ISSN (Online) : 0974-5645
ISSN (Print) : 0974-6846
DOI : 10.17485/ijst/2015/v8i4/60435

An Enhanced Distributed Weighted Clustering Routing Protocol for Key Management

K. Gomathi[1*] and B. Parvathavarthini[2]

[1]Computer Applications, Sathyabama University, India; gomathikrishna@gmail.com
[2]St. Joseph Engineering College, India; parvathavarthini@gmail.com

Abstract

Key management is an essential part of multicast security. The distribution of keys in an authenticated manner is a difficult task in MANETS and when a mobile node leaves or joins generates new session key. The combination of Enhanced Distributed Weighted Clustering Routing Protocol (EDWCRP) and RSA has been proposed to secure multicast key distribution. Cluster Head (CH) maintains the group key and it also updates the group key whenever there is a change in the membership. A Secondary Cluster Head (SCH) is also elected to avoid the CH from becoming a bottleneck. Mobile nodes get authenticated using MD-5 hash authentication mechanism. The performance of the system is evaluated based on attackers and metrics like Packet Delivery Ratio, energy consumption and packet drop. As demonstrated by simulation results, the proposed algorithm improves the overall performance and reduces energy utilization.

Keywords: Cluster Head, Secondary: Cluster Head, EDWCRPs, RSA, MD-5

1. Introduction

MANETs are set of wireless nodes that intercommunication using common wireless medium. The topology of the network impermanent is due to its mobile nature. The mobile nodes may enter and leave the network at any time. Here the network is amorphous, formed without any preplanning. Each node acts as both host and router cooperate themselves for data forwarding. To implement group oriented applications in MANET multicasting technique is used[1]. The blend of MANET with multicasting introduces new challenges towards secure data transmission. The secret keys are also known as Traffic Encryption Key (TEK) used to encrypt and decrypt data by sender and receiver respectively. For achieving maximum security Key management techniques are used[2]. This technique takes the liability of creation, distribution and updates the secret keys when the membership changes. If the entire network is considered as single network, when the node join or leave new secret key must be evaluated and distributed to entire network. This is entire waste of valuable network resources. To overcome this issue Multicast group is divided into smaller subgroups known as Clusters Each cluster is managed by the head known as Cluster Head (CH), and it supervise local key administration. The mobile node movement does not affect entire network, the concern cluster with less members are taking part in key management.

Except Weight based clustering, other clustering methods like low maintenance clustering, mobility based clustering, flooding based clustering and channel based clustering considers only one feature of mobile node to elect the cluster heads. This type of CH election not suitable for all type of applications[3,4,5]. So in our research CH is elected by considering all the features of mobile node and also secondary cluster head used to monitor the CH. Here RSA algorithm used for generating secret keys by using contributory key management approach. Unlike the other two key management techniques named Centralized and Decentralized, the contributory key management method gives high reliability in generating secret keys[2]. So the main motivation behind our work is to combine the advantages of both Enhanced Distributed Weight based Clustering and distributed/contributory key management

**Author for correspondence*

using RSA algorithm. Due to this combination node with longer lifetime is selected as CH and communication between the nodes achieved with high reliability. The main objective of multicast security is guarantee authentication between the nodes, and this is implemented by using MD-5 hash authentication technique[6]. The attackers are introduced to prove our proposed protocol robustness when comparing with existing methods[7].

2. Previous Work

In[8] proposed efficient resource allocation in multicasting over mobile ad hoc networks. In this geographic region is divided into many virtual zones. The node closest to the source elected as zone leader and this is responsible for its zone communications. Here distance is the metric used for selecting zone leader.

In[9] proposed distributed group key management protocol over non-commutative division semi rings. In this distributed group key agreement protocol proposed for four persons, using non-commutative division semi ring and the protocol can be extended for 'n' persons by using the same methodology.

In[10], proposed an efficient group rekeying method using enhanced one way function tree protocol, here hybrid key management technique used that combines centralized and decentralized key management. When new member joins in the group, existing Group Key Controller (GKC) decides whether to have single GKC or two GKC based on rekeying cost. The rekeying cost calculated for every membership change, so the computation overhead is high.

In[11], proposed a secure key management system in group structured mobile ad hoc networks, here member in group is considered not more than two hops. This proposal doesn't require any trusted third party such as Key Distribution Center (KDC). Group Leader is randomly shifted to maintain the energy level.

