Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2013, Article ID 723913, 7 pages
http://dx.doi.org/10.1155/2013/723913

Research Article

Efficient Cluster Head Selection Algorithm for MANET

Khalid Hussain,[1] Abdul Hanan Abdullah,[1] Saleem Iqbal,[1] Khalid M. Awan,[1] and Faraz Ahsan[2]

[1] *Faculty of Computing, Universiti Teknologi Malaysia, Skudai, Johor Bahru 83100, Malaysia*
[2] *University Institute of Information Technology, PMAS-ARID Agriculture University, Rawalpindi 46300, Pakistan*

Correspondence should be addressed to Abdul Hanan Abdullah; hanan@utm.my

Received 27 May 2013; Accepted 8 October 2013

Academic Editor: Heidi Steendam

In mobile ad hoc network (MANET) cluster head selection is considered a gigantic challenge. In wireless sensor network LEACH protocol can be used to select cluster head on the bases of energy, but it is still a dispute in mobil ad hoc networks and especially when nodes are itinerant. In this paper we proposed an efficient cluster head selection algorithm (ECHSA), for selection of the cluster head efficiently in Mobile ad hoc networks. We evaluate our proposed algorithm through simulation in OMNet++ as well as on test bed; we experience the result according to our assumption. For further evaluation we also compare our proposed protocol with several other protocols like LEACH-C and consequences show perfection.

1. Introduction

Cluster head (CH) election is the process to select a node within the cluster as a leader node. Cluster Head maintains the information related to its cluster. This information includes a list of nodes in the cluster and the path to every node [1].

The responsibility of the CH is to communicate with all the nodes of its own cluster. However CH must be able to communicate with the nodes of other clusters as well, which can be directly or through the respective CH or through gateways. Communication is done in three steps. First of all the cluster head receives the data sent by its members, secondly it compresses the data, and finally transmits the data to the base station or other CH. Suitable cluster head can reduce energy utilization and enhances the network lifetime [2].

Electing a specific node as a cluster head is a very important but sophisticated job. Various factors can be considered for electing the best node as a cluster head [3]. Some of these factors include location of the node with respect to other nodes, mobility, energy, trust, and throughput of the node.

Nodes of WSN and MANET have limited battery and resources. Process of election increases the overall processing overhead of the network. So the election process must also consider the processing and energy limitations of the nodes.

One cluster head per cluster must be selected during an election process, because multiple cluster heads within a single cluster can give rise to cluster reformation, Quality of Service (QoS), and routing management issues [4].

In the recent years, various surveys of CH election schemes were presented. Aim of these surveys is to discuss their parameters, need of reclustering [5], and performance [6]. However to the best of our knowledge, no overview of the CH election emphasizing position of node in cluster, trust factor of nodes, and single cluster head selection per election process has been discussed so far.

In this paper, efforts have been made to discuss an extensive number of schemes proposed previously for CH election in both WSN and MANET. To have a better understanding, comparison of various CH selection techniques is made, in terms of parameters used and possibility of multiple CHs selection.

By using the predistinct techniques spanning tree [4] to designate the new cluster head, registration, authentication, and verification of each register node in such cluster are time incontrollable assignment. It can be practicable in wired situation where resource and time are not an immense

concern. But in tangible period and wireless ad hoc network it is a contest.

In this paper we proposed an Efficient Artificial Intelligence based algorithm for cluster head section in mobile ad hoc network. To evaluate the proposed algorithm we carried out a two-dimensional domain simulation in OmNet++, which provides conventional wireless scenarios to implement as shown in Figure 1. We use the blacklist mechanism which is discussed in Section 2; the up-dation of the routing table is also discussed in the subsection. The new extended algorithm and node authentication algorithm are discussed in Section 3. Section 4 will show the simulation results. Conclusion of the work along with some limitation and future work has been discussed in the last section.

