ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 5, May 2013

DSCAM with Rough Sets Generic SSL-DES-96

S.R.M.Krishna[1], P.Kamakshi Prasad[2], Y.Vishnutej[3], P.Narendra Kumar[4]

Assistant Professor, Department of CSE, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, INDIA[1]

Professor, Department of CSE, JNTU Hyderabad, Hyderabad, INDIA [2]

Student, Department of CSE, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, INDIA [3]

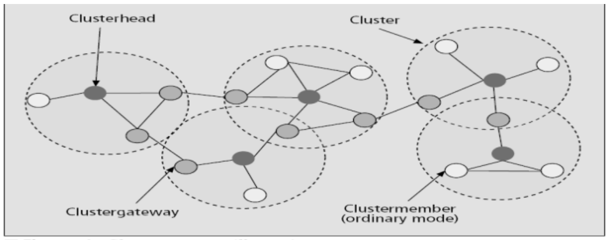
Student, Department of CSE, Gayatri Vidya Parishad College of Engineering, Visakhapatnam, INDIA [4]

Abstract: A technology can be sustainably viable only if it can find widespread use. In order to allow ad hoc networks to achieve commercial success, we must solve the scalability problem. One approach is through clustering. Various clustering algorithms have been devised as building blocks for this purpose. This paper proposes a clustering technique for MANETs, which is distributed, dominating set based, weighted and adaptive to changes in the topology called Distributed Scenario-based Clustering Algorithm for Mobile ad hoc networks (DSCAM).
The purpose of the proposed work is to provide QOS through cluster classification based on their battery power and signal strength using rough sets idea. we incorporate security, provide guaranteed QoS and enhancement for use in heterogeneous mesh and sensor networks and this is accomplished by using SSL-DES-96(double encryption) enhancement algorithm. The performance of this algorithm is evaluated through simulation and data transfer among the nodes is done through SFTP.

KEYWORDS: Mobility, Multi cluster head, Dominating Set, classification, Rough set

1. INTRODUCTION

Clustering has been used for multi-hop networks since their appearance because of its effectiveness in supporting quality of services in multi-hop networks an example of multi-hop networks is a mobile adhoc, network. As the network topology of mobile adhoc networks changes as nodes roam around, any clustering scheme should be adaptive to such changes. In a clustering scheme[7] the mobile nodes in a MANET are divided into different virtual groups, and they are allocated geographically adjacent into the same cluster according to some rules with different behaviours for nodes included in a cluster from those excluded from the cluster. A typical cluster structure is shown in Fig. 1.



■ **Figure 1.** *Cluster structure illustration.*

It can be seen that the nodes are divided into a number of virtual groups (with the dotted lines) based on certain rules.

Under a cluster structure, mobile nodes may be assigned a different status or function, such as cluster head, cluster gateway, or cluster member. A clusterhead normally serves as a local coordinator for its cluster, performing intra-cluster transmission arrangement, data forwarding, and so on. A cluster gateway is a non-clusterhead node with inter-cluster links, so it can access neighbouring clusters and forward information between cluster. Subsequently, it is important to define an efficient clustering algorithm that provides good performance with minimum clustering management overhead incurred by changes in network topology.

While selecting the dominating nodes, redundancy is achieved by choosing the value of parameter k greater than one and parameter r allows increasing local availability. These two parameters can be conveniently set depending on the requirement

Dominating nodes are potential nodes to become cluster heads and during the cluster formation phase, the ordinary nodes select their best as the clusterhead. This selection is based on quality, which is a function of parameters such as stability of the dominating node with respect to its neighbors, remaining energy with the node and connectivity. Selection of clusterhead based on these parameters help in maintaining the structure of the created cluster as stable as possible thus minimizing the topology changes and associated overheads during clusterhead changes .

A. Advantages of Clustering

They include (i) shared use of applications within the group (ii) provision for optimization in routing mechanism (ii) efficient handling of mobility management (iv) spatial reuse of resources (v) virtual circuit support (vi) better bandwidth utilization (vii) aggregation of topology information and (viii) minimizes the amount of storage for communication

II. DSCAM ALGORITHM

The procedure consists of the following steps:

Step I

Computation of (k, r) − Dominating set. DSCAM uses distributed algorithm which works in two stages. The first stage computes clusterhead nomination of each node and the second stage selects optimal (k, r) − Dominating set.

Step II

Dominating nodes computes its quality by assigning various weights[9] to different parameters such as degree of the node, battery power, transmission rate and mobility[8] and send the message containing the quality to all other nodes within r-hop distance.

Step III

Ordinary nodes and gateway nodes select the most qualified dominating node within r-hop distance as their clusterhead. They send NODE JOIN REQ(NJ) message to the most qualified node.

