Trust based Cluster Computing in Ad hoc Network using Group Key Climbing and Chaining (GKC^2)

S.Vijayalakshmi
Dept. of MCA
Hindustan University
Padur

P.Annadurai
Dept. of MCA
KMPGCS
Pondicherry

ABSTRACT

Cluster computing in ad hoc network draws special attention among the research community as it mandates the usage of single bandwidth for many receivers associated with the group/cluster. Ad hoc network operational environment has incited the adoption of cluster computing as it innately assists its formation. Cluster computing in ad hoc network has undergone a paradigm shift in the deployment of community centric applications like multiparty video conferencing, multiplayer online video games, online software patch update and online auction etc. Clusters in ad hoc network collaborate with each other through trust based routing using group key GK. Cluster members in the group are in possession of three keys namely a private key for decryption, public key for encryption for one-one communication between the group members and the local group key (LGK) for corresponding with the group head and broadcasting the message to other peers. Group head handshakes with other group members using the established and recommended LGK. The global group key (G^{2}K) possessed by each group head aids in inter group communication for encrypting the group message and the LGK for decrypting the enciphered group message. The inter collaboration between the clusters necessitates strong association among the group keys namely LGK and G^{2}K triggering upscale/upward group communication through efficient group key climbing and chaining mechanism. The cluster key pool viz. the group key associated with the group head and the group member's key are established during the set up and connection phase that sustains until the clusters encounters one of these special conditions. Group head drifting from the cluster, a node joining/leaving to/from a cluster (forward and backward secrecy), compromised keys, and periodical key updates induces a rekey mechanism for the cluster. The storage, computation and communication complexity involved in key generation and exchange mechanism leverages trust based cluster routing in ad hoc network.

General Terms

Ad hoc Network, Cluster computing, Group Oriented Reconstructive strategy, Reclustering.

Keywords

Cluster based routing, Local Group key, Global group key, cluster head selection, Rekeying.

1. INTRODUCTION

A collection of wireless nodes that self-configure to form a network without the aid of any established infrastructure is called mobile Ad hoc network (MANET). They can be also defined as a collection of mobile nodes that intercommunicate on shared wireless channels. The nodes entering or leaving the network have routing capabilities which allow them to create multi hop paths connecting node which are not within radio range [1]. The characteristics of MANETs like no fixed network infrastructure, dynamic network configuration, mobility of nodes and frequent node failure, low battery power, etc differentiate them from other wireless networks.

The process of dividing the network into interconnected substructures is called clustering and the interconnected substructures are called clusters. The cluster head (CH) of each cluster act as a coordinator within the substructure. Each CH acts as a temporary base station within its zone or cluster. It also communicates with other CHs. The Cluster based routing provides an answer to address nodes heterogeneity, and to limit the amount of routing information that propagates inside the network [2]. Clustering is one of the techniques used to manage data exchange amongst interacting nodes. Each group of nodes has one or more elected Cluster head(s), where all Cluster heads are interconnected for forming a communication backbone to transmit data. Moreover, Cluster heads should be capable of sustaining communication with limited energy sources for longer period of time. Misbehaving nodes and cluster heads can drain energy rapidly and reduce the total life span of the network [3].

Clustering in Mobile Ad Hoc Networks (MANETs) has many advantages as routing efficiency, transmission management, information collection compared to the traditional networks. But the highly dynamic and unstable nature of MANETs makes it difficult for the cluster based routing protocols to divide a mobile network into clusters and determination of cluster heads for each cluster. The clustering technique adopts any one of the following clustering approaches like Location based, Neighbor based, Power Based, Artificial Intelligence Based, Mobility based and Weight Based [4]. Each approach advocates its own formation of clusters and cluster head selection for the smooth transit of messages across clusters. A hierarchical routing is possible by clustering in which paths are recorded between clusters instead of between nodes. It increases the routes lifetime, thus decreasing the amount of routing control overhead [5]. The cluster head coordinates the cluster activities inside the cluster. The ordinary nodes in cluster have direct access only to cluster head and gateways. Gateway nodes are those that are present in the overlapping zone of two clusters to facilitate the data transmission across clusters [6].