1.1. Cluster Head Selection in MANET. All the abovementioned research works are in the scenario of wireless sensor networks. WSN and MANET have some common features like limited battery, mobility issues, and so forth. However, applications of the WSN are not applicable in MANET because nodes in WSN are designed to sense data and send to the central authority; however in ad hoc network nodes may have complete processing capabilities, for example, laptops, cell phones, and so forth. WSN has a central authority called base station, whereas MANET is a completely independent network without any infrastructure. These differences raise the need of some other solutions for election processes that are specially designed for ad hoc networks.

Weighed cluster algorithm (WCA) is proposed for MANET [7]. WCA elects the CH based on factors like mobility, ability to handle nodes, communication range, and so forth. The algorithm calculates the average weight of each node based on the provided factors. The node with the minimum weight is selected as a cluster head.

In K-hop connectivity ID clustering algorithm (KCO-NID) [8], the node having maximum connectivity is elected as CH. If two nodes have the same connectivity value then they select the node having lower ID as CH. Another approach is used for dynamic CH election based on energy level of the node [9]. In this approach nodes share their IDs and energy value using broadcast messages. After random period, the node with maximum energy level will be elected as Cluster Head. If two nodes have the same energy level, the node having the maximum number of neighbors will be elected as Cluster Head.

An identifier based clustering algorithm is proposed [10]. In this scheme a unique ID is assigned to each node. The node having minimum ID is elected as cluster head. Degree of a node is calculated by every node on the basis of distance parameter. If the Euclidean distance [11] is within the transmission range, the node will be elected as CH.

Two variants of the cluster head selection, distance-constrained and size-constrained, are proposed for MANET [2]. Two different algorithms are proposed for cluster head election. First algorithm is based on distance. According to this algorithm CH is selected if every member node is within a limited distance from the nearest CH. Second algorithm is based on the size of the cluster, where each cluster is only allowed to have a limited number of members. In this case CH is selected such that the size of each cluster is not larger than a predefined value.

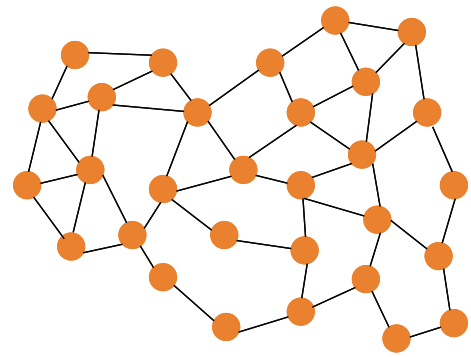

Figure 1: Conventional wireless network.

Another solution for CH election is proposed for MANET [12]. In this paper authors proposed an adaptive invoked weighted clustering algorithm, which maintains stable clusters. In Weighted Clustering Algorithm (WCA) a node is selected to be the cluster head with minimum weighted sum of four indices-node degree (number of direct links to its neighbors), sum of distances to all its neighboring nodes, mobility, and remaining battery power, respectively [7]. WCA lacks in knowing the weights of all the nodes before starting the clustering process and in draining CHs rapidly. To solve this problem S. Rouhini proposed a probability based adaptive invoked weighted clustering algorithm (PAIWCA). This can enhance the stability of the network by taking battery power of the node into consideration for selecting cluster heads and for forming clusters. The weight of a node is calculated before the clustering process thus by minimizing the overhead of reclustering in electing a cluster head.

Reputation-based trust management strategy for clustered ad hoc networks is proposed for clustered ad hoc networks [13]. In this paper a cluster head backup mechanism was maintained. The existing CH selects its backup which has maximum trust value. Cluster head updates all the information to its backup. If CH cannot communicate with other nodes, it transfers this role to the backup CH.

Another trust based approach is proposed for MANET [14]. In this work, any candidate for CH broadcasts the message with its mobility, battery power value to all its one hop neighbors. Receivers calculate the global weight of the sender by using the received information and adding trust value of the sender. If global weight is greater than a predefined value, the receiver will vote for the sender. After a certain time, the candidate node will count the votes. If the number of votes is greater than half of the number of members, it advertises itself as leader.