Step IV

On receiving the NODE JOIN REQ message, the dominating node accepts the request by sending NJ ACK packet if the degree (number of accepted cluster members) of that dominating node does not exceed the threshold.

Step V

If a dominating node does not receive any NODE JOIN REQ message for a specified time interval it can select the most qualified dominating node within r-hop distance as its clusterhead and can join with that cluster. This is known as cluster merging and this method reduces the total number of clusters in the network. This is possible only if that dominating node has k other dominating nodes within r-hop distance. This will reduce the total number of clusters created.

Step VI

If the ordinary node does not receive any NJ ACK messages within the stipulated time it can send NJ message to the next qualified dominating node within r-hop distance.

Step VII

If the node does not receive any NJ ACK messages even after k attempts and if it does not receive any new CLUSTER HEAD ADVERTISEMENT (CHA) message during the above period and if the total number of clusters in the network is above the allowable threshold then change its status to clusterhead and send CHA message to all nodes within r-hops.

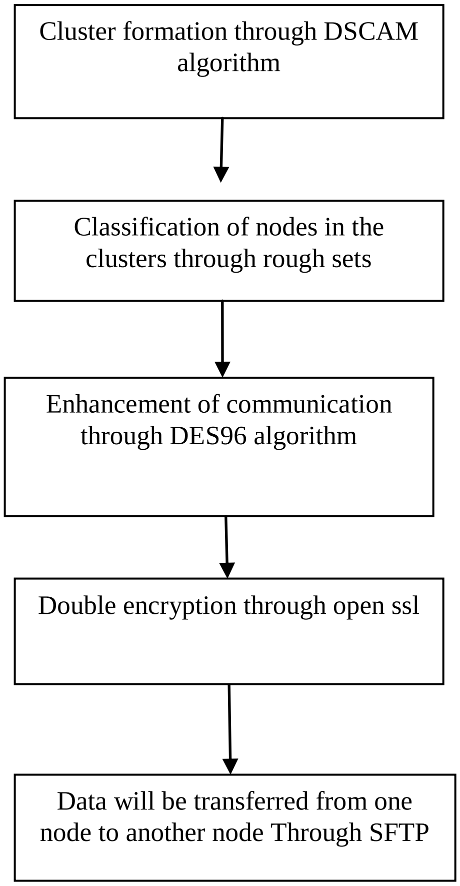
Step VIII

In case of clusterhead failure or if the battery power of the clusterhead goes below the minimum desired level, clusterhead sends this using CHA message. All the nodes attached to that clusterhead select the next qualified dominating node as its new cluster head.

III. THE PROPOSED ALGORITHM

Despite their increasing popularity, scenario-based clustering algorithms are not secure and they do not always provide the defined Quality of Service. The purpose of the proposed work is to incorporate security, provide guaranteed QoS and enhancement for use in heterogeneous mesh and sensor networks and this is accomplished by using DES-96 enhancement algorithm.

Steps Involved:


Cluster formation through DSCAM algorithm
Classification of nodes in the clusters through rough sets
Enhancement of communication through DES96 algorithm
Double encryption through open ssl
Data will be transferred from one node to another node Through SFTP

Step 1: Formation of Clusters using DSCAM[1][5]
Step 2: Cluster Classification through Rough Sets[11][12].
Cluster Classification is done through rough sets. Rough set theory is an elegant and powerful methodology in extracting and minimizing rules from decision tables and Pawlak information systems[11]. Its central notions are core, reduct, and knowledge dependency. It has been shown that finding the minimal reduct is an NP hard problem.
Our approach focuses on the elimination of the redundant attributes in order to generate the effective reduct set (i.e., reduced set of necessary attributes) and formulating the core of the attribute set The purpose of using rough set theory is to provide QOS through cluster classification based on their battery power and signal strength.
Step 3: Providing enhancement of communication through DES-96[2]

Step 4: guaranteed QoS in heterogeneous mesh and sensor networks is accomplished by using SSL.
The openssl[3] program provides a rich variety of commands each of which often has a wealth of options and arguments.
The pseudo-commands list-standard-commands, list-message-digest-commands, and list-cipher-commands output a list of the names of all standard commands, message digest commands, or cipher commands, respectively, that are available in the present open ssl[3] utility.

enc.sh

```
#$1 = filename
openssl enc -aes-256-cbc -salt -in $1 -out y.txt -pass
#pass:"gvpcoe"
```

dec.sh

```
openssl enc -d -aes-256-cbc -in y.txt -out y.dec -pass
#pass:gvpcoe
```

Step 5: Data transfer among the nodes is through SFTP. SFTP is an interactive file transfer program, similar to ftp, which performs all operations over an encrypted ssh[4] transport.
Syntax:Sftp host name @ ip address file name.

