ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

# Design of Hybrid Multicasting Network for Authentication

R.Vidhyalakshmi[1], P.Sankardayal[2], G.Sankareeswari[3]

Assistant professor, Department of IT, Sri Vidya College of Engg & Tech, Tamilnadu, India[1]

PG scholar, Department of CSE, P.S.R. Engineering College, Tamilnadu, India[2]

Assistant professor, Department of CSE, Sri Vidya College of Engg & Tech, Tamilnadu, India[3]

**ABSTRACT---**Wireless Ad Hoc Network is a collection of wireless hosts that can be rapidly deployed as a multi hop packet radio network without the aid of any established infrastructure or centralized organization. The cost reduction and fast progress experienced by wireless communication technologies have made them suitable for a wide spectrum of applications; one of edging is multicasting Networks. Multicasting system aim at on condition that a platform for various applications that can improve safety and efficient group of announcement. This proposed asynchronous key verification technique as a part of the protocol poses a significant diminution in the communication holdup.

**KEYWORDS---**Ad Hoc, Cluster, Network Security, Public key cryptography, Hash function

## I. INTRODUCTION

### A. Definition

Ad Hoc is defined as "Arranged or incident when necessary and not planned in advanced" according to oxfords advanced learner lexicon. This gives an elucidation of what ad hoc networks are is to say networks set up on the fly for a special purpose. Moreover ad hoc networks are typically such networks that are set up for one time occurrences such as conferences or military operations. This can be paraphrased into the following definition an ad hoc network is a flexible and adaptive network with no fixed communications

### B. Application

Ad hoc network has many applications two of them are already mentioned is to say crisis management and martial operations. Another application is Bluetooth which is designed for personal use and enables printers, scanners, mobile phones and composition players to be connected wireless to a personal area network this creates a tremendous flexibility because it enables devices to move freely between different networks. Ad hoc networks can also be used in the multi player sport one can visualize a game played from a device that can establish communication with other nearby devices, and these devices can then establish a cluster of interconnected devices and use this as a platform for playing the game. There are many implementations of ad hoc networks one of them is today's laptops prepared with 802.11 wireless PCI cards, they establish an ad hoc network, if the ad hoc manner is activated. This is particularly useful for business meetings in places where no current infrastructure is available say for example on an ad hoc conference in for example a eatery. If those enchanting part wishes to share data such as reports, diagrams and statistics they can activate their ad hoc mode and effortlessly transmit the data. This has proven extremely useful and completely eliminates the need for cable and routers.

C. Network Security

Network security consists of the provisions and policies adopted by a network superintendent to prevent and observe unconstitutional access, exploitation, modification, or denial of a computer network and network-accessible possessions. Network security involves the endorsement of access to data in a network, which is controlled by the network bureaucrat. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a diversity of computer networks, both public and secret, that are used in on a daily basis jobs conducting transactions and transportation among businesses, government agencies and folks.

D. Cluster

Cluster is an anthology of nodes. Clustering is a popular architectural apparatus for enabling scalability of network management functions. It has been exposed that clustered network topologies superior support routing of multicast traffic and the recital gain dominates the overhead of creating and maintaining the clusters .Each cluster is proscribed by a cluster-head, which is accessible to all nodes in its cluster, either directly or in excess of multi-hop paths.

Clustering, based either on the simple archetype of intra-cluster density versus inter-cluster sparsity or on other more complicated formulations.

E . Public Key Cryptography

The Public key cryptography is used two key i. Public key ii. Private key.

Public Key: Here public key is defined as node id for each node.

Private Key: Here private key is nothing but a node key value.

F. Hash Key

Hash Key is generated for each node, each node has been public key, private key, Common Key. Combination of Private key and common key produces the hash key.

G.Hash Key Generation Properties

The hash key generation has the following properties:

All hash keys are calculated using the some CRC checksum algorithm.

- Hash keys can be calculated to identify the unidirectional flows. In this case a flow from node A to node B and a flow from node B to A will generate different hash key values.
- Hash keys can be calculated to identify bidirectional flows. In this case a flow from node A to B and a flow from node B to A will generate the same hash key values. This method provides the best security,performance, third person or unauthorized user does not hack the original key value. Here hash key is acts as a shared key or single for all nodes.

## II. PROPOSED WORK

A. Objective

Asynchronous authentication scheme as using shared key management is proposed to resolve the most conflicting security requirements such as group authentication and conditional privacy .The proposed hash verification scheme as a part of the protocol poses a significant reduction in the message delay, then we use shared key process so requirement of the storage management is very less.

B. Advantage:

- It follows a two tired hierarchical policy combining both time and secret transaction asymmetry in order to achieve scalability and resource efficiency.
- It reduces delay on data transferring and get high throughput percentage.