We have compared the abovementioned techniques in Table 2. In this table we compared the techniques and highlighted the parameters used in the above solutions. We also highlight the handling of case of tie in the above mentioned algorithms.

1.2. Cluster-Weighed Modeling. According to the statistics, cluster-weighted modeling (CWM) is an algorithm-based

method for analyzing the nonlinear prediction of outputs (reliant variables) from inputs (liberated variables) constructed on density estimation by a conventional of simulations (clusters) that are every theoretically suitable in a subsection of the input galaxy. The inclusive methodology works conjointly with input-output galaxy and an original style was suggested by Neil Gershenfeld [3, 15].

1.3. Basic Form of Model. To construct the cluster model on the basis of input, delinquent output can be formulated like: $y = x + e'$ where e' being the error for packet mishandling/retransmissions. To achieve the expected theory on the basis of the output variable y in reflection of input variable x, the joint probability solidity function can be explained as (y, x). In this situation the input and output variables can be invariant or multivariate. For the appropriateness, any typical constraints are not signposted in the symbolization here and numerous changed behaviors of these are probable, including backdrop of immobile values as a stride in the standardization or are considered expanding via Bayesian analysis. The essential prophesied tenets are acquired by fabricating the conditional probability solidity $(y \mid x)$ from which the calculation using the restrictive estimated value can be acquired; with the restrictive modification providing a symptom of ambiguity.

The significant step of the demonstrating is that $p(y \mid x)$ is presumed to yield the following procedure, as a combination model:

$$p(y, x) = \sum_{1}^{n} w_j p_j(y, x), \tag{1}$$

where n is the number of clusters and $\{w_j\}$ are weight (total number of packets sent from source to destination in specific time) that total to one. The occupations $p_j(y, x)$ are common probability solidity functions that communicate to each of the n clusters. These functions are exhibited by disintegration into a conditional and a peripheral solidity:

$$p_j(y, x) = p_j(y \mid x)\, p_j(x), \tag{2}$$

where $p_j(y, x)$ is a successful packet delivery expecting y assumed x, and it is assumed that the input-output couple should be associated with node j on the source of the assessment of x. This typical might be a waning archetypal in the weakest circumstances.

$p_j(x)$ is imperiously solidity for tenets of x, assuming that the input-output couple should be concomitant with node j. The qualified sizes of these utilities between the clusters conclude whether a specific assessment of x is connected with any assumed cluster center. This solidity influence needs to be a Gaussian function highlighted as a parameter; signifying the cluster center.

In identical fashion for regression analysis, it will be significant to deliberately renovate initial data as portion of the overall modeling strategy. The potential candidates need to be evaluated modestly in an autonomous fashion, while minimizing the possible errors of packet mishandling for each cluster on the basis of standard disseminations incorporating the cluster-weighing densities $p_j(x)$.

1.4. Technique. Assume that θ is the set of ambiguous factors and predictions in the perfect. Assume that E is taken as the altered proof. Before evaluating the assumed result on the bases of preliminary previous probability distribution, we assume that the confirmation is occupied into justification, to assume about θ.

To evaluate our proposed technique, Bays' theorem is applied:

$$P(\theta \mid E) = P(\theta) \cdot \frac{P(E \mid \theta)}{P(E)}. \tag{3}$$

$P(\theta \mid E)$ is the probability distribution of the ambiguous amounts and subsequently the confirmation is reserved into interpretation, the posterior probability.

$P(\theta)$ is the probability distribution in lieu of ambiguity roughly and the factors and expectations formerly and the indication is reserved into interpretation, the prior probability. $P(E \mid \theta)/P(E)$ is a factor in lieu of the impression of the indication on conclusions about θ.

On the other hand in the sustenance of, Bayes' theorem possibly will be applied continually. It is continuous practice in which every application the last one posterior becomes the different preceding.

