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

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 (G2K) 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 G2K 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
Trust based Cluster Computing in Ad hoc Network using Group Key Climbing and Chaining (GKC^2)

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.

References

- 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
- Narasimha, C. , and Jalaja Kumari, B. , "Efficient and Secured Multicasting Over

Index Terms

Computer Science

Wireless

Keywords

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