## III. IMPLEMENTATION

A. Architectural model

Ad hoc network topology is formed with the help of various nodes creation. Clusters are formed based on the location and their connectivity with other nodes. Each cluster is controlled by the cluster heads from them only messages are passed to another cluster. Source nodes are in connection with cluster heads.

`

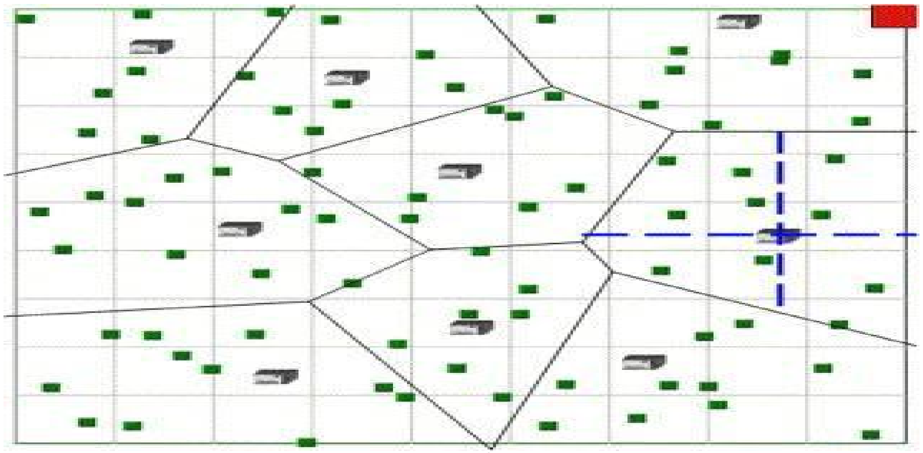


Fig. 1. Cluster formation

B. Key Establishment

Proposed system use RSA based key generation, and then use of hashing technique for memory optimization. Create one pair wise key and one shared key.

Pair wise key means,

- A public-key, which may be known by anybody, can be used to encrypt messages, then verify signatures
- A private-key, known only to the recipient and used to decrypt messages and sign (create) signatures.

Hash Key is generated for each node, each node has been public key, private key, CommonKey. Combination of Private key and common key produces the hash key.

C. Group Key management

Nodes get keys dynamically in the key distribution phase and then start to broadcast their geographic based. All nodes getting keys from the same leader form a group, as illustrated in the communication range is 300 meter. The key was asymmetric based group key method in both Leader and member have a common key for sharing.

D. Collective Key management

Leader get keys dynamically in the key distribution phase and then start to broadcast their geographic condition messages per. All leader nodes getting keys from the server form, as illustrated in the communication range of leader is 300 meter. The key was asymmetric based shared key method in each cluster heads have a common key for sharing.

E. Performance Analysis

- The network is analyzed by affecting the network using, compare both the theoretical and simulation results
- Since cooperative authentication protocol is of particular importance in the high-load scenario.

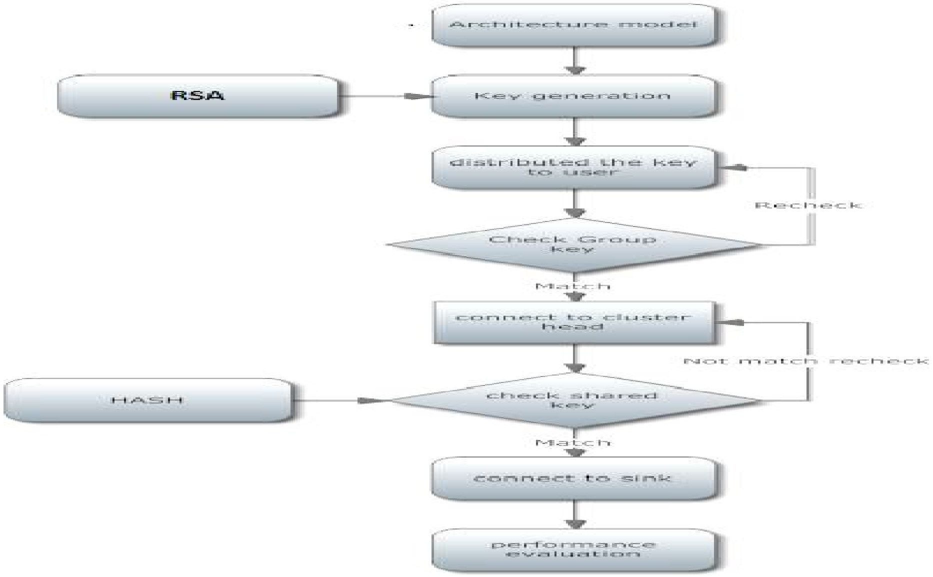


Fig.2. Data Flow diagram for authentication.

