Optimal Dynamic Clustering and Secure Transmission Approach to Prevent and Detect the Sinkhole Attack in Wireless Sensor Networks

[1]D. Udaya Suriya Raj Kumar [2]V. Rajamani Vayanaperumal

[1]Dept. of CSE, Research Scholar, Sathyabama University, Chennai.
[2] Dept. of ECE, Veltech Multitech Dr. Rangarajan Dr. Sakunthala Engineering College, Avadi, Chennai.
E-mail: u_suriya@yahoo.com

Abstract

The objective of this paper is to mainly focus on a trust aware model between the communicating sensor nodes and the base station. To perform efficient data aggregation in sensor networks, an improved cluster head selection has been proposed in this study. The algorithm employed for the study is based on Energy Efficient Dynamic Clustering (EEDC) incorporated adaptive Genetic Algorithm (AGA). The main aim of authentication based schemes is to confirm the authenticity of a node by validating its key information. The sinkhole attack in WSN occurs due to the drawing of the attention of all or almost all traffic from a particular domain by a compromised node. The compromised node is the one which looks attractive among all other surrounding nodes in terms of routing metric. The changes that have been occurring in the control fields imply the adversity of the nodes and can be detected by the BS using the proposed strategy. An improved ant colonization technique based secure routing protocol for path selection. To overcome the node failure and to increase the efficiency of the overall network, the proposed mechanism encompasses two paths for data forwarding.

Keywords: Adaptive Genetic Algorithm, Energy Efficient Dynamic Clustering, Improved Ant Colonization Technique;

I. INTRODUCTION

Wireless sensor networks (WSNs) comprise of small sensor units for sensing and sending data to base stations through an established ad-hoc mesh network of the sensor organization. The major application of WSNs is in military services for tracking enemy attack, environmental monitoring such as fire detection and in medical fields such as cardiac monitoring. Most of the WSNs are positioned in hostile environmental conditions without proper security. The security aspects of routing protocols of WSNs are also not reliable as it suffers from resource constraints of the sensors like low computational power, limited power supplies, limited memory and limited communication range. Hence, WSNs are prone to many types of attacks among which sinkhole attacks are most common. It is a network layer attack wherein the malicious node tends to attract traffic, thereby the complete and correct sensing data are prevented from reaching the base station [1]. The invader also involves in inserting a compromised node relatively close to the base station for making an attack. Based on the link quality of the routes, the routing metric selects the best route for data transmission. But the compromised node misleads the metric by conveying fake routing information to its neighboring nodes, thus causing major traffic during while passing through it to the base station. The results will be the adversity in WSNs as it sends bogus information to the base station. Selective forward attack altered routing information attack and knowledge spoofing attack is other attacks that are further triggered by the sinkhole attack [2].

The detection and protection of sinkhole attacks have been studied by many proposed methods [3]. For a few decades, two-layered architecture in WSNs called clustering had been extensively studied for various purposes. Clustering refers to division of nodes into various groups/clusters among which some nodes are chosen to represent as the head of each group called cluster-heads. The gathering of data from regular nodes followed by aggregation and transmission of the same to a base station (BS) is the task of cluster-head [4] has attempted LEACH method [5] in the area of clustering in homogeneous WSNs. The LEACH protocol works based on the random probabilistic approach in selecting the cluster-heads, which have a proper load balancing among all the nodes. An emergent algorithm based clustering approach is known as ACE [6] protocol in which the node degree was considered as the main factor to form clusters with reduced overlapping. But, the inconsideration of the energy of the nodes in the cluster-head election process becomes a drawback. [6] Protocol is another approach which uses the state transitions for election of cluster-heads. In EEHC, hierarchical clustering focusing on longevity of the network lifetime has been investigated [7]. It was found that in EEHC, the cluster-heads are elected with a probability proportional to the density of neighbor nodes in the range of the node. The most widely used clustering approach was distance based clustering as it has been applied to many problems [9], [10]. The distance-vector method called the CODA has also been proposed in which the distance of the nodes to the BS was considered for the cluster head selection [8]. The clustering approach based on the residual energy and a local competition for the cluster-head election named EECS is proposed [9]. It is an extension of the LEACH protocol for a distance-based method of cluster formation. Neighbor based clustering approach called EECABN [10] operates by introducing a novel weight for electing the cluster-heads with respect to factors such as the distance between the nodes and the BS, the neighbors and the consumed energy [11]. The drawbacks of existing approach discussed so far is proposed to be overcome in the present study of novel Energy-Efficient Distance-based Clustering integrated with adaptive Genetic Algorithm (EEDC-AGA). The EEDC-AGA algorithm considers both consumed energy and the distance for selecting the cluster-heads. The simple ant colony routing algorithm approach for WSNs is also being proposed in this study for the selection of cluster node based on energy. The entire network can then be established and updated to have cluster heads of pheromone concentration based on support for multiple path characteristics achieved by means of mutual exchange between the respective distances and consumed energy value information. Finally, with respect to the pheromone concentration, adjacent cluster is chosen as the next hop routing. Cluster based Wireless Sensor Networks is also proposed for providing continuous transmission security, thereby avoiding dangerous attacks and the node compromise attack from sinkhole malicious nodes WSNs communication.