2. Explanation

2.1. Elements Explanation. θ used as a special case for the interpretation of the influence, and it delineates a discrete set of standards. Assume that H is one of these potential standards. In the following equation H represents "hypothesis"; otherwise usually H epitomizes indeterminate constraint or magnitude in a perfect:

$$\frac{P(E \mid H)}{P(E)} > 1 \Rightarrow P(E \mid H) > P(E). \tag{4}$$

When the confirmation becomes according to the suggested assumption, it seems and gives more confidence when hypothesis is true. On the other side the antithesis dispute relates for a diminution in confidence. In this circumstance confidence does not modify

$$\frac{P(E \mid H)}{P(E)} > 1 \Rightarrow P(E \mid H) > P(E). \tag{5}$$

2.2. Bayes Estimator. As per estimation philosophy and decision philosophy, a Bayes estimator or a Bayes action is a measuring and authentic methodology which diminishes the posterior predictable assessment on the bases of a loss function which calls posterior expected loss. On the other side it enhances the posterior probability of an effective task.

2.3. Description. Understand that an anonymous constraint θ is recognized to have an earlier dissemination π. Let $\delta = \delta(x)$ be an estimator of θ (constructed on certain capacities x), and let $L(\theta, \delta)$ be a harm task, such as adjusted inaccuracy. The Bayes risk of δ is demarcated as $\pi\{L(\theta, \delta)\}$ and someplace the anticipation occupied terminated the probability distribution of θ; this explains the threat occupation as a task of δ.

Table 1: Simulation parameters for cluster head selection.

Examined protocol	AODV
Simulation time	25 min
Transmission range	250 m
Traffic type	UDP
Traffic load	255, 250, 245 pps
Packet size	4096
Data rate	trunc-normal
Channel error rate	0.0
Channel data rate	$11.04858e + 6$

An estimator δ is supposed to be a Bayes estimator if it diminishes the Bayes threat between all estimators. Consistently, the estimator which diminishes the subsequent predictable harm $E\{L(\theta, \delta) \mid x\}$ for each x also diminishes the Bayes threat and consequently is a Bayes estimator [1].

If the preceding is inappropriate then an estimator which diminishes the subsequent predictable damage for each x is called a generalized Bayes estimator [2].

3. Proposed Solution

3.1. Black and White List. In addition to two additional fields identified earlier that have been inculcated in the X-AODV for the purpose of decision making of routing path, another field "BlackNwhite" is added that maintains the status of each node based on malicious activity. Figure 2 shows snap of scenario in which by using the X-AODV the neighbor node identified node 11 as malicious. X-AODV change the color of malicious node to gray. To fairly evaluate we run the simulation for a period of 25 sec in multiple network scenarios, that is, 12, 15, 25, 40, 50, and 65 nodes. During this period our proposed protocol identified the malicious behavior of the nodes shown in Table 2.

4. Simulation, Result, and Analysis

According to defined parameters in Table 1 we create three scenarios, but in base parameters they were the same as above. In every scenario we change the traffic load and evaluate the performance of the X-AODV. In our proposed protocol we have not chosen the predefined cluster head nor attack or malicious node in the network. For crystal evaluation we run every scenario for a period of 25 minutes and during this period of time our proposed protocol detects the malicious behavior of the multiple nodes. In Table 2 we presented the 20-node scenario in which X-AODV detect multiple node, as malicious.

Figures 2(a) and 2(b) show the three- and five-minute real simulation picture of the 10-node scenario which shows that ECHSA detect node 5 just after 3 minutes and nine and two just after five minutes as malicious and mark the node as gray and set its flag in routing table as shown in Table 2.

Cluster Head selection is usually based on spanning tree that works on sequence number and the node with minimum sequence number is selected as Cluster Head. In our proposed solution, Cluster Head selection/reselection is performed periodically. But instead of just using the concept of spanning tree, it also takes into consideration the Black & White while selecting Cluster head. Any node having minimum sequence number but with status of black is not selected as Cluster Head, instead chance is given to the next higher sequence number node. Figure 3 shows the scenario of selecting Cluster Head, highlighted as yellow.

