ppubyj and the public key, D_{pub}, of the master secret key, can be generated from any t CHs' public keys yjpub Where Dpub=H2PpubD.

C.Key revocation: The key revocation scheme is comprised of three sub-processes: misbehavior notification, revocation generation and revocation verification (Liao and Lin, 2008; Blundo *et al*., 2004) .

Misbehavior notification: If CHi is found misbehaved, then CHj generates an accusation, IDi,TjKj,v against CH_i and securely transmits it to CHv , where $Tj_{??}$ is a time stamp used to withstand message replay attacks and Kj,v is the pair-wise key of and $Ch_{v1\le v\le n,\ v\neq i,\ j}$. To prevent CH_i from temporarily behaving normally (artificially), the accusation should not be sent to that node.

Revocation generation and revocation verification: As like in IMKM scheme (Liao and Lin, 2008), generation of a revocation requires the joint effort of t CHs. The D-PKG with the largest ID acts as the role of revocation leader. Each of the *t* unrevoked, having the smallest IDs, generates a partial revocation, REVj=H1IDiyj and sends it to the revocation leader securely using the pair-wise key. The revocation leader checks whether the equation H2PpubREVj=yjpub holds. If the partial revocation is not valid, the revocation leader considers CH_j to be misbehaving and issues a signed accusation against it.

The revocation leader can construct a complete revocation from these partials. as explained in the previous section. A complete revocation is derived as ID'=H1IDiD by using t CHs. The revocation leader then floods <IDi, IDi'> throughout the network to inform others that CH_i has been compromised.

Each cluster head verifies it by checking whether the equation H2PpubIDi'=H1IDiDpub holds. If the equation holds, the cluster head then records IDi in its Key Revocation List (KRL) and declines to interact with it thereafter.

Key joining: A new cluster head CHk can join the network from the following steps:

- After selecting a random prime number which is not currently used by any other CHs, a share dk∈Zm0 and computes yk = dk+Akm0. Then the secret for the j^{th} user is computed as yj(k) = y(k) mod mj. He sends yj(k) to user j secretly for all 1 = j = n
- After receiving the shares of CHk, each CHs will update their existing shares as yj' = yj+yj (k) mod mj

Key eviction: The key eviction is done after the revocation leader sends a signed message to all other unrevoked CHs. If CHkis to be revoked, then the share of CHk, each CHs will update their existing shares as yj'=yj-yj(k) mod mj.

By using the above distributed key management schemes, each CH can easily add or update its share key in a secure and efficient manner, thus greatly reducing communication and computation costs compared with the existing IMKM scheme.An efficient, one round Authenticated Group Key Agreement protocol (AGKA) for cluster-based MANETs, is used to derive the group session key as in the IMKM scheme. The key updates are done based on the value of Pmwhich changes after a predefined interval, so as to increase the security.

Efficient route discovery: If the destination node is available in the communication rage of the source node, then they can communicate directly. If not, the source node depends on some intermediate nodes to transmit the data to the destination. This kind of communication is called as cooperative communication. The source node discovers the route by broadcasting the Route request to all other nodes in the network. It will lead to routing overhead in the Adhoc network if it is a large network. The mobile node is resource limited because of its dynamic nature. So, it will consume more energy to discover the route among large scale network. To overcome this issue, we are limiting the area of discovery in the following manner:

- Initially, the network area is equally divided into zones
- In each and every zone, the cluster has formed and each cluster has its own cluster head
- If the member node needs to transmit the data to any other mobile node in the sense, it should send the data only via its cluster head
- The cluster head find the zone in which zone the destination is available by referring the position table. Then limit the area into request zone in the following manner

- The source node restricts the area where the RREQ packets are sent to find the route to reach the destination. The request zone is minimized by detaining it to the smallest rectangular area within hat the source and destination nodes are present

The source node broadcasts the RREQ message to the nodes present in the request zone only. Thus, the routing overhead is reduced as well as the time requires for discovering the route is also reduced.