IV. DES 96 KEY GENERATION ALGORITHM

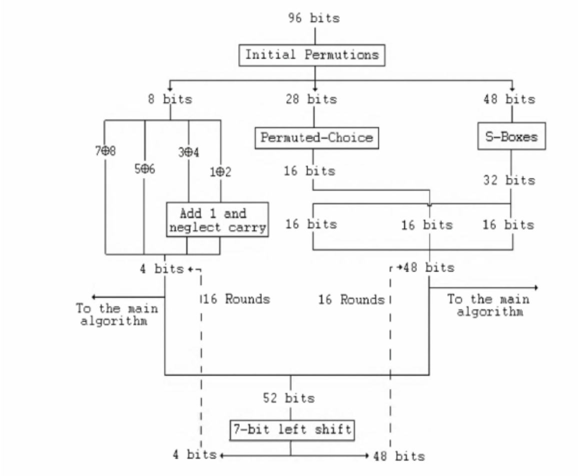
The proposed key generation algorithm can be seen in figure and is described in the following steps:

Step 1:
The 96-bit key enters an initial permutation that discards the 12 parity bits to give an 84-bit key. The initial permutations are shown below.

Step 2:
The 84 bits are now divided into three parts:
a. 48 bits enters the S-Boxes to produce a 32-bit output.
b. 28 bits enter a permuted choice to produce a 16 bit output. This permuted choice is shown below
c. 8 bits are processed as the following: each two adjacent bits are XORed together to produce 4 bits.

Step 3:
The leftmost 16 bits of the 32-bit output of Step (2,a) are swapped with the 16-bit output of Step (2,b) and all these outputs are combined to produce a 48-bit block to be sent to the main algorithm as Kl (the first sub key)

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021



.

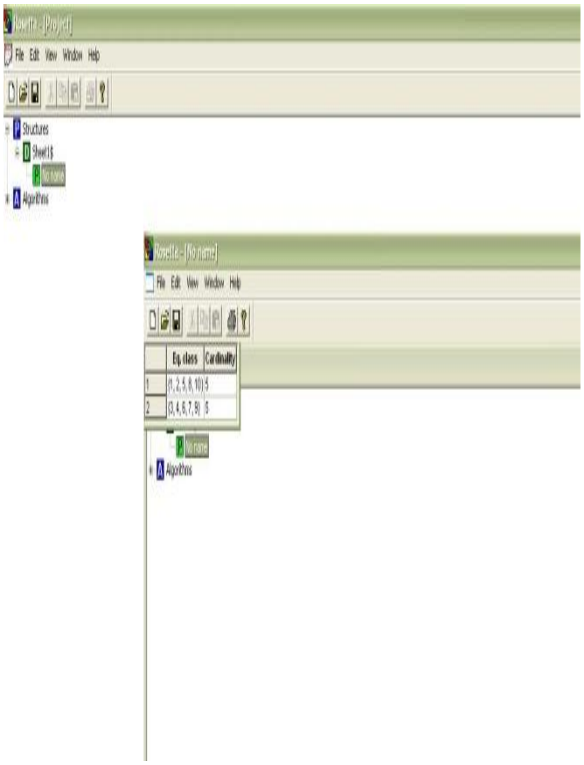
Step 4:
The 4-bit output from Step (2,c)is used twice after adding 1to the two least significant bits and discarding the carry. First, the 4 bits are sent to the main algorithm to control the arrangement of the S-Boxes. The first bit determines whether to swap boxes 2 and 3, the second bit is used to control the swapping of boxes 1 and 7, the third controls boxes 4 and 6, and the fourth controls boxes 5 and 8. The 4 bits are the recombined with the 48 bits to prepare the sub-key of the next round.

Step 5:
For the next round, a shift of 7 bits to the left takes place and the rightmost 48 bits are sent to the main algorithm and the leftmost 4 bits are dealt with as the output of Step (2,c), and so on for 16 rounds[10]. The only change to the main algorithm was the 4 bits sent with each sub-key to determine the arrangement of the SBoxes for each round.