2. CLUSTER FORMATION IN AD HOC NETWORK

Cluster computing in ad hoc network evince special attention from the research community as little effort is directed towards the realization/manifestation of secure trustable computing/routing within the peer MANET nodes. The cluster head acting as a group arbitrator/coordinator for diverse group activities ought to win the confidence of other group members and other voted/elected cluster heads for its continued sustenance. The onus of authenticating the genuine, trustable group member within the group rests with CH. The selection of trustworthy network partners/nodes in cluster based computing promotes hassle free and fair routing within the cluster [7]. Cluster based computing optimizes the usage of network resources and protocol implementation by equalizing the bandwidth for one receiver to multiple receivers in a cluster.

The proposals introduced for the election of cluster heads in mobile ad -hoc networks include the Highest-Degree, the Lowest-Identifier, Distributed Clustering Algorithm, the Weighted Clustering Algorithm (WCA) [8].

1) Highest-Degree (HD) algorithm: It uses location information for cluster formation. It elects the cluster head from the highest degree node in a neighborhood.

2) The Lowest-Identifier algorithm: The node with the minimum identifier (ID) is elected as a cluster head. This causes battery drainage resulting in short lifetime span of the system.

3) The Distributed Clustering Algorithm: It is a modified version of the Lowest-Identifier algorithm. Each cluster selects its cluster head from its neighboring nodes having the lowest ID. In this algorithm every node can determine its cluster and only one cluster, and transmits only one message.

4) Weighted Cluster Algorithm: It employs combined metrics-based clustering. In order to calculate a weight factor Wv for every node v a number of metrics, including node degree, CH serving time and moving speed, are taken into consideration. As a result, WCA has increased number of overheads. The cluster set-up procedure is invoked, when a node moves to a region which is not covered by the clusterhead, throughout the whole system.

2.1 Advantages of Clustering

Clustering in Ad Hoc networks has many advantages compared to the traditional networks. They are as follows: 1) It allows the better performance of the protocol for the Medium Access Control (MAC) layer by improving the spatial reuse, throughput, scalability and power consumption.
2) It helps to improve routing at the network layer by reducing the size of the routing tables.
3) It decreases transmission overhead by updating the routing tables after topological changes occur.
4) It helps to aggregate topology information as the nodes of a cluster are smaller when compared to the nodes of entire network. Here each node stores only a fraction of the total network routing information.
5) It saves energy and communication bandwidth in ad-hoc networks [9].

3. SECURITY CHALLENGES/ISSUES OF CLUSTER COMMUNICATION IN AD HOC NETWORK

The highly dynamic and unstable nature of MANET's makes it difficult for the Cluster based routing protocol to divide a mobile network into clusters and determination of cluster heads for each cluster. Clustering reduces communication and control overheads due to pre determined paths of communication through cluster heads. It is vital for scalability of media access protocols, routing protocols and the security infrastructure. Routing protocols which considers only bidirectional links may have link asymmetry due inefficient or abnormal routing. Untapped network capacity is represented by the undiscovered unidirectional links, which reduces the network connectivity. A large number of mobile terminals are managed by a MANET using a cluster topology. The construction and maintenance of a cluster structure requires additional cost compared with a topology control without cluster. Clustering has some side effects and drawbacks [10].

1) The maintenance cost for a large and dynamic mobile network requires explicit message exchange between mobile node pairs. As the network topology changes quickly and concerns many mobile nodes, the number of information message exchange grows to reach a critical point. This information exchange consumes a lot of network bandwidth and energy in mobile nodes.

2) A ripple effect of re-clustering occurs if any local events take place like the movement or the death of a mobile node, as a result it may lead to the re-election of a new cluster-head. When a new cluster-head is re-elected it may cause re-elections in the whole of the cluster structure. Thus, the performance of upper-layer protocols is affected by the ripple effect of re-clustering.

3) One of the major drawbacks of clustering in MANETs is that some nodes consume more power when compared to others nodes of the same cluster. As special node like a cluster-head or a cluster-gateway manage and forward all messages of the local cluster leading to their power consumption being higher compared to ordinary nodes. It may cause untimely shutdown of nodes [11].