RESULTS AND DISCUSSION

We conduct a series of experiments by varying the speed of the mobile nodes, varying the size of the packet to be transmitted and varying the data transmission interval. The nodes are distributed in the simulation area of 1500×1000m. The UDP/CBR (Constant Bit Rate) traffic is generated between the source and destination. The bandwidth for each channel is 2 Mb at initial time. After that it will be updated by using the dynamic bandwidth allocation algorithm. The data packets are scheduled after 0.05 ms. The detailed simulation parameters are listed in Table 1.

Table 1: Simulation perameters

Parameter type	Parameter value
Simulation time	20 ms
Simulation area	1500×1000m
Number of nodes	10,20,30…,100
Mobility Speed	10,20,30,40m ms^{-1}
Path loss model	Two ray ground
Channel bandwidth	2Mbps
MAC protocol	802.11
Transmission range	250m
Traffic model	CBR

The performance is evaluated by using the network parameter packet delivery ratio, packet loss ratio, end to end delay, routing overhead and throughput.

The packet delivery ratio is the ratio of the data packets delivered to the destination successfully. The packet delivery ratio is one of the important parameter to evaluate the quality of the network. The formula used to find the Packet delivery ratio is as follows:

PDR = No. of packets delivered/Time

Figure 1 gives the graph for Packet delivery ratio. It shows that the proposed scheme Dynamic relay node selection algorithm provides high performance when increasing the mobility speed too. But the performance slightly varies according to the node speed. Higher the packet delivery ratio indicates that the high performance of the network. The comparison analysis of packet delivery ratio of the proposed scheme while varying the size of the packet to be transmitted with the existing scheme IMKM is shown in Fig. 2. The packet delivery ratio while varying the interval between two packet transmission is obtained for both proposed and existing scheme and compared by using the graph as shown in Fig.3. The simulation results obtained prove that, the proposed scheme outperforms than the existing scheme IMKM (ID based multiple secret key management scheme).

The packet loss ratio is used to evaluate the quality of the network provided by the routing scheme. Fig. 3 shows the graph for Packet loss ratio of the proposed scheme in various simulation environment of different node speed.