The section 2 discusses on the proposed approach EEDC-AGA and Ant colony algorithm In Section 3, described Experiment Results and Discussion in detail then Section 4 discusses the conclusions from the study.

II. PROPOSED APPROACH

The prevention of complete authentic sensing data to reach the base station (sink) is termed as sinkhole attack which leads to intensive threat to higher-layer applications [12]. In this attack, the compromised node promotes attractive and unfaithful routing information for drawing maximum traffic. This results in an adverse management of attracting more traffic, which is formulated to the base station. The sinkhole node, thus by involving in the routing process can further launch more severe attacks such as selective forwarding, modifying or eaves dropping the packets via the route [13]. These routing attacks cause a major hindrance to the sensor nodes for these networks especially forms a serious threat to sensor networks as the sensor nodes in WSNs are deployed in open areas provided with weak computation and battery power. Energy-Efficient Distance-based Clustering integrated with Adaptive Genetic Algorithm (EEDC-AGA) considers both consumed energy and the distance for selecting the cluster-heads and the ant colony optimization algorithm is used as a countermeasure for overcoming the sinkhole attack and after that the detection process is executed by the cluster head and the base station. The ant colony optimization algorithm first finds the attack path within the network and second the detection algorithm is executed for detection of compromised node in between the attack path.

A. Energy-efficient Dynamic Clustering Approach

Transmitting data to the base station by clustering approach complexities should be avoided between sensor nodes. The clustering technique for WSNs is thus called “cluster based wireless sensor network”. With the help of dynamic clustering of the sensor nodes called multi-hop technique, in manipulating the consumption of energy. The Energy Efficient Dynamic Clustering (EEDC) algorithm is such dynamic clustering approach which provides data to multiple base stations and hence known as two tier hierarchy network. The adaptive genetic algorithm-based (AGA-based) EEDC clustering protocol is proposed in this work proves to be an excellent performance to maintain optimal probability prediction in the lifetime of the network. The proposed GA-based EEDC-AGA protocol basically has primary phases such as a preparation phase for sending the information states cluster heads, Route update Phase for node IDS and regulates geographical positions to the base station.

B. Preparation Phase

Cluster head selection is the primary step of every clustering scheme and this proposed EEDC follows the hybrid scheme for considering energy and distance among the cluster-heads. Two steps are involved in cluster-head election such as 1) local competition phase and 2) distance condition phase. To determine the optimal value of P for various base station placements, LEACH is proposed in performing setup phase of the first round. By following the cluster head selection procedure, each node is first determined for the probability of being a candidate cluster head (CCH). For this, every sensor node selects a random number r from the interval [0, 1]. If r is smaller than Th(s), based on a prescribed probability p, then the node is considered as CCH. The value of p_{set} is assumed larger in this protocol, p =0.5. Then, each node sends its ID, location information, and the status of CCH to the BS. Once the BS received the messages sent by all nodes, GA operations are performed to determine the optimal probability, p opt = k opt set /n, by minimizing the total amount of energy consumption in each round. EEDC creates a set-up phase for CHs' selection, and a steady-state phase for time slot scheduling and transmission. The energy consumption across the network could not be balanced by the rotation of cluster heads and the metric of residual energy. When a node is finalized as a cluster head, the initial energy of it gets decreased as it transmits data to BS. The node need not be a cluster head in the same round, its threshold value must be less than a random number between 0 and 1, which otherwise will have its end. This leads to shortening of the lifetime of the whole network. Hence the threshold value comprises the cluster head selection can be decreased. The consumed energy can be reduced for life time residual energy in which the proposed formula relates to

$$Th(s) = \begin{cases} \frac{p}{1-p(r\,mod(1/p))}\tan\left(\frac{E_{cur}}{E_{max}}\right) & if\ n \in G \\ 0 & otherwise \end{cases} \qquad (1)$$