Table 2: Routing table with Black- and White list

Node number	Black & white identification flag	Black & white identification time
0	1	239.11
1	0	0
2	1	395.81
3	0	0
4	1	191.23
5	1	342.01
6	0	0
7	0	0
8	1	550.88
9	0	0
10	1	265.66
11	1	318.27
12	1	482.76
13	1	581.62
14	1	292.85
15	0	0
16	1	143.24
17	1	423.65
18	1	449.81
19	1	516.56

In Table 2 we have defined the 20-node experimental results in which the ECHSA make an election within those good nodes which have the status of 0. Due to the segregation process the good nodes have comparatively less quantity, so election process takes less amount of resources.

Algorithm 1 describes the overall mechanism for selection of the Cluster Head. When a network is required to select the cluster head, then every node will check its routing table according to Algorithm 1. The mathematical representation of X-AODV with probabilistic extension along with the parameters describe in Notations section.

When a node is elected as Cluster Head, it is mandatory for that node to inform all registered nodes in the cluster about its selection and the register node required to revoke their authorization certificate from new cluster head. Energy is a big issue in Wireless Network as well as in sensor network, so we also minimize this process in our proposed protocol. Algorithm 2 describes the Cluster Head announcement and also the acceptance from the registration node as well as the authorization from the Cluster Head. In this process we accommodate this announcement and certificate revoke procedure through these nonce messages.

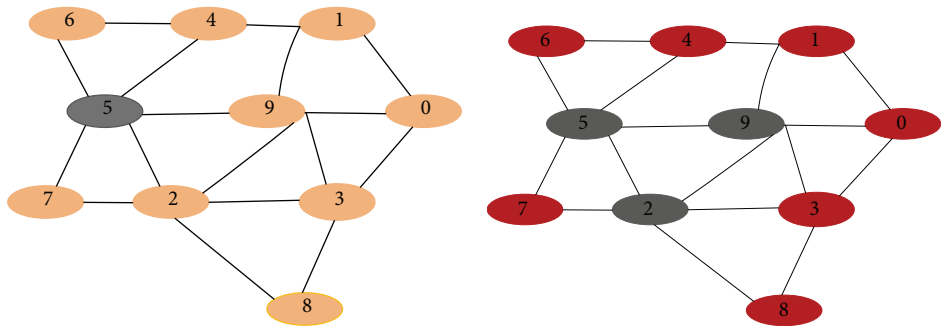

FIGURE 2: (a) and (b) Disqualify node identification for cluster head selection process (black/whitelist).

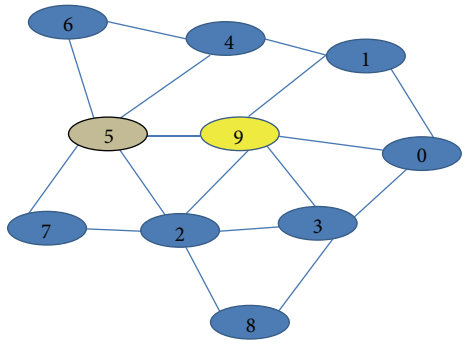

FIGURE 3: ECHSA select cluster head.

```
(1) Check R.T
(2) Check Sequence #
(3) Select highest Seq #
(4) If
        Seq # > all other Nodes
(5) Then
        Check Black List
        If
            Black List is un-check
        Then
            Elect as CH
        Else
        Reject
        endif
(6) endif
```

ALGORITHM 1: New cluster head.

Given a vector θ of parameters to determine, a prior PDF $p(\theta)$ over those parameters and a PDF $p(y \mid \theta, \xi)$ for making observation y, given parameter values θ and an experiment design ξ, the posterior PDF can be calculated using Bayes' theorem:

$$p(\theta \mid y, \xi) = \frac{p(y \mid \theta, \xi)\, p(\theta)}{p(y \mid \xi)}, \tag{6}$$