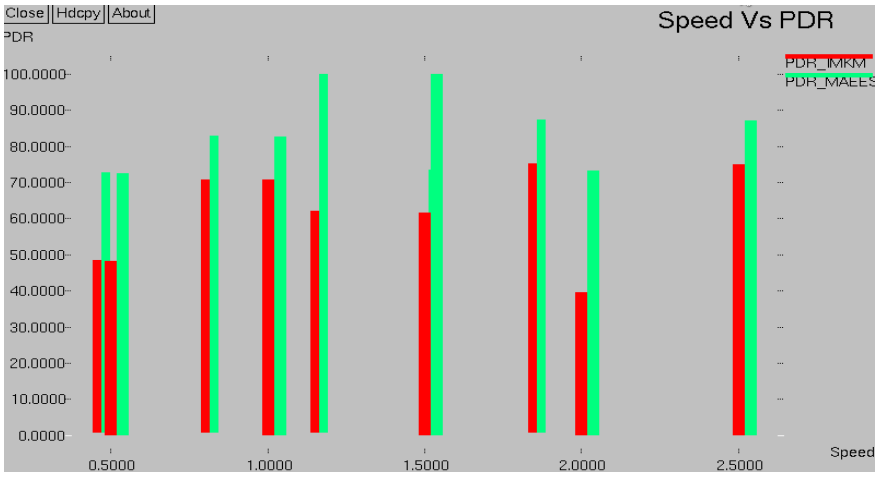

Fig.1: Packet delivery ratio analysis by varying node speed

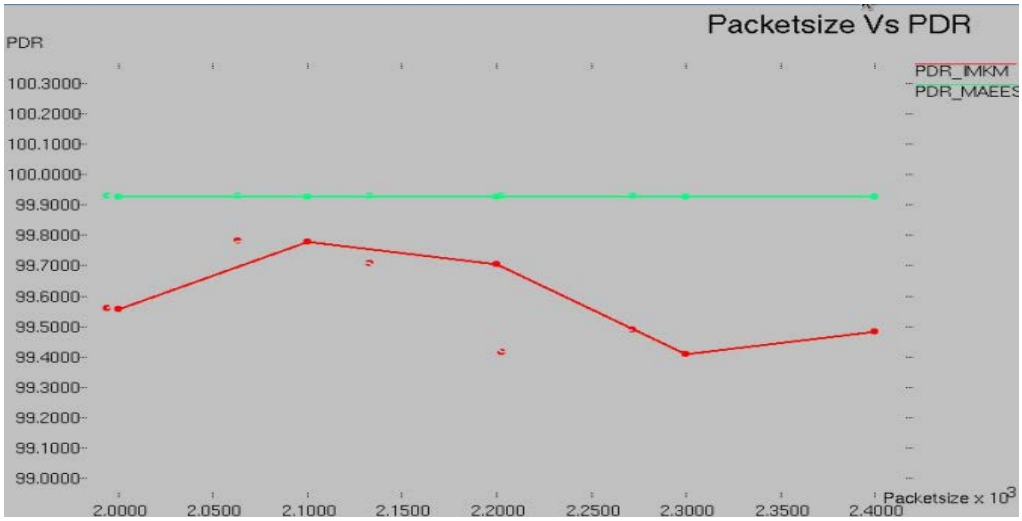

Fig. 2: Packet delivery ratio analysis by varying packet size

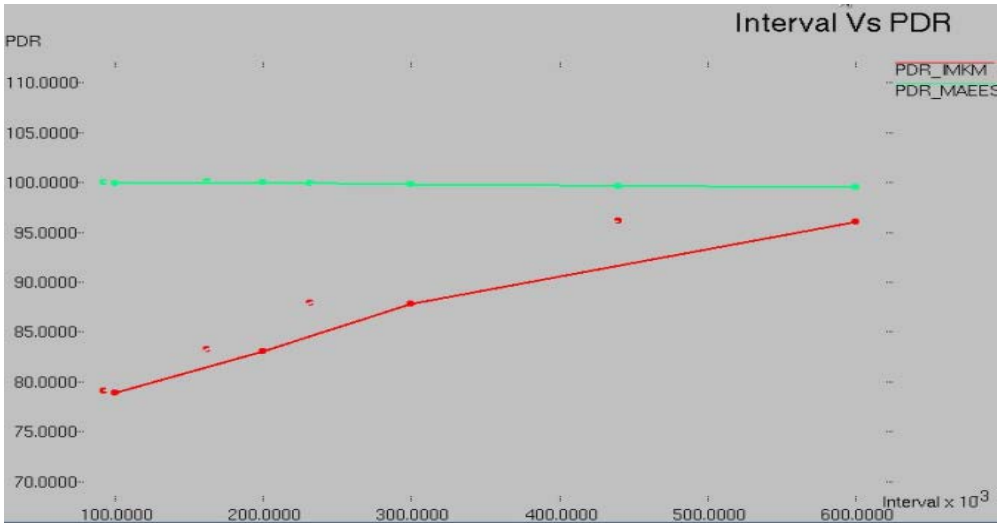

Fig. 3: Packet delivery ratio analysis by varying interval between two packet transmissions

The packet loss ratio of the proposed scheme is compared with the existing approach IMKM. The packet loss ratio of the proposed scheme is lower than the IMKM as shown in Fig. 4. Lower the Packet loss ratio indicates that the high performance of the network. The packet loss ratio of the proposed scheme is compared with the existing scheme IMKM is shown in Fig. 5 which can be obtained by varying the Packet size.

Figure 6 also shows the comparison analysis of the packet loss ratio obtained by varying the interval between two packet transmissions. By analyzing Fig. 4-6, the proposed scheme performs well than the existing scheme IMKM.