In[12], proposed a cluster-based key management scheme for MANET. In this nodes in closer distance or better connectivity would get together and choose a head of cluster (CH). The main advantage over here is reduce communication overhead by delay rekeying policy. Every member node receives nonce from CH to authenticate communication.

2In[13], proposed an efficient group key agreement scheme for MANETs based on merkle identity tree. Merkle tree is a kind of binary tree, in which the nodes store values. Members want to join in multicast group first they have register with Key Generation Center (KGC). The KGC divides the whole group into subgroups based on regional information. The main advantage of this method is communication delay is reduced.

In[14] proposed region based group key management protocol. In this network is divided into subgroups based on their region. For secure data transmission Novel Re-keying Function Protocol (NRFP) is used and this is based on decentralized key management scheme.

In[15] proposed an efficient key management scheme for MANET with authentication. In this lowest id algorithm is used for CH election. Here CH generates group key by using cluster members contribution. Nodes in the cluster are authenticated by means of hash authentication technique. Monitoring node used to see the status of CH.

3. Proposed Work

Amongst different clustering algorithms, the most suitable one that takes multiple metrics (Degree difference, Energy or battery power, Mobility and transmission range) into account for cluster configuration is Enhanced Distributed Weight-Based Clustering approach. The advantage of this clustering algorithm is the flexibility of adjusting the weighting factors for each system parameter to make it suitable for different scenarios.

In our enhanced version of Weight based approach includes monitoring node also known as SCH which monitors the energy level of CH, and when the CH downs it will take the responsibility of CH and it will extend the lifetime of the network. The details contained in the CH will be shifted to SCH and that will become new CH. The election procedure initiated to find the new SCH. In previous work, during CH sudden death that particular cluster will be collapsed and that moment transaction will be affected. In Present work to avoid that one SCH monitors CH lifetime and it will take the role of CH just before the death. And also authentication between the nodes is introduced by means of MD5 hash authentication technique. For Key management distributed (Contributory) group Key Agreement approach is used for forming the group key.

In our experiment we introduce attackers in network layer to prove our efficiency. In fabrication attacks, intruder generates false routing messages, in order to disturb the normal network operation and to consume network valuable resources in our simulation fabrication type attacks named fault data injection attack and route disruption attack are introduced and proved our proposed EDWCRP protocol proficiency by comparing existing protocol. The proposed protocol EDWCRP is represented by following flow diagram (Figure 1) that includes two main modules, clustering and key management[16,17,18].

4. Clustering

The process of clustering involves form a subgroup and nominates a head known as cluster head (CH). To elect efficient CH, initially weight will be computed for each and every node in the network. To begin with weight computation process each node is identified by unique ID and all nodes calculate their own weight based on Degree difference, Energy (battery power), Distance (from this node to all other) and mobility (speed). The Equation (1) is used for calculating weight value for mobile node.