Where p is the desired percentage of cluster heads (e.g., p= 0.05), r = current round, and G is the set of nodes which are not found as cluster-heads in the last $1/P$ rounds. Based on this threshold, each node will be a cluster-head at some point within $1/P$ rounds. During round 0 (r = 0), each node has a probability P is becoming a cluster-head. The nodes that are cluster-heads in round 0 cannot be cluster-heads for the next $1/P$ rounds. Thus the probability that the remaining nodes are cluster-heads must be increased as there are fewer nodes that are eligible to become cluster-heads. After $\frac{1}{P} - 1$ rounds, T = 1 for any nodes that have not yet been cluster-heads, and after $1/P$ rounds, all nodes are once again eligible to become cluster-heads.

Algorithm 1: Cluster Head Election

```
Start ()
    Specify the probability (p), number of nodes (n)
    $E_{init}(s)=E$, s=1,2, …, n;
Preparation ()
    If($E_{init}(s)>0$& rmod$(1/p_{set}) \neq 0)$
    Then
    $r \leftarrow random(0,1) and\ compute\ Th(s) given\ by$ (1)
    $if(r < Th(s))$
    then
    Add node $s$ as CCH
    Else
    Add node $s$ as sleep node
    End if
    Send To BS $(ID_u, (x_u, y_u), CCH(u)) \leftarrow$ All nodes send message to BS;
    GA in BS $(p_{opt}) \leftarrow$ Optimal probability is determined
    BS$(p_{opt}) \leftarrow$ BS broadcasts a message back to all nodes
    Result CCH(i)
```

C. Local Competition Phase

There exists competition scheme in the proposed method in which the nodes compete to be elected as the cluster head candidate. The probability of each node being selected as the cluster-head candidate has to be determined first for which the probability of the Candidate Cluster Head (CCH) indicates remainder energy of node i which represents

$$P_{ccH}(i) = \frac{EConsume(i)}{Einitial(i)} \qquad (2)$$

$(P_{CCH}(i))$ is calculated for each node and then a message is broadcast to the other nodes called CCH-Inf. This message includes the node ID, the probability$P_{CCH}(i)$, and the node degree d (the number of neighbors in a certain range of the node$i$). In the Proposed competition scheme, a competition range defined R_iShould be reasonable which means it should not be too long or too short to increase the number of clusters-head candidate advertisements. The neighbours of each node s which defines its degree $d_s = |N(s)| = \sum_{s^* \in SN,\, s^* \neq s} \{dist(s, s^*) < tr_{range}\}$ Were found. tr_{range} is the transmission range of s and s^* is the neighboring nodes. Each sensor node shows distance d to the location of the sink node and finds the minimum distance d_{min} and the maximum distance d_{max}. On this basis, sensor node calculates its competition range $R_i$for forming clusters with unequal cluster sizes. The competition range R_i is predefined as:

$$R_i = \frac{d_{max} - d_{min}}{d_{max}} \times d_{(s_i, BS)} + d_{min} \qquad (3)$$

The CCH-Inf Message format include Node ID, $P_{CCH}(i)$, D, R_i. The Fields are Node ID consists of the address of the each node, $P_{CCH}(i)$ consists of the address of the target node, D consists of neighbours in a certain range of the node i and R_i is the competition range fixed or variable as a function of distance to BS. To receive CCH-Inf message from all its neighbours, each node has to wait t seconds. The waiting timet_{wait}, should not also be too short as some nodes may not receive the message CCH-Inf, and too long as it increases the time complexity. Then node i waits for t wait seconds and receives the message CCH-Inf from all its neighbours. The probability of being elected, $P_{CCH}(i)$will then be compared with that of its neighbors. If $P_{CCH}$is found to be greater than P_{CCH} the probability of all its neighbours, then it is chosen as a cluster-head candidate for broadcasting a CCH-ADV message to higher power levels as described in distance condition step. The two nodes with the same energy in the range of R_{comp} in the network operation is only rare, however if it occurs, the node degree can be used as the tie break in the beginning of operations. This helps to reduce cluster-head candidate advertisements and time complexity. If two nodes are located in the range of R from each other, with the same residual energy, the node with the higher degree is selected as a cluster-head candidate. On the whole, if two nodes are located in the range of R_{comp} from each other and have the same residual energy and node degree, the node with higher node ID is elected as cluster-head candidate.