The time taken by the source node to deliver the data successfully to the destination is called as End to End delay. The following equation is used to calculate the end to end delay:

$$\text{End to end delay} = AT - STn$$

Where:

AT = Arrival Time
N = Number of connections
ST = Sent Time

Figure 7 shows that the end to end analysis of the proposed scheme. The delay increases as the mobility speed of the node increases. But, the slight variation is

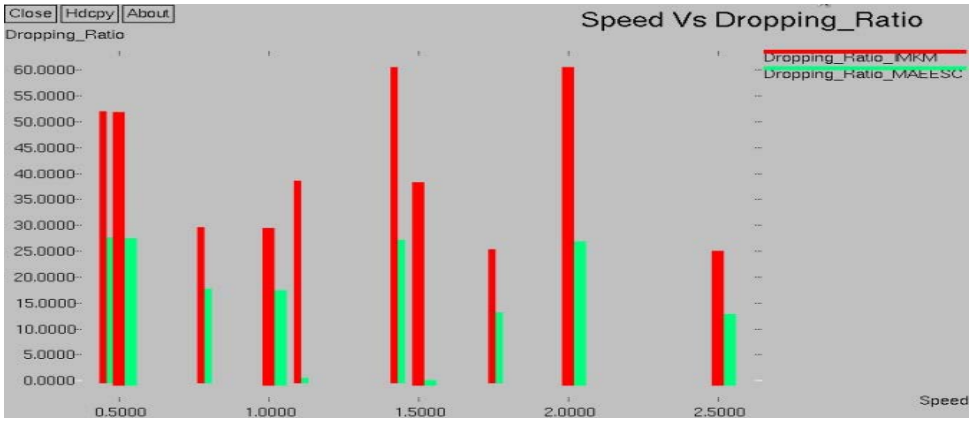

Fig. 4: Packet loss ratio analysis by varying speed of the nodes

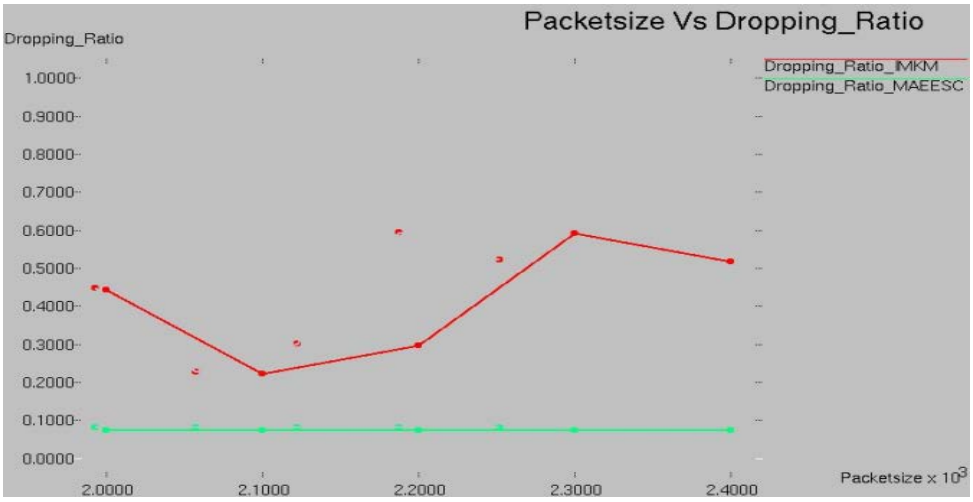

Fig. 5: Packet loss ratio analysis by varying packet size

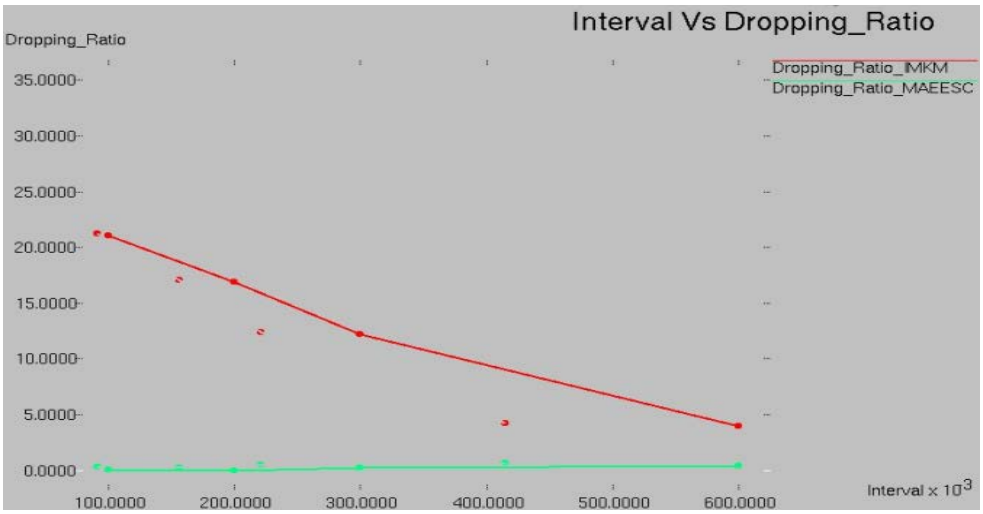

Fig. 6: Packet loss ratio analysis by varying interval between two packets

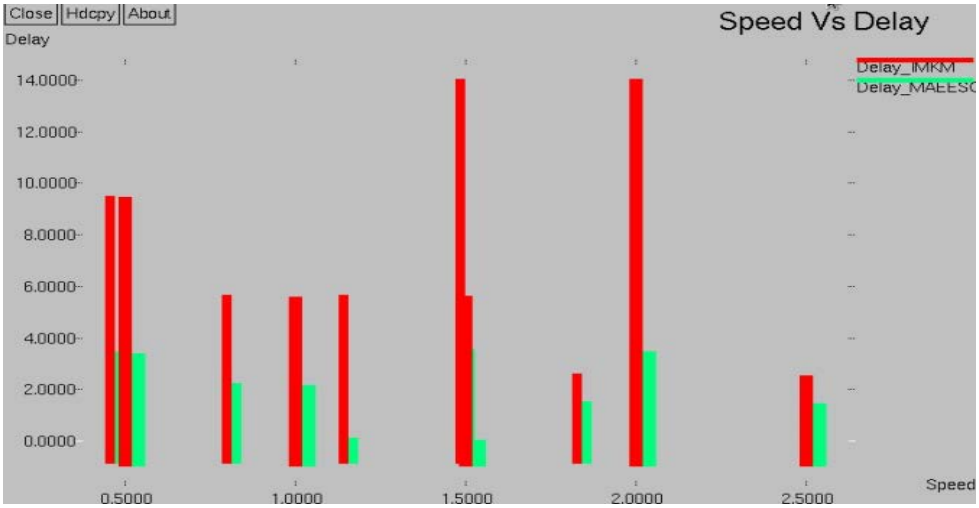

Fig. 7: End to end delay analysis by varying mobility speed