## IV. CONCLUSION

In recent years there has been a growing interest in the use of ad-hoc networks in security-sensitive applications such as digital battlefield, border protection and situation awareness. The collaborative nature of these applications makes multicast traffic very common. This paper has presented RSA, HASH KEY, Which combining both time and secret-information asymmetry in order to achieve scalability and resource efficiency. It reduces delay on data transferring and gets high throughput ratio compare to existing scheme.

## V. RESULT

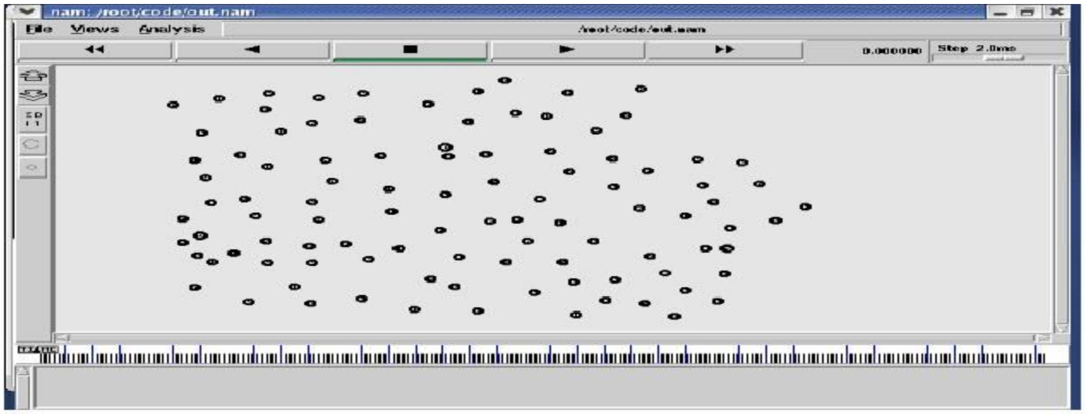
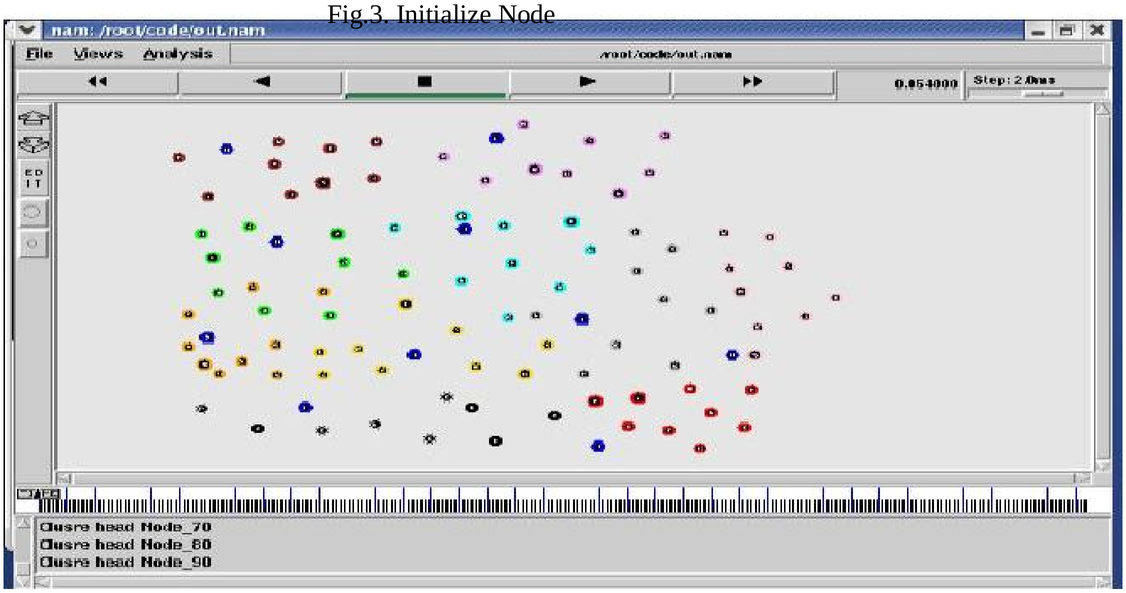