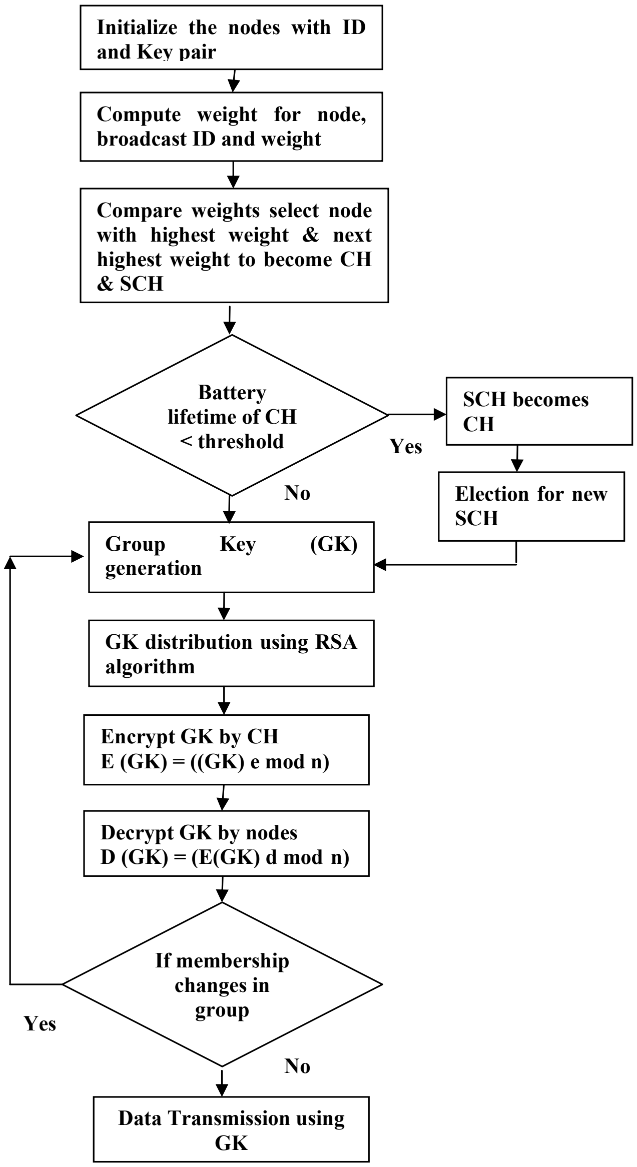

Initialize the nodes with ID and Key pair
Compute weight for node, broadcast ID and weight
Compare weights select node with highest weight & next highest weight to become CH & SCH
Battery lifetime of CH < threshold
Yes
SCH becomes CH
Election for new SCH
No
Group Key (GK) generation
GK distribution using RSA algorithm
Encrypt GK by CH
E (GK) = ((GK) e mod n)
Decrypt GK by nodes
D (GK) = (E(GK) d mod n)
If membership changes in group
Yes
No
Data Transmission using GK

Figure 1. Flow chart for CH election and Group Key Management.

$$W_n = W_1^* \Delta_n + W_2^* E_n - W_3^* M_n + W_4^* D_n \qquad (1)$$

Where,

W_n - Computed weight of node 'n'.
Δ_n - Degree Difference of node 'n'.
E_n - Energy of node 'n'.
M_n - Mobility of node 'n'.
D_n - Distance from all other neighboring nodes to node 'n'.
W_1, W_2, W_3, W_4 - co-efficient.

The co-efficient are assigned with the values, $W_1 = 0.5$, $W_2 = 0.35$, $W_3 = 0.05$, $W_4 = 0.1$ and the total of these co-efficient is 1. The Degree difference and Battery Power are considered significantly and assigned with higher values 0.5 and 0.35. The following Equations 2, 3, 4, 5 are used for calculating Δ_n, E_n, M_n, D_n respectively and these values are applied for calculating total weight value W_n by using Eq.1. The weight values are stored in each node with its ID and these are transmitted to neighbors to nominate CH.

4.1 Degree Difference (Δ_n)

It is the difference between assumed cluster size N and the existent number of neighbours d_n. It is represented in Eq 2.

$$\Delta_n = |d_n - N| \qquad (2)$$

4.2 Battery Power or Energy (E_n)

Battery power in each node is known as energy and it is measured by the unit Joules. Energy E_n of node 'n' is calculated Eq 3 as

$$E_n = E_0 - E_{used} \qquad (3)$$

E_0 and E_{used} are initial and used energy of node 'n'

4.3 Speed or Mobility (M_n)

Almost stable nodes have more chance to become a CH. M_n - Moving speed of node 'n' is calculated by following formula,

$$M_n = \frac{1}{T}\sum_{t=1}^{T}\sqrt{\left(X_t - X_{t-1}\right)^2 + \left(Y - Y_{t-1}\right)^2} \qquad (4)$$

The X, Y axis positions of node 'n' at time t and t – 1 are (X_t, Y_t) and (X_{t-1}, Y_{t-1}). The 'T' that represents cumulative time.

4.4 Distance (D_n)

It is defined as sum of distance from node 'n' to all other nearby nodes. Here in Eq 5. $N(n)$ represents set of neighbors of node 'n', the D_n is estimated as

$$D_n = \sum_{n \in N(n)} \{\text{distance}\,(n, n)\} \qquad (5)$$

4.5 Cluster Head (CH) Nomination

Figure 2 and Figure 3 represents Cluster Head election and Cluster Head lifetime monitoring algorithms respectively. The Secondary Cluster Head (SCH) also elected to avoid bottlenecks while the death of CH.

```
Algorithm for Cluster Head Election
Step 1: Calculate weight for every node based on the Metrics like Node Degree, Mobility, Connectivity and Energy Remaining.
Step 2: Broadcast Weight value and its Id to all its Neighboring nodes and the neighborhood table updated with weight value.
Step 3: CH and SCH elected based on the weight value.
If (The Node with highest weight value).
Elect that Node as a CH.
If (The Node with next highest weight). Elect that Node as a SCH.
Else, Ordinary nodes send Join request to CH to form a Cluster.
```