Algorithm 2: Local competition Local Competition ()

```
Calculate probability$P_{CCH}(i)$
Broadcast the CCH-Inf message to the $R_{comp}$range
wait for $t_{wait}$ seconds to receive CCH-Inf message
IF the CCH-Inf message is received THEN
    evaluate the received CCH-Inf messages
    IF ∀j; $P_{CCH}(i) \geq P_{CCH}(j)$ THEN
        broadcast the CCH-ADV messages to the higher power levels
    ELSEIF ∀j, $P_{CCH}(i) \geq P_{CCH}(j)$ and ∃j; $P_{CCH}(j) = P_{CCH}(i)$ THEN
        IF ∀ j; $d_i > d_j$THEN
            broadcast the CCH-ADV message to the higher power levels
        ELSEIF ∀j; $d_i \geq d_j$and ∃j; $d_i > d_j$THEN
            IF ∀j; node $\mathrm{ID_i} > node\ \mathrm{ID_j}$THEN
                broadcast the CCH-ADV messages to the higher power levels
            ELSE
                wait $t_{wait}$ seconds for the CH-ADV message
            ENDIF
        ELSE wait $t_{wait}$seconds for the CH-ADV message
        ENDIF
    ELSE wait $t_{wait}$ seconds for the CH-ADV message
    broadcast the CCH-ADV message to all the nodes in $R_c$range
ENDIF
```

D. Distance Condition Phase

Once the cluster-head candidates are elected, each cluster head candidate has to pass the distance condition to get elected as a cluster-head. Hence, each cluster-head candidate should have possible farthest distance maintained from other cluster-head candidate before being elected as the cluster-heads. For checking such distance, each elected cluster-head candidate should broadcast the information about its node ID and the $P(i)$ probability in the CCH-ADV message to the higher power levels and waits for t_{wait}seconds. During such broadcasting, the other cluster-head candidates located in those levels could know the information which can be avoided for ordinary nodes (i.e., non cluster-head nodes). However, if a cluster-head candidate comes to know the information, it calculates the distance between the sender and itself based on the signal power. If this distance is greater than or equal to a threshold distance, $D_{th}$the message is ignored otherwise the receiver cluster-head candidate checks consumed energy level of sender by$P(i)$ probability. The receiver cluster-head candidate becomes an ordinary node and sends a Join-Req message to the sender candidate cluster head for having greater energy level than its own. This message can be considered as an acknowledgement to the sender that the mentioned node satisfies the distance condition. After waiting for t_{wait} seconds, if the cluster head candidate receives no CCH-ADV message, it elects itself as the cluster-head, and then broadcasts CH-ADV message to the nodes in its range ofR_c. Similar to the previous step, if two clusters-head candidates are in the same range, the distance between them is less than D_{th} and they have the same energy, then the cluster-head candidate with the higher node ID is elected as the cluster-head. The pseudo code of the cluster-head election phase of the proposed EEDC-AGA is presented in Algorithm 1.

Algorithm 3: Distance Condition ()

```
IF the current node is a cluster-head candidate THEN
Wait for $t_{wait}$seconds to receive the CCH-ADV message
IF the CCH-ADV message received THEN
Evaluate the received messages and calculate the distance
using $\sqrt{((X_{CCH}(i) - X_{CCH}(j))^2 + (Y_{CCH}(i) - Y_{CCH}(j))^2}$
IF ∀j;$dist \geq D_{thr}$THEN
Broadcast the CH-ADV messages to all the nodes in the $R_c$range
ELSE
IF ∀j; $P_{CCH}(i) > P_{CCH}(j)$ THEN
Broadcast the CH-ADV message to all the nodes in the $R_c$range
ELSE IF ∀j; $P_{CCH}(i) > P_{CCH}(j)$ and ∃j; $P_{CCH}(j) = P_{CHH}(i)$ THEN
IF ∀j; $node\ ID_i > node\ ID_j$THEN
Broadcast the CH-ADV message to all the nodes in the $R_c$
ELSE
Send a Join-Req message to the cluster-head candidate
Send a Join-Req message to the cluster-head candidate
ENDIF
Broadcast the CH-ADV messages to the RC $R_c$range
wait $t_{wait}$ seconds for the CH-ADV message
Cluster(c);
ENDIF
```