4. TRUST BASED CLUSTER COMPUTING IN AD HOC NETWORK

Cluster members in the group are in possession of three keys namely a private key for decryption, public key for encryption for one-one communication between the group members and the local group key (LGK) for corresponding with the group head and broadcasting the message to other peers. Established and Recommended LGK assist in handshaking between the Group head and the group members. The global group key (G^2K) possessed by each group head aids in inter group communication for encrypting the group message and the LGK for decrypting the enciphered group message.

Cluster computing in ad hoc network signifies the signaling of constrained free communication through cluster head. The cluster head meticulously plans the routing as to only the required number of data packets will be replicated on demand, based on the number of receivers in the cluster. The cluster head possessing the LGK a shared secret session key enables the intra cluster broadcast communication (ICBC) to all the cluster members. The possession of LGK by cluster head permits the cluster member to participate in inter group communication by forwarding encrypted data to CH which in turn transcends across other higher level clusters. The private and public key available with the cluster members promotes the intra group communication by encrypting the data with the receiver's public key and deciphering using the receiver's private key. The public key of each member is registered in cluster head along with LGK and Global Group Key (G^2K). The LGK is for downward group communication and G^2K is for upward group communication. Each cluster member has a key pool consisting of its own private key, public key to facilitate communication between the cluster members and Local group key for governing ICBC.

The CH equipped with keys like LGK, G^2K, the member's Public key for facilitating the interaction between CH to group member. The handshaking between the two cluster heads CH1 and CH2 is promoted by the two keys namely LGK a private key and G^2K a public key. CH1 wishing to send a message to CH2 will encrypt the message using the recipient's public key and transmit to the specific/concerned cluster which uses the private key for decryption that aids in inter cluster member interaction (ICMI). The challenge-Response system is employed to exchange the G^2K between the cluster head for inter cluster interaction. The intermediate cluster present en route to the destination will participate in the global group key chaining and climbing mechanism by contributing/sharing its key pool for end to end communication. CH1 has keys namely $LGK_1$and G^2K_1. CH2 has keys LGK_2 and $G2K_2$.

A node say N1 in cluster C1 with CH1 as the cluster head generates a message that has to be received by the Node N2 in cluster C2 with CH2 as the cluster head. Clusters C1 and C2 satisfying the in range requirements evades the role of intermediate cluster. The message from N1 will be digitally signed using its own group key G^2K_1 and encrypted using the recipients global group key G^2K_2. The LGK_1 enables the message to be delivered to the cluster head where the digital signing is facilitated. The destination cluster on receipt of the encrypted message will decrypt using the local group key LGK_2 and forward the same to the intended node/cluster member using its public key registered in the cluster head. The role of an intermediate cluster is required in case of the two clusters falling out of transmission range. The message generated by the cluster C1 reaches the destination cluster C2 spanning through several intermediate clusters (IC). The message is digitally signed by the collective global group keys of the clusters present in the forwarding route. On receipt of the encrypted digitally signed message the destination cluster decrypts the message using the local group key LGK_2 and bears the onus of forwarding the data to the cluster member in C2.