Cluster Head Selection Algorithm

CH: $\eta_1 \xrightarrow{Msg} \{a_1, \ldots, a_n\}$
$M_1 = \{\text{Public Key, CH, } \eta_1\}$
$\sum M_1 = \text{Signs}\{H(M_1)\}$
CH $\rightarrow *: \{\sum M_1\}$
R_n: $\eta_2 \xrightarrow{Msg} \{\text{CH}\}$
$M_2 = \{\text{Reply Acceptance, CH, } R_n, \eta_1, \eta_2\}$
$\sum M_2 = \text{Signs}\{H(M_2)\}$
$R_n \rightarrow$ CH: $\{\sum M_2\}$
CH: $M_3 = \{\text{Acceptance Confirmation, CH, } R_n, \eta_1, \eta_2\}$
$\sum M_3 = \text{Signs}\{H(M_3)\}$
CH $\rightarrow R_n$: $\{\sum M_3\}$

ALGORITHM 2: Node registration.

where $p(y \mid \xi)$ is the marginal probability density in observation space

$$p(y \mid \xi) = \int p(\theta)\, p(y \mid \theta, \xi)\, d\theta. \tag{7}$$

The expected utility of an experiment with design ξ can then be defined:

$$U(\xi) = \int p(y \mid \xi)\, U(y, \xi)\, dy, \tag{8}$$

where $U(y, \xi)$ is some real-valued functional of the posterior PDF $p(\theta \mid y, \xi)$ after making observation y using an experiment design ξ.

To evaluate the Cluster Performance we use the same parameters described in Table 1 but in three different scenarios.

Packet loss ratio is one of the important parameters for a node to be considered a good node as well as consider for Cluster Head selection. In these scenarios on the bases of throughput we evaluate the performance of X-AODV. In Figure 4 we evaluate the performance of X-AODV just on 10 nodes, after a period of time we increase the number of nodes up to 65 and then reevaluate the performance of the proposed protocol. Figure 5 presents the performance evaluation of

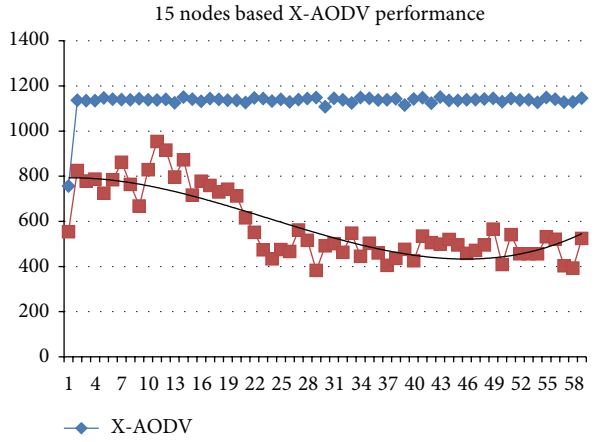

Figure 4: Cluster head selection in 15 good nodes.

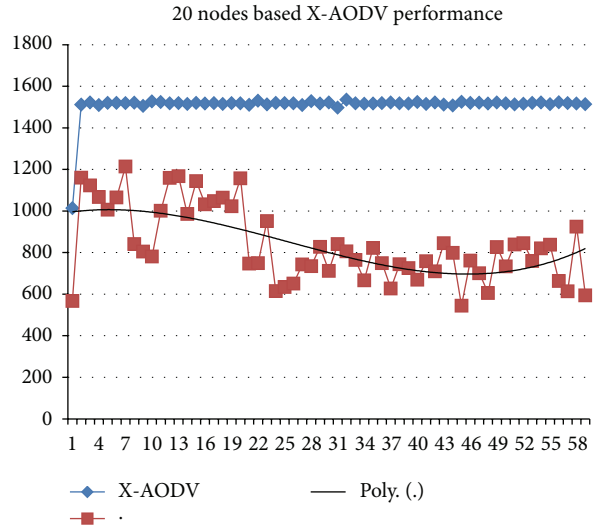

Figure 5: Cluster head selection in 20 good nodes.