E. Route Update Phase

This phase specifies the paths between the cluster-heads to the BS. In this study, it is assumed that the BS has no restriction (like energy constraint). A route message can be broadcasted by the BS in the network at the beginning of the phase with enough energy for enabling all the nodes can hear the message. Its distance to the BS can be estimated based on the power of the received message. Then the node produces a cost proportional to the delay at the time for the message to get to the BS, and adds this cost to the message. Each node, then forwards the message to all the nodes locating in the range of R around it. The node may receive several messages from different nodes. If multiple messages are received, the node checks the messages and selects the node with the lowest cost as its next-hop node, and forwards the message with the cost to all the nodes in the range of R c around it. If the costs of every pair of nodes in the network are determined, the shortest path among the cluster-heads can be determined by means of improved Ant colony based shortest path algorithms.

F. Ant Colony Algorithm

The ant colony optimization algorithm (ACO) is a probabilistic technique formulated based on the real ant colony behaviour for solving or reducing computational problems to finding better paths through graphs. In natural ant colony, the shortest path from nest to food is found by the mutual cooperation which can be changed with respect to environmental conditions considered as obstacles. Similarly, our ant colony optimization algorithm works on two principles first the path must be a good path which means a non obstacles path and second it must be a short one when compare with the other successful paths. This non obstacles path or optimal path is a calculated using the past data transaction information of that path from the neighbor nodes which are considered as ants. Let A and E a nest and a food source, FC as an obstacle. Because of obstacles, the ant only passes go to F or C from A to E, or by E to A, the distance between points is indicated in the Fig.1. For each unit of time, 30 ants from A to B, 30 ants from E to D, are present after leaving the hormone content quality. At the initial time, the information on the path to the BF, BC, DF, DC did not exist, as ants located in the B and E can randomly select path. From a statistical point of view, the same probability of selection of BF, BC, DF, and DC is taken. After a time unit, the path of the amount of information on the BCD is twice the path BHD information content. There are 20 ants pass by B and D to reach C, 10 ants by B and D to F till T red moments. With the passage of time, the ants will have more probability to choose the path BC. Eventually, the route chooses D from nest to food source to find the shortest path the equation is $\sum_{i=1}^{n}(xi)^2$

Where n=1, 2...n.