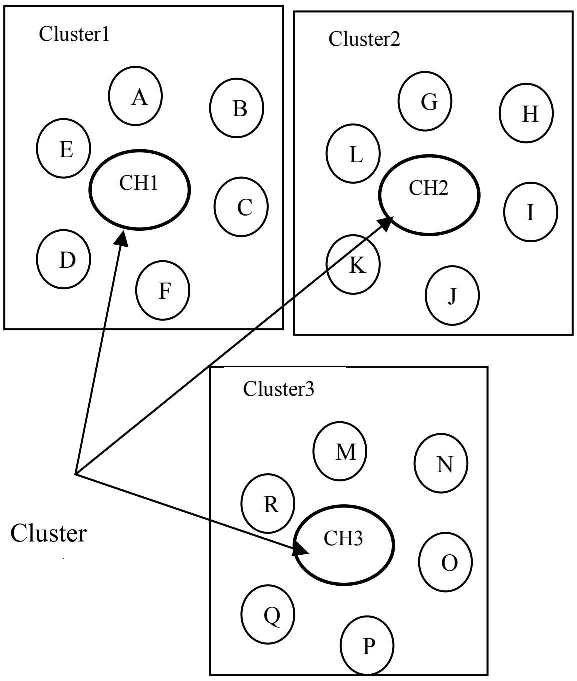


Fig 1: Cluster Formation in Adhoc Network

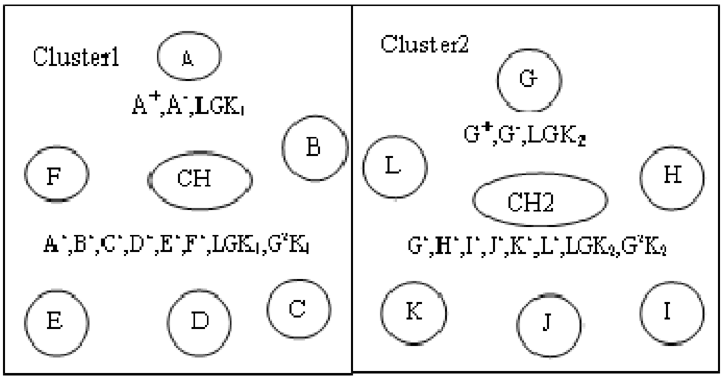

Cluster1
A
A^+,A^-,LGK_1
B
F
CH
$A^-,B^-,C^-,D^-,E^-,F^-,LGK_1,G^2K_1$
E
D
C
Cluster2
G
G^+,G^-,LGK_2
L
H
CH2
$G^-,H^-,I^-,J^-,K^-,L^-,LGK_2,G^2K_2$
K
J
I

Fig 2: Key Pool Maintained by each cluster member and its cluster head

Table 1: Notations used

Notation/Symbol	Meaning
CHI & CH2	Cluster head 1 and 2
A^+,A^-	Public, private key pair of each cluster member
LGK_1	Local Group Key for cluster 1
G^2K_1	Global Group key for cluster 1
LGK_2	Local Group Key for cluster 2
G^2K_2	Global Group key for cluster 2
m	Message to be sent across cluster members present in different clusters.

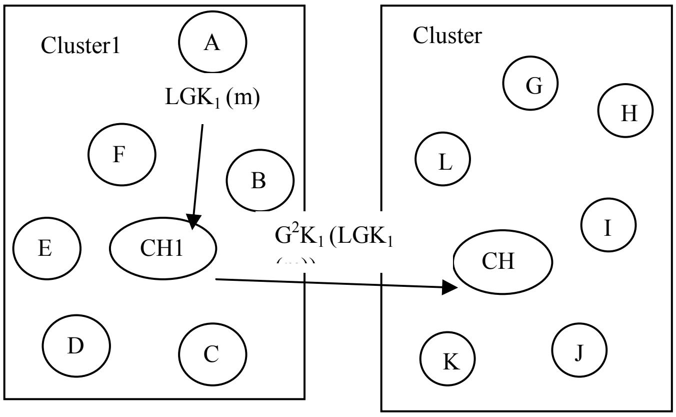


Fig 3: Digital Signing of Message Directed to the Destination Cluster

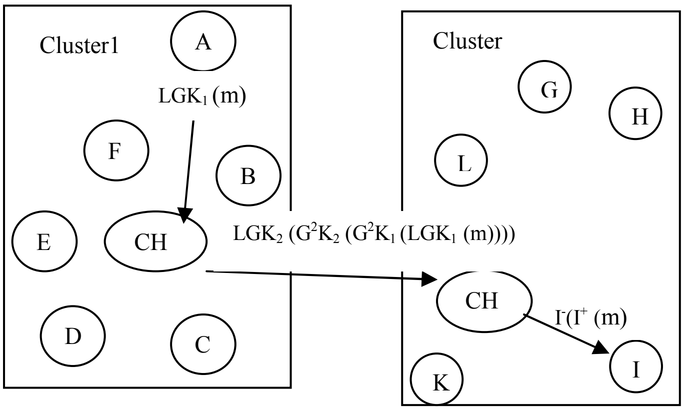


Fig 4: Decryption of Message by the Recipient Cluster hosting the specific cluster member