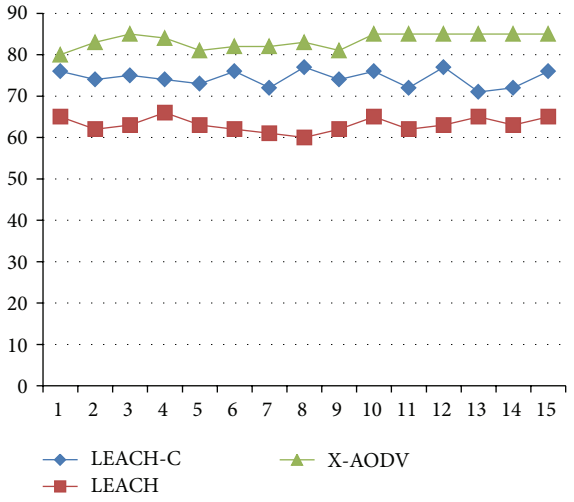

Figure 6: X-AODV comparison with different protocols.

20 nodes, whereas in Figure 6 we compare our proposed protocol with some latest protocols with the same parameters and found the Cluster Head Selection performance more batter as compare to the previous one.

Figure 4 describes the selection performance of ECHSA and in this scenario the coordination is between 15 nodes and with the help of IMBDM five nodes were detected as malicious. Hence, at the time of CH selection, those nodes are not allowed to participate for election. Then performance of the network for the simulation time is shown in Figure 4. Blue line shows the sent data, whereas the brown line shows the overall network throughput for the first minute where malicious nodes tried to inject fake routing entries on the network to disrupt communication. The result can be divided into 3 logical phases. First, while the default CH was activated at the time of network initialization, a good throughput was achieved among member nodes. However, as the malicious nodes started disrupting the topology after approximately 15 seconds, the goodput of the network dropped to half. Around 40 seconds, ECHSA was activated and blacklisted nodes were detected and discarded for packet forwarding; hence new CH was selected and fresh routes were discovered. Thus, network was restored through new routes. Similar is the inclination visible in the later part of the result. Estimated drop was around 20% which practically doubled due to multiple malicious nodes in the network, that is, 5. Even then, the network was able to maintain more than 50% of communication in the first minute, while the malicious nodes were active on the control plane. This shows that the proposed algorithm selects new cluster head without disturbing the normal communication as well as required additional resource.

The same process was repeated to analyze the behavior of ECHSA, with increased member and malicious nodes. We kept the world size the same but doubled the number of good and malicious nodes; that is, out of 30 nodes in total, 10 were malicious. Consequently, the election of a new CH was held between 20 nodes. The disruptions by malicious nodes and detection by good ones occurred little earlier, mainly due to increased nodes and network density. However, the restoration of the network initiated on approximately the same time, the reason being delay in coordination between increased nodes for CH and routes setup. The estimated drop was around half (55%), but overall 65% communication was successful, majorly due to more alternate routes possible as network density increased.

Based on the above scenarios, it has been determined that ECHSA not only works in denser environment, rather better. On average, ECHSA which has retained 63% communication with 1/3rd nodes within a network are malicious. Above all, the malicious attackers on the control plane are discarded and network starts functioning smoothly within the first minute of the topology setup.

At the end we also compare our proposed algorithm with the other Cluster Head Selection protocol and Figure 6 presents the comparison analysis with LEACH and LEACH-C.

5. Conclusion

In this paper we have presented a novel artificial intelligence based Algorithm to select new cluster head in MANET. On the bases of minimum packet loss ratio as well as malicious behavior of the node our algorithm excludes node for election as cluster head. ECHSA has the AI capabilities to select the cluster head by just populating the B&W list. Results and evaluation show that our technique is more efficient and required minimum resource for cluster head selection. With the help of our proposed protocol a significant escalation comes in the MANET lifetime. By enhancing the AI capability (bay estimator) an additional enhancement in MANET lifetime and resource consumption can be accomplished. We also experiment our algorithm in different scenarios with multiple data rate for critical evaluation and fair cluster head.