Calculation of Probability value$P_{ij=\frac{\tau ij}{\sum_{p=1}^{n}\tau ip}}$

Where i=1,2 j=1,2...........n. To find the shortest path

$$TG_{ij} = \frac{Max-time-S^j it+1}{Max-time-min-time\ i+1} \quad .$$

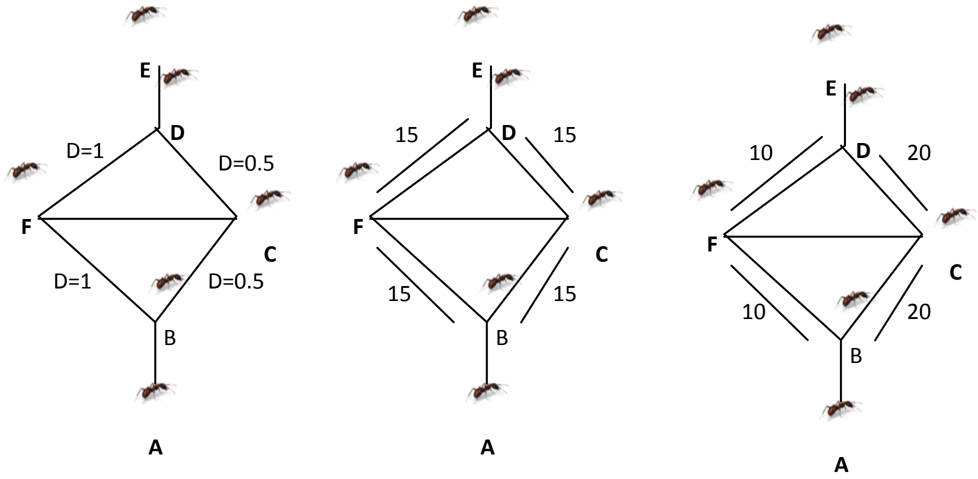


Fig.1. Ant seeks food path

G. Sinkhole Countermeasures

As said before the ACO algorithm will not select the path which has obstacles. Here obstacle means the path containing data transaction failures. In wireless network the transaction failure is quite common, so consider transaction failures as obstacle will make all paths a useless path. In comparison with sinkhole attack and the normal transaction the failure rate is much bigger so we need to fix a threshold value for considering the obstacle path. The threshold value needs to be set by the network administrator who known the network infrastructure better than others because the normal data transmission failure rate varies from one network to another network. Now we can find the obstacle path and non-obstacle paths. The non-obstacle path has nearly zero possibilities to be sinkhole path so the nodes within those paths are considered non compromised nodes. The obstacle paths have higher possibilities of containing compromised nodes. So the data transmission is carried out only through the non-obstacle paths and from those non-obstacle paths shortest path will be selected for transmission. The obstacle paths are further subjected to the detection process for verification and identification of compromised node.

H. Sinkhole Detection Process

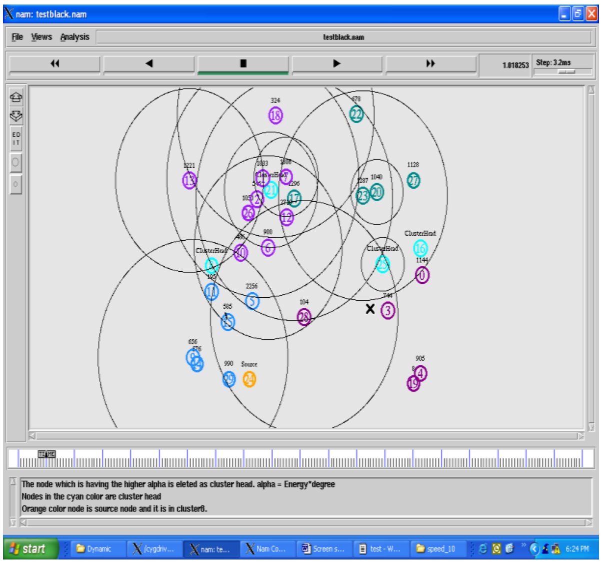
The proposed work is developed for event driven applications in which, an event is detected by a node, a control packet is sent to the BS by means of single hop communication. The following information such as the unique number of the control packet (id), the transmitter node (Nid), data packet identifier (Pid), the size of the data packet (Psize) and Packet Inter-Arrival Time are contained in the control packet. After direct transmission of this packet to the BS, the transmitter node sends the data packet, which facilitates routing table to the hop node. The data packet is routed hop by hop until it reaches the BS. When a data packet is reached to the BS, the following three situations might be occurred

- **Data arrives at BS properly:**

When data arrives at BS, it is compared to the control packet and the accuracy of the data is determined. Data arrives at BS while manipulating it means that the adversary node has changed data en route and transferred them to BS. BS detects this manipulation through comparing the data packet with the original control packet.