5. RESULTS AND DISCUSSIONS

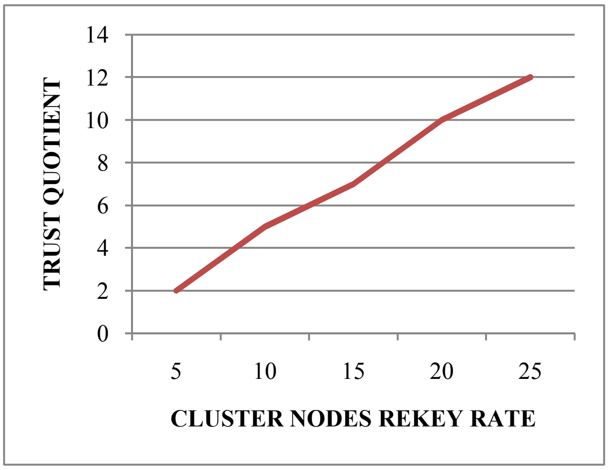
Rekey operation can be performed in any of the following cases/situations that occur. The cluster head being compromised by a security breach incident, the cluster members/head being drifted away from the vicinity, the periodic update and refreshments of the group keys, a node joining/leaving the cluster are the events that necessitates rekey operation to witness re clustering through cluster oriented reconstructive and rehabilitative strategy to preserve the privacy and secrecy of the cluster. The delay encountered in distributing the renewed/refreshed group keys to the group members is attributed to the group key exchange and propagation latency time.

The trust quotient tagged with the cluster head is likely to vary/change in diverse scenarios stemming from rekey operation. This metric is very critical in determining the cluster fidelity to sustain and support safe, secure cluster communication. The re clustering approach would obviously inflate the trust quotient metric associated with new cluster head as the follow up activities are validated by the new group keys. The delay incurred in this group key creation and exchange will not be compensated thereby culminating to an increased key propagation and exchange latency time.

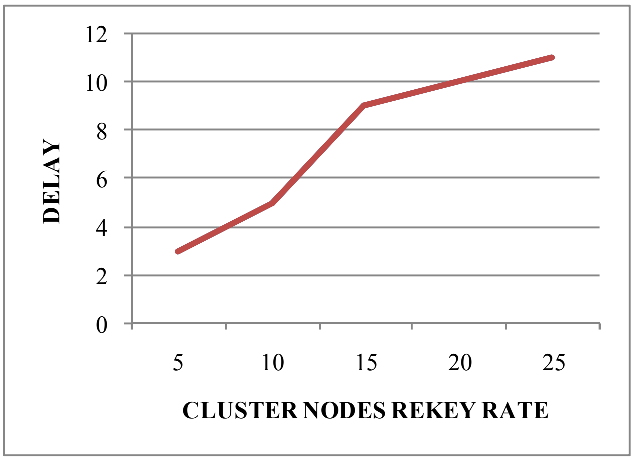
The rekey operations are scheduled in such a way to minimize the latency time associated with it to guarantee a faster and easier communication among the clusters. The time lag involved in rekeying operation would entail increased propagation time from the source cluster member to the destination cluster member. The cluster member's stability and robust cluster dynamics would significantly boost the trust quotient. The pace at which the cluster head hands off from the original network triggers the rekeying action that affects the trust ability metric.

End to end delay analyzed for various cluster scenarios/sizes signals the fact that it is inflated for the network organized into clusters rather than non cluster approach except during the rekey operation. This method is also helpful in analyzing the trustworthiness of the intermediate clusters (Relay Cluster) used in routing the cluster message from the source to the destination. The more the participation of RC in route discovery phase categorizes the specific cluster as the reliable and trustable with substantial trust ability metric.

Graph1 depicts the steady increase in trust quotient metric associated with cluster head in managing the cluster effectively in times of rekey and re cluster formation. Graph 2 portrays the inflation in delay factor stemming from the fresh group key creation and exchange latency time associated with cluster reorientation and reconstructive strategy.



Graph 1: Effect of Cluster Nodes Rekey Rate on Trust Quotient



Graph 2: Effect of Cluster Nodes Rekey Rate on Delay

6. PERFORMANCE EVALUATION AND ANALYSIS

Cluster dynamics: The mobile nodes are susceptible to large scale movements thereby rupturing the topology often and necessitating frequent hand offs and handovers. This culminates to a network scenario/behavior where rekey operations are frequently invoked and initiated due to dynamicity in topology.