Figure 2. Algorithm for Cluster Head Election.

```
Algorithm for Cluster Head Lifetime
SCH monitor the battery level of CH for every 30s.
If (Battery level of CH < Minimum
    Threshold Level).
        SCH will become New CH,
        Send CH_LIFE DOWN Msg to all
        member nodes,
        Election procedure initiated to find
        new SCH.
Else,
    Re election not needed.
```

Figure 3. Algorithm for CH life time.

5. Group Key Management

5.1 Group Key Distribution (CGKD)

After the nomination of Cluster Head, it initiates the group key generation process by collecting cluster members ID and public key. Here in (Figure 4) represents step by step procedure of calculating GK.

The Eq 6, that represents group key calculation using RSA algorithm.

$$GK = ((\alpha)^{pk1 + pk2 + \ldots pKn + CH_k} \bmod p) \text{ x } (R_v) \qquad (6)$$

Where,

GK - Group Key of Cluster.
α - primitive root of p.
CH_k - private key of cluster head.
pk_1, pk_2 … pk_n - public keys of cluster members.
p - prime number.
R_v - secret random value generated while renewing the GK.

The distribution of group key is initiated with the encryption of GK by Cluster head and decryptions in the other end absolutely the cluster members using RSA algorithm. (Figure 5) represents the algorithm for encryption and decryption in key distribution.

```
Algorithm for the Gk Generation
Step 1:
    If (Node present within the cluster)
        If CH gets public keys of all
           nodes
             calculate group key as
             follows:
             CH: GK = ((α) ^(pk1+pk2+….pKn +CH_k) mod p) X (R_v)
        End if
    End if
```

Figure 4. Algorithm for the GK generation.

```
Algorithm - Encryption and Decryption
for Key Distribution

Step 1: CH → nodes within the cluster:
        Encrypt GK using RSA algorithm

        E (GK) = ((GK) e mod n)
         in which {e, n} are public key
        pair.

Step 2: Decrypt GK in Nodes:
        D (GK) = (E (GK)d mod n) in
        which {d,n} are private key pair.
```

Figure 5. Algorithm for Encryption and Decryption in key distribution.

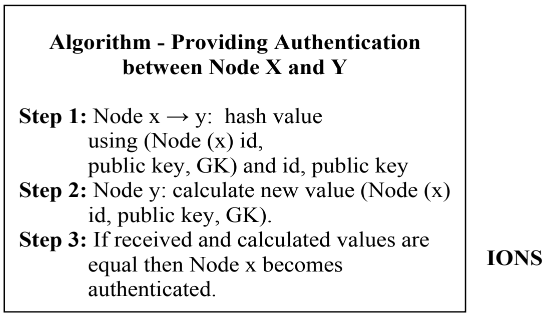
5.2 Providing Authentication

Within the cluster, if any two nodes wish to communicate first it will authenticate each other. For example node x and y becomes authenticated nodes by using following algorithm shown in (Figure 6).

6. Results and Discussions

6.1 Scope of the Research and Simulation Results

We use NS2 Network Simulator[18] to simulate our proposed protocol EDWCRP. Our simulation runs for 50 seconds with 200 mobile nodes and they will move in an area of 750 meter X 750 meter. Table 1 describes our simulation parameters and settings.



Algorithm - Providing Authentication between Node X and Y

```
Step 1: Node x → y:  hash value
        using (Node (x) id,
        public key, GK) and id, public key
Step 2: Node y: calculate new value (Node (x)
        id, public key, GK).
Step 3: If received and calculated values are
        equal then Node x becomes
        authenticated.
```

IONS

Figure 6. Algorithm providing authentication.