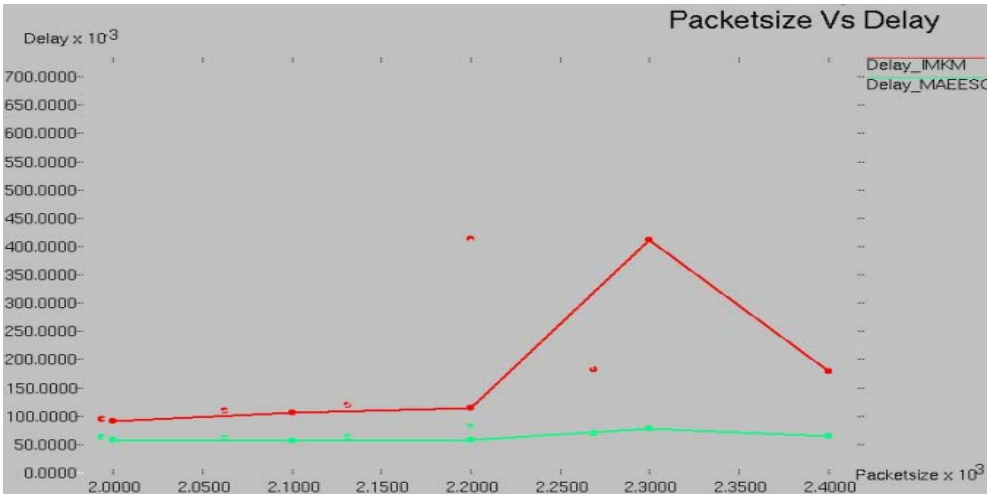

Fig. 8: End to end delay analysis by varying packet size

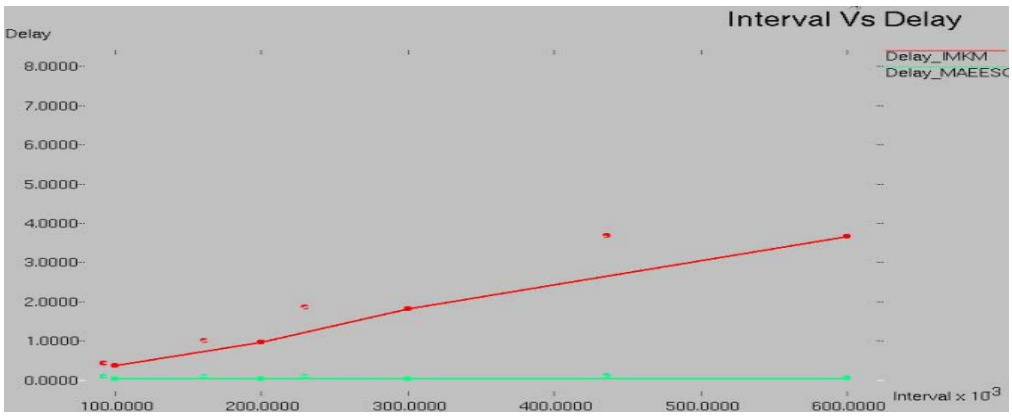

Fig. 9: End to end delay analysis by varying interval between two packets

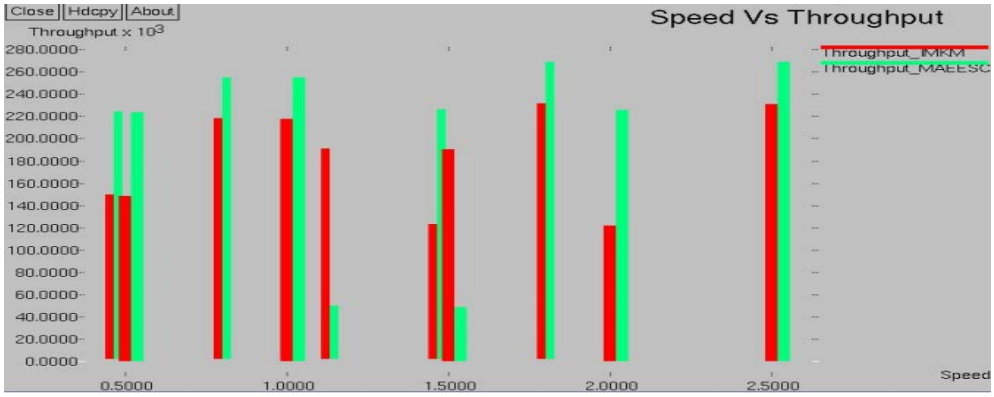

Fig. 10: Comparison analysis of throughput by varying node's mobility speed

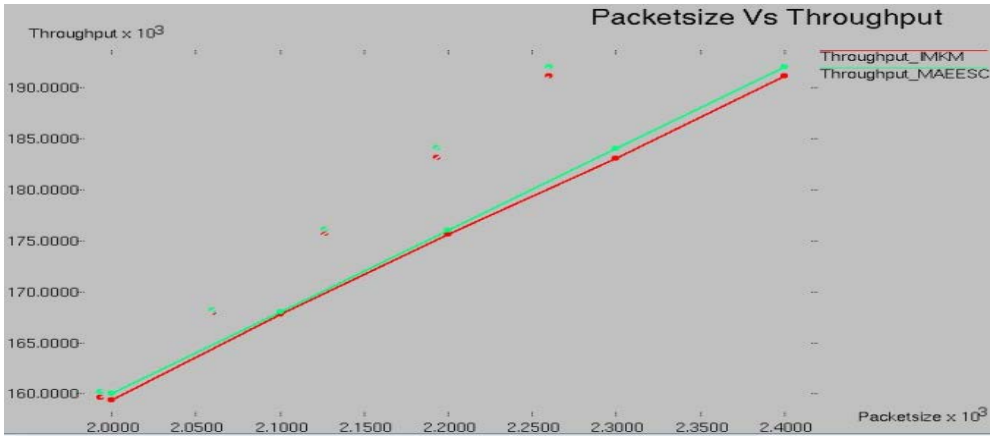

Fig. 11: Comparison analysis of throughput by varying packet size

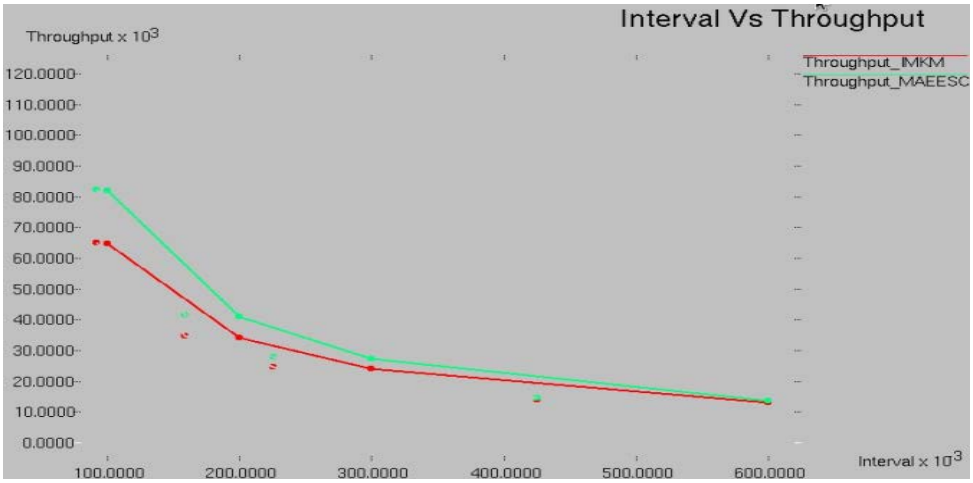

Fig. 12: Comparison analysis of throughput by varying interval between two packet transmissions

there. The proposed scheme leads to only tolerated delay in the network even though the speed increases. The delay for both proposed and existing scheme is obtained by varying packet size and interval between two packets. Figure 8 gives the comparison analysis of end to end delay by varying packet size. The comparison analysis of