Fig.3. Initialize Node



Clusre head Node_70
Clusre head Node_80
Clusre head Node_90

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

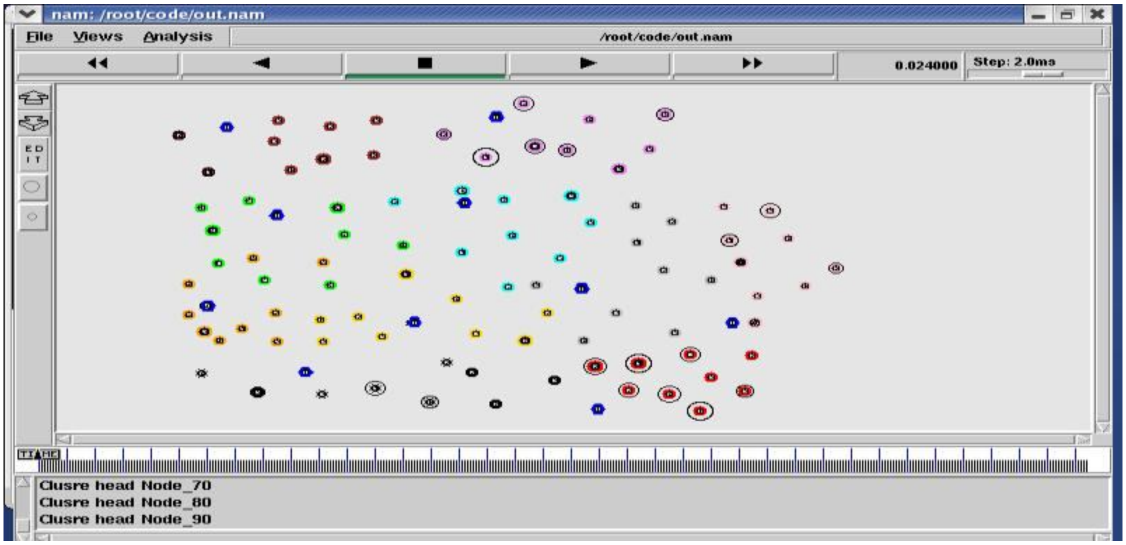
(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Fig.4. Cluster Head Selection



Clusre head Node_70
Clusre head Node_80
Clusre head Node_90

Fig.5. Transmitting the Data

## REFERENCES

[1] C. E. Perkins, Ad Hoc Networking. Addison-Wesley, 2001.

[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] 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.

[5] R. Canettiet al., "Multicast security: a taxonomy and efficient construc-tions," in Proc. 1999 IEEE INFOCOM

[6] R.Safavi-Naini and H.Wang, "Multi receiver authentication code: models, bounds, constructions, and extensions", Inf.Computation, vol-151,no.1-2, pp 148-172, may 1999.

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

[8] A. Perrig, "The BiBa one-time signature and broadcast authentication protocol," in Proc. 2001 ACM Conf. Computer Commun. Security.

[9] L. Reyzin and N. Reyzin, "Better than BiBa: short one-time signatures with fast signing and verifying," in Proc. 2002 Australian Conf. Info. Security

Privacy, pp. 144–153.

[10] A. M. Hegland, E. Winjum, S. F. Mjolsnes, C. Rong, O. Kure, and P.Spilling, “A survey of key management in ad hoc networks,” IEEE Commun. Surveys & Tutorials, vol. 8, no. 3, pp. 48–66, Dec. 2006.

[11] F. R. Yu, H. Tang, P. Mason, and F. Wang, “A hierarchical identity based key management scheme in tactical mobile ad hoc networks,”IEEE Trans. Netw. Service Management, vol. 7, no. 4, pp. 258–267,Dec. 2010.

[12] R. Gennaro, et al., “Strongly-resilient and non-interactive hierarchical key-agreement in MANETs,” in Proc. 2008 European Symp. Research Computer Security.

[13] G. Hanaoka, T. Nishioka, Y. Zheng, and H. Imai, “A hierarchical non-interactive key-sharing scheme with low memory size and high resistance against collusion attacks,” Computer J., vol. 45, no. 3, pp.293–303, 2002.

[14] M. Younis, K. Ghumman, and M. Eltoweissy, “Location-aware combinatorial key management scheme for clustered sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 17, no. 18, pp. 865–882, Aug. 2006.

[15] E. C. H. Ngai and M. R. Lyu, “An authentication service based on trust and clustering in wireless ad hoc networks: description and security evaluation,” in Proc. 2006 IEEE International Conf. Sensor Networks,Ubiquitous, Trustworthy Computing.

[16] Y. Lu, B. Zhou, F. Jia, and M. Gerla, “Group-based secure source authentication protocol for VANETs,” in Proc. 2010 IEEE GLOBECOM Workshop Heterogeneous, Multi-hop Wireless Mobile Networks.

[17] M. Youssef, A. Youssef, and M. Younis, “Overlapping multihop clustering for wireless sensor networks,” IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 12, pp. 1844–1856, Dec. 2009.

[18] J. Y. Yu and P. H. J. Chong, “A survey of clustering schemes for mobile ad hoc networks,” IEEE Commun. Surveys & Tutorials, vol. 1, no. 1,pp. 31–48, 2005.