Table 1. Simulation Parameters

Parameters	Settings
Number of Nodes in Network	200
Area size	750 X 750
Channel Type	Wireless Channel
Radio Propagation Model	Two Ray Ground
MAC Type	802.11
Interface Queue Type	Drop Tail Queue
Routing Protocol	EDWCRP
Time of Simulation end	50 Sec
Maximum Speed	5m/s
Pause time	1 s
Number of Attackers	5,10,15,20 and 25
Attack 1	False data Injection Attack
Attack 2	Route disruption Attack
Initial Energy in Joules	16.3 joules
Initial Sending Power	0.660
Initial Receiving Power	0.395
Initial Idle Power	0.035
Transmission Rate	100
Packet Size	512 bytes

6.2 Performance Metrics used in the Experiment

6.2.1 *Energy Consumption*

It is the energy consumption of all the nodes during when the data is transmitted.

6.2.2 *Packet Delivery Ratio*

It is the ratio between received packets by the receiver and generated packets by the sender.

6.2.3 *Packet Drop*

It is the packets that are crashed at the data transmission.

Our Enhanced Distributed Weighted Clustering Routing Protocol (EDWCRP) is compared with the existing Distributed Weighted Clustering Routing Protocol (DWCRP) based on varying the attackers. In our experiment, we vary the number of attackers from 5 to 25 and measure the metrics like Delivery ratio, Packet Drop, Energy consumption for the DWCRP and EDWCRP protocols. when the number of attackers increased automatically packet drop will be more resulting in reduced Packet Delivery ratio.

Figure 7 shows the energy consumption of both proposed EDWCRP and existing DWCRP. The figure that shows energy consumption of EDWCRP is 37% less than the existing DWCRP. So, the proposed protocol Enhanced Distributed weighted Clustering Routing protocol which can save more energy better than other Clustering algorithms.

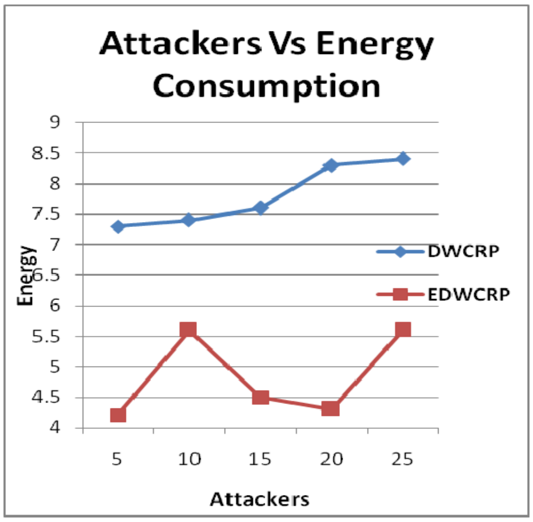


Figure 7. Attackers vs. Energy consumption.

Figure 8 shows the packet delivery ratio of both the techniques DWCRP and EDWCRP. When we have more number of attackers in the network automatically that reduces the Packet Delivery Ratio (PDR). By applying our proposed protocol PDR is 49% increased when measured with existing one.

The packet drop increases relatively with number of attackers, even though the (Figure 9.) shows packet drop is reduced to 27% by having our proposed protocol when evaluated with existing protocol.

7. Conclusion

To perform efficient cluster based routing in MANET, we combine the enhanced distributed weighted clustering with distributed key management using RSA algorithm. During CH election it is necessary to consider all metrics rather than focusing on one particular metric. By simulation results, we have proved the efficiency of our proposed protocol. Our secure Key management technique with MD5 hash authentication incur low energy consumption, less packet drop and significantly increases the packet delivery ratio of the network. In the near future, the protocol can be extended to include group key management for inter clustering to provide secure transmission of collected data.

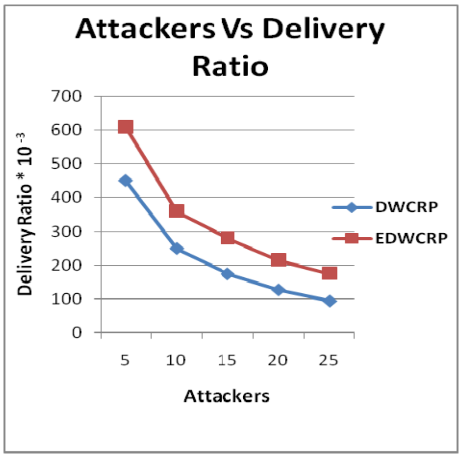


Figure 8. Attackers vs. Packet Delivery Ratio.