Notations

Θ: Parameters to be determined
Y: Observation or data
ξ: Design
$p(y\theta, \xi)$: PDF for making observation y, given parameter values θ and design ξ
$p(\theta)$: Prior PDF
$p(y\xi)$: Marginal PDF in observation space
$p(\theta y, \xi)$: Posterior PDF
$U(\xi)$: Utility of the design ξ
$U(y, \xi)$: Utility of the experiment outcome after observation y with design ξ.

Acknowledgment

This research is supported by the Ministry of Science, Technology and Innovation (MOSTI) and was conducted in collaboration with the Research Management Center (RMC) at the Universiti Teknologi Malaysia (UTM) under Vot no. R.J130000.7928.4S014.

References

[1] A. A. Abbasi and M. Younis, "A survey on clustering algorithms for wireless sensor networks," *Computer Communications*, vol. 30, no. 14-15, pp. 2826–2841, 2007.

[2] R. Agarwal and D. Motwani, "Survey of clustering algorithms for MANET," http://arxiv.org/abs/0912.2303.

[3] M. Chatterjee, S. Sas, and D. Turgut, "An on-demand weighted clustering algorithm (WCA) for ad hoc networks," in *Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM '00)*, 2000.

[4] P. Chatterjee, "Trust based clustering and secure routing scheme for mobile ad hoc networks," *International Journal of Computer Networks and Communication*, vol. 1, no. 2, pp. 84–97, 2009.

[5] S. Chinara and S. K. Rath, "A survey on one-hop clustering algorithms in mobile ad hoc networks," *Journal of Network and Systems Management*, vol. 17, no. 1-2, pp. 183–207, 2009.

[6] C.-L. Fok, G.-C. Roman, and C. Lu, "Rapid development and flexible deployment of adaptive wireless sensor network applications," in *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems (ICDCS '05)*, pp. 653–662, June 2005.

[7] K. Hussain, A. H. Abdullah, K. M. Awan, F. Ahsan, and A. Hussain, "Cluster head election schemes for WSN and MANET: a survey," *World Applied Sciences Journal*, vol. 23, no. 5, pp. 611–620, 2013.

[8] D. Nguyen, P. Minet, T. Kunz, and L. Lamont, "New findings on the complexity of cluster head selection algorithms," in *Proceedings of the IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks (WoWMoM '11)*, June 2011.

[9] F. G. Nocetti, J. S. Gonzalez, and I. Stojmenovic, "Connectivity based k-hop clustering in wireless networks," *Telecommunication Systems*, vol. 22, no. 1–4, pp. 205–220, 2003.

[10] K. Ramesh and D. K. Somasundaram, "A comparative study of clusterhead selection algorithms in wireless sensor networks," *International Journal of Computer Science & Engineering Survey*, vol. 2, no. 4, 2011.

[11] S. Rohini and K. Indumathi, "Probability based adaptive invoked clustering algorithm in MANETs," http://arxiv.org/abs/1102.1754.

[12] L. Xu and Y. Zhang, "A new reputation-based trust management strategy for clustered ad hoc networks," in *Proceedings of the International Conference on Networks Security, Wireless Communications and Trusted Computing (NSWCTC '09)*, pp. 116–119, April 2009.

[13] A. Zabian, A. Ibrahim, and F. Al-Kalani, "Dynamic head cluster election algorithm for clustered Ad-Hoc networks," *Journal of Computer Science*, vol. 4, no. 1, pp. 42–50, 2008.

[14] N. Zaman, A. B. Abdullah, and L. T. Jung, "Optimization of energy usage in wireless sensor network using Position Responsive Routing Protocol (PRRP)," in *Proceedings of the IEEE Symposium on Computers and Informatics (ISCI '11)*, pp. 51–55, March 2011.

[15] H. S. Lee, K. T. Kim, and H. Y. Youn, "A new cluster head selection scheme for long lifetime of wireless sensor networks," in *Computational Science and Its Applications—ICCSA 2006*, vol. 3983 of *Lecture Notes in Computer Science*, pp. 519–528, Springer, 2006.