delay obtained by varying the interval between two packets is shown in Fig. 9. Figure 9 show that the proposed scheme leads to less delay when compared with the existing approach IMKM in all scenarios.

Throughput is the amount of packets delivered to the destination per unit of time. The Throughput is calculated by using equation:

Throughput = No.of packets delivered/Time period

The system provides high throughput while the node is moving when compared with the node with high mobility speed as shown in Fig. 10. The throughput obtained by varying size of the packets to be transmitted is high when compared with the existing scheme IMKM as shown in Fig. 11. The comparative analysis of the proposed scheme with the existing approach IMKM of the throughput by varying interval between two packets is given by the graph shown in Fig. 12. As a result, the proposed secure and energy efficient route discovery scheme is able to guarantee QoS requirements in the Mobile Adhoc Network.

CONCLUSION

In this study, we have proposed a new scheme to enable secure and energy efficient communication among mobile nodes. The network area is divided into zones for grouping (cluster) the nodes. Each cluster has its own cluster head. The cluster head should have the capability to communicate with all other remaining nodes in its zone. The CH used ID based secret key management scheme to ensure secure communication. The misbehave nodes in the network is detected by verifying its sub share values. The energy consumption for route discovery is reduced by limiting the route discovery area. The route discovery message is only broadcast to the CH except misbehave nodes.