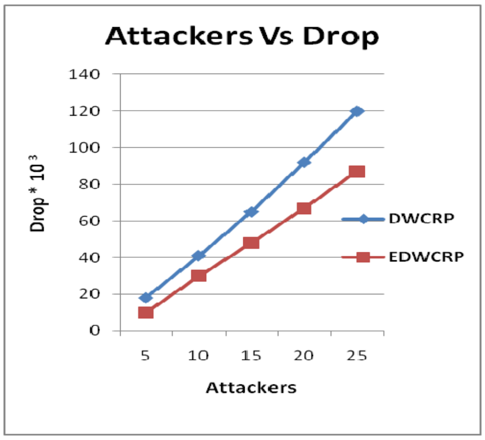


Figure 9. Attackers vs. Drop.

8. References

1. de Morais Cordeiro C. Multicast over wireless mobile Ad hoc Networks: present and future directions. IEEE Network; 2003. p. 52–9. DOI: 0890-8044/03.
2. Vennila R, Duraisamy V. Multi-level group key management technique for multicast security in Manet. J Theor Appl Inform Tech. 2013 Mar; 49(2):472–80.
3. Anupama M, Sathyanarayana B. Survey of cluster based routing protocols in mobile Ad hoc Networks. International Journal of Computer Theory and Engineering. 2011; 3(6):806–15.
4. Agarwal R, Motwani M. Survey of clustering algorithms for MANET. IJCSE. 2009; 1(2): 98–104.
5. Mehta S, Sharma P, Kotecha K. A survey on various cluster head election algorithms for MANET. Proceedings of International Conference on Current Trends in Technology (NUiCONE); 2011. p. 1–6.
6. Kahate SA, Hande KN. Implementing authentication mechanism using extended public key cryptography in wireless network. Int J Adv Res Comput Sci Software Eng. 2012 May; 2(5):35–40. ISSN: 2277 128X.
7. Shanthi N, et al. Study of different attacks on multicast mobile Ad hoc Network. J Theor Appl Inform Tech. 2009:45–51.
8. Rajkumar K, Abinaya S, Swaminathan P. Efficient resource allocation in multicasting over mobile Ad hoc Networks. Indian Journal of Science and Technology. 2014 Apr; 7(S4):71–5.
9. Anjaneyulu GSGN, Sanyasirao A. Distributed group key management protocol over non-commutative division semi rings. Indian Journal of Science and Technology. 2014 Jun; 7(6):871–6.
10. Parvathavarthini B, Valli S. An efficient group rekeying method using enhanced one way function tree protocol. IJCNS. 2006 Dec; 6(12):211–8.
11. Chauhan KK, Tapaswi S. A secure key management system in group structured mobile Ad hoc Networks. IEEE Explore; 2010. p. 307–11. DOI: 10.1109/WCINS.2010.5541789.

12. Xie H-T. Cluster-based key management scheme for MANET. Intelligent Systems and Applications (ISA). IEEE; 2011. p. 1–4. DOI:10.1109/ISA.2011.5873305.
13. Chen L-Q, et al. An efficient group key agreement scheme for MANETs based on Merkle identity tree. 2010 Second WRI World Congress on Software Engineering. IEEE Computer Society; 2010. p. 151–4. DOI: 10.1109/WCSE.2010.16.
14. Vimala N, Balabubramaniam R. A new region based group key management protocol for MANETs. Int J Comput Sci Inform Secur. 2010; 8(2):194–200.
15. Suganthi N, Sumathy V. An efficient key management scheme for mobile Ad hoc Networks with authentication. Int J Comput Network. 2010; 2(5):103–7.
16. Gomathi K, et al. A novel Weighted Clustering Architecture for Intra and Inter Cluster Routing in Wireless Mobile Ad hoc Sensor Networks (WIICRP) for Disaster Management. Proceedings of Annual convention on GeoSpatial Technologies and Applications (GEO Summit-2011); 2011 Jun 27–29. p. 39.
17. Gomathi K, Parvathavarthini B. An efficient cluster based key management in MANET. Proceedings of Second International Conference on Trendz in Information Sciences and Computing [TISC-2010]. IEEE Xplore; 2010. p. 202–5. DOI: 0.1109/TISC.2010.5714639.
18. Gandhi M, Roop LK, Gomathi K, Kumar D. Novel weight based intra cluster routing applying RSA algorithm. Proceedings of SAM 2012 Conference; 2012. p. 28–34.
19. NS-2 simulator. Available from: http://www.isi.edu/nanam/ns.