RESULTS :

Node No	Battery pow	Signal stren	Quality
N1	High	High	High
N2	High	Low	High
N3	Low	High	Low
N4	Low	Low	Low
N5	High	Low	High
N6	Low	High	Low
N7	Low	Low	Low
N8	High	Low	High
N9	Low	High	Low
N10	High	Low	High

Table-1: Classification of node



	Eq. class	Cardinality
1	{1, 2, 5, 8, 10}	5
2	{3, 4, 6, 7, 9}	5

Figure 3: Rosetta tool for classification

S.no	Length of the plain	Time taken in DES		Time taken in	
		Encryption	Decryptio	Encryption	Decryptior
1	58	41	20	5973	150
2	21	31	20	6284	29
3	22	51	50	47798	65

Table-2:Time results b/w DES vs DES96

Plain text	DES			DES96		
	Cipher text	Encryption	Decryptio	Cipher text	Encrypti	Decrypt
Distributed scenario	kd?(_?@:_ «@h_D_&	89	76	"?Î.N?F®.¦ &_ÎÆ¦v?N	4975	290
networks	k2dÞ?Wsß ¾:?ì×Yã8	25	17	v¦.îöNÖÎ	6415	19
we are from computers	öbï?¼A~ Ú?fï?ó¯â °¡???	31	10	î¦ ?N¦ fN ö¶ Æö¶ ®.¦NÎ	2753	32

Table-3:Encryption/Decryption results

V.CONCLUSION

DSCAM for MANETs creates clusters in such a way that they remain stable over a long period of time. We provide QOS through cluster classification based on their battery power and signal strength using rough sets The designed system incorporates security, provides guaranteed QoS and enhancement for use in heterogeneous mesh and sensor networks accomplished by using SSL-DES-96(double encryption enhancement algorithm The DES96, is introduced here to resist brute-force attack, differential cryptanalysis, and linear cryptanalysis. These attacks are considered in the design because they are the most effective attacks against the original DES. Detection of malicious nodes and dynamic route discovery are the topics suggested for further research.

REFERENCES

[1]. Anitha, V.S., M.P. Sebastian, "Scenario-based Diameter-bounded Algorithm for Cluster Creation and Management in Mobile Ad hoc Networks," 13th IEEE/ACM International Symposium on Distributed Simulation and Real Time Applications, pp. 97-104, 2009.

[2]. Mohammed M. Alani," DES96 - Improved DES Security," 7th International Multi-Conference on Systems, Signals and Devices, 2010

[3]. Website :www.openssl.org

[4]. Website : www.openssh.org

[5]. Anitha, V.S. and M. P. Sebastian, "SCAM: Scenario-based Clustering Algorithm for Mobile Ad hoc Networks," Proc. First International Conference on Communication Systems and Networks, 2009.

[6]. Prithwish Basu, Naved Khan and Thomas D.C.Little,"A Mobility based Metric for Clustering in Mobile Ad Hoc Networks",in proceedings IEEE ICDCW 01 April,pp.413-18.

[7]. C.R.Lin and M.Gerla,"Adaptive clustering for mobile wireless Networks",in IEEE JSAC vol.15,sept.1997,pp.1265-75

[8]. Inn Inn Er and Winston K.G.Seah,"Performance Analysis of Mobility-based d-hop (MobDHop)clustering Algorithm for MANETs",Computer Networks,Vol.50,Issue 17 2006.

[9]. Wonchang Choi and Miae Woo,"A distributed Weighted Clustering Algorithm for Mobile Ad Hoc Networks,"Proc.IEEE ICIW 2006.

[10]. E.Biham and A.Shamir,"Differential Cryptanalysis of the full 16-round DES",in Proc.of CRYPTO'92,page 487.

[11]. Pawlak, Z., "Rough sets: basic notion," Int. J. of Computer and Information Science 11, 344-56, (1982).

[12]. Greco, S., Matarazzo, B., Slowinski, R., Stefanowski, J., Zurawski, M., "Incremental versus non-incremental rule induction for multicriteria classification," Peters, J.F. et al. (Eds.): Transactions on Rough Sets II, LNCS 3135, Springer-Verlag Berlin Heidelberg, pp. 33 – 53 (2004).

BIOGRAPHY

S.R.M.Krishna received B.Tech degree in CSE from GVPCOE(Affiliated to jntuk),M.Tech from JNTUK and pursuing ph.D in JNTUH.

P.Kamakshi Prasad received Doctorate award from IIT kharagpur, and presently working as prof.. in JNTUH.He had so much passion for Research work.

Y.Vishnu Tej received B.Tech degree in Computer Science and Engineering from GITAM University (Affiliated to Andhra University). Currently pursuing M.Tech in Computer Science and Engineering from Gayatri Vidya Parishad College of Engineering , Visakhapatnam , INDIA. My areas of research include routing algorithms, Mobile ad-hoc networks, mobility management. Presently, working on rough set theory

Penta Narendra Kumar received B.Tech degree in Computer Science and engineering from M.V.G.R.College of Engineering (Affiliated to JNTU-Kakinada) .Currently pursuing M.Tech in Computer Science and Engineering from Gayatri Vidya Parishad College of Engineering, Visakhapatnam, INDIA. My areas of research include Mobile ad-hoc networks, mobility management. Presently, working on Peer-Peer to networks.