Forward secrecy: The outgoing cluster member is prohibited from participating in future or forward communication between the cluster members and cluster head. The cluster head also may wish to quit the cluster either through soft or hard state leave. The soft state leave allows its cluster members to become a part of existing cluster through negotiations with the new cluster head. The hard state leave strands its cluster members without getting annexed to any of the existing clusters.

Backward secrecy: The incoming fresh cluster member should not have access to the past communication exchanged between cluster members and head.

Intra cluster and Inter cluster communication: The cluster members and the head present within the cluster facilitate the transmission of message between the clusters and within the cluster through efficient group key chaining and exchange mechanism.

7. CONCLUSION

Ad hoc network a purpose driven network contains mobile nodes that connect with other nodes present within the transmission range through multi hop mechanism. Each node in ad hoc network acts as relay node to establish far flung path to the remote nodes. The cluster formation in ad hoc network is a meticulous technique to manage the data movement efficiently and increase the route lifetime. Clustering in Mobile Ad Hoc Networks (MANETs) has many advantages as routing efficiency, transmission management, information collection compared to the traditional networks. The intra and inter cluster communication is facilitated by the use of two keys namely LGK and G^{2}K that aids in seamless interaction and transmission. The message from one cluster may reach the other clusters through efficient wrapping by the recipient cluster group keys that is delivered to the intended cluster where the packets are subjected to unwrapping. The group keys sharing and exchange between the cluster heads considerably inflates the computational, storage and communication complexity that leverages the safe and secure communication between the clusters.

8. REFERENCES

[1] V.Varadharajan, R.Shankaran and M.Hitchens, “Security for cluster based ad hoc Networks”, Elsevier Computerscience.com, Computer communications, October 2003.

[2] Anupama, M., and Sathyanarayana, B., “Survey of Cluster Based Routing Protocols in Mobile Ad hoc Networks”, International Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011

[3] Renuka, A.T., and Shetty, K.C., “Cluster Based Group Key Management in Mobile Ad hoc Networks”, International Journal of Computer Science and Network Security, VOL.9 No.4, April 2009

[4] Venkataramanan, V., Shankar, K., Vinoth, D., Archana, S., “Analysis of Cluster Based Zone Routing Protocol in MANET through Network Simulator” International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013

[5] Bheemalingaiah, M., Naidu, M.M., Rao, D.S., “Energy Aware Clustered Based Multipath Routing in Mobile Ad Hoc Networks”, *I. J.* Communications, Network and System Sciences, 2009, pp. 91-168 Published Online May 2009 in SciRes (http://www.SciRP.org/journal/ijcns/).

[6] Gupta, N., Shrivastava, M., Singh, A., “Greedy Cluster Head Selection Based Routing Protocol for Mobile Ad Hoc Networks” , International Conference on Electrical Engineering and Computer Science Engineering (ICEECS) 16th Sept, 2012, Pune- ISBN: 978-93-82208-18-1

[7] Ferdous, R., Muthukkumarasamy, V., Sithirasenan, E. , “Trust-Based Cluster Head Selection Algorithm for Mobile Ad Hoc Networks” IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), during 16-18 Nov 2011, pp. 589 - 596

[8] Gazdar, T., Benslimane, A. , Belghith, A. , "Secure Clustering Scheme Based Keys Management in VANETs" Vehicular Technology Conference (VTC Spring), 2011 IEEE 73rd during 15-18 May 2011, pp.1-5

[9] Rachedi, A., Benslimane, A. , "Trust and Mobility-based Clustering Algorithm for Secure Mobile Ad Hoc Networks", International Conference on Systems and Networks Communications, 2006. ICSNC '06. Pp.72.

[10] Elhdhili, M.E., Kamoun, B.F., "Reputation based clustering algorithm for security management in ad hoc networks with liars Third International Conference on Risks and Security of Internet and Systems, 2008. CRiSIS '08. During 28-30 Oct. 2008 pp.141-148

[11] Narasimha**,** C., and Jalaja Kumari, B.,*"* Efficient and Secured Multicasting Over MANET's through EGMP", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 5, May 2012 ISSN: 2277 128X, pp. 169-172.