According to our simulation results, our proposed scheme improves the performance of the mobile ad hoc networks by providing secure and energy efficient communication among mobile nodes.

REFERENCES

Blundo, C., P. D'Arco, A. de Santis and M. Listo, 2004. Design of self-healing key distribution schemes. Des. Codes Cryptogr., 32: 15-44.

Boneh, D. and M.K. Franklin, 2001. Identity-based Encryption from the Weil Pairing. In: Advances in Cryptology, Kilian, J. (Ed.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-42456-7, pp: 213-229.

Broch, J., D.B. Johnson and D.A. Maltz, 1999. The dynamic source routing protocol for mobile ad hoc networks. Internet-Draft, draft-ietf-manet-dsr-03.txt, October 1999.

Camp, T., J. Boleng, B. Williams, L. Wilcox and W. Navidi, 2002. Performance Comparison of two location based routing protocols for ad hoc networks. Proceedings of the Infocom 21st Annual Joint Conference of the IEEE Computer and Communications Societies, 2002, IEEE Xplore, pp: 1678-1687.

Douceur, J.R., 2002. The Sybil attack. Proceedings of the 1st International Workshop on Peer-to-Peer Systems, March 7-8, 2002, Cambridge, MA., USA., pp: 251-260.

Haas, Z.J. and M.R. Pearlman, 1998. The performance of query control schemes for the zone routing protocol. Proceedings of the ACM SIGCOMM Conference on Applications, Technologies, Architectures and Protocols for Computer Communication, August 31-September 4, 1998, Vancouver, Canada, pp: 167-177.

Khalili, A., J. Katz and W.A. Arbaugh, 2003. Toward secure key distribution in truly ad-hoc networks. Proceedings of the Symposium on Applications and the Internet Workshops, January 27-31, 2003, Orlando, FL., USA., pp: 342-346.

Ko, Y.B. and N.H. Vaidya, 1998. Location-Aided Routing (LAR) in mobile ad hoc networks. Proceedings of the 4th ACM/IEEE International Conference on Mobile Computing and Networking, October 25-30, 1998, Dallas, Texas, USA., pp: 66-75.

Liao, H.C. and C.J. Lin, 2007. A WiMAX-based connectionless approach for high mobility MANET. Proceedings of the 9th International Conference on Advanced Communication Technology, February 12-14, 2007, Phoenix Park, Korea, pp: 479-483.

Liao, H.C. and C.J. Lin, 2008. A position-based connectionless routing algorithm for MANET and WiMAX under high mobility and various node densities. Inform. Technol. J., 7: 458-465.

Luo, H., J. Kong, Z. Petros, S. Lu and L. Zhang, 2004. URSA: Ubiquitous and robust access control for mobile ad hoc networks. IEEE/ACM Trans. Networking, 12: 1049-1063.

McCullagh, N. and P.S. Barreto, 2005. A new two-party identity-based authenticated key agreement. Proceedings of the Cryptographers' Track at the RSA Conference, February 14-18, 2005, San Francisco, CA., USA., pp: 262-274.

Narasimha, M., G. Tsudik and J.H. Yi, 2003. On the utility of distributed cryptography in P2P and MANETs: The case of membership control. Proceedings of 11th International Conference on Network Protocols, November 4-7, 2003, IEEE Computer Society Washington, DC, USA., pp: 336-345.

Perkins, C.E. and P. Bhagwat, 1994. Highly dynamic Destination Sequenced Distance-Vector routing (DSDV) for mobile computers. ACM SIGCOMM Comput. Commun. Rev., 24: 234-244.

Shamir, A., 1985. Identity-Based Cryptosystems and Signature Schemes. In: Advances in Cryptology, Blakley, G. and D. Chaum (Eds.). Springer, Berlin, Heidelberg, ISBN: 978-3-540-15658-1, pp: 47-53.

Shin, S. and T. Kwon, 2007. Efficient and secure key agreement for merging clusters in ad-hoc networking environments. IEICE Trans. Commun., E90-B: 1575-1583.