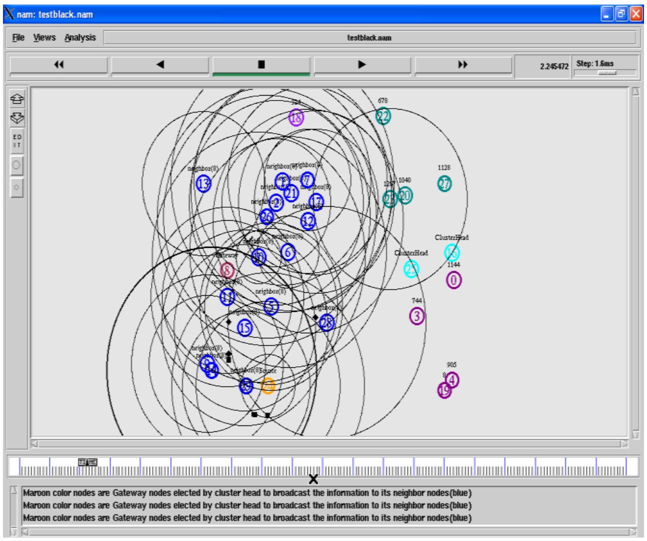
- **Data packet never arrives at BS:**

The adversary node drops the packet and does not allow it to reach BS. When BS receives the control packet, it waits for a moment to receive the original data packet. Otherwise, it detects the existence of an adversary node in the network. In the first two cases, the malicious node disrupts the network. After receiving these two situations in the network, it looks for the malicious nodes and tries to remove them from the network routing. After comprehensive the existence of a malicious node in the network, BS checks data transmission path and keeps existing nodes in its memory. Once BS detects existence of errors in a packet, repeatedly, it checks the path each time and compares the nodes kept in memory with the new path, keeping similar nodes in memory and deleting the remaining data. Accordingly, BS detects the malicious node, notifying other nodes not to transmit data to the malicious node anymore. The below figure-2, figure-3 and figure-4 shows that the election of cluster head, Sending data packet request to the neighbour node and data can be broadcast through the cluster head.



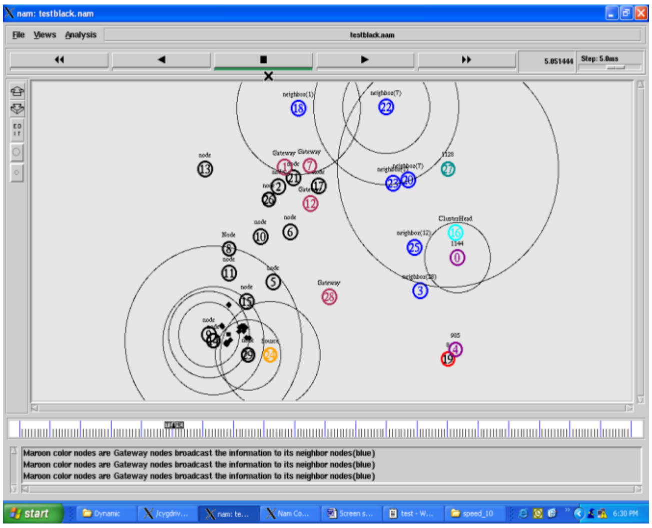
The node which is having the higher alpha is eleted as cluster head. alpha = Energy*degree
Nodes in the cyan color are cluster head
Orange color node is source node and it is in cluster8.

Fig2. Shows the election of Cluster head



Maroon color nodes are Gateway nodes elected by cluster head to broadcast the information to its neighbor nodes(blue)
Maroon color nodes are Gateway nodes elected by cluster head to broadcast the information to its neighbor nodes(blue)
Maroon color nodes are Gateway nodes elected by cluster head to broadcast the information to its neighbor nodes(blue)

Fig 3. Shows Sending data packet Request to the neighbour node



Maroon color nodes are Gateway nodes broadcast the information to its neighbor nodes(blue)
Maroon color nodes are Gateway nodes broadcast the information to its neighbor nodes(blue)
Maroon color nodes are Gateway nodes broadcast the information to its neighbor nodes(blue)

Fig 4. Shows Data can be broad cast through cluster head

III. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed algorithm is evaluated through the network simulator NS-2. Here consider a random network of 250 sensor nodes deployed in a 100m × 100m area, with a fixed BS located near the sensing. The BS has unlimited energy. Simulation time for every simulation was 10 minutes and the number of attackers from 10 to 20 attackers, 512 bytes for the packet size. Consider two metrics: the energy consumption and the memory storage. 1) Energy Consumption: the proposed protocol compared with EEDC-AGA with ACO to determine the benefits of Cluster based Wireless Sensor Networks and compared with Efficient and Secure Key Management

Scheme for Hierarchical Wireless Sensor Network (ESKMS) in terms of energy consumption.

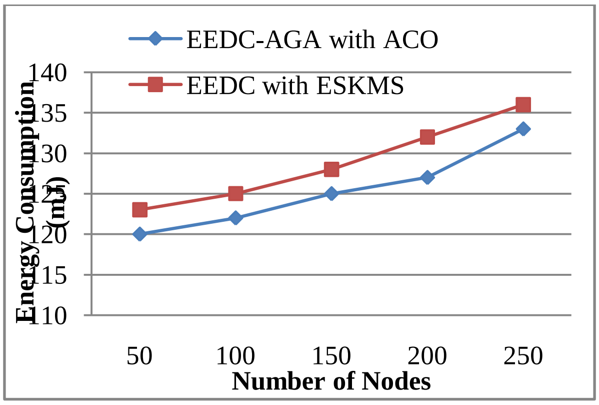


Fig.5. Energy consumption vs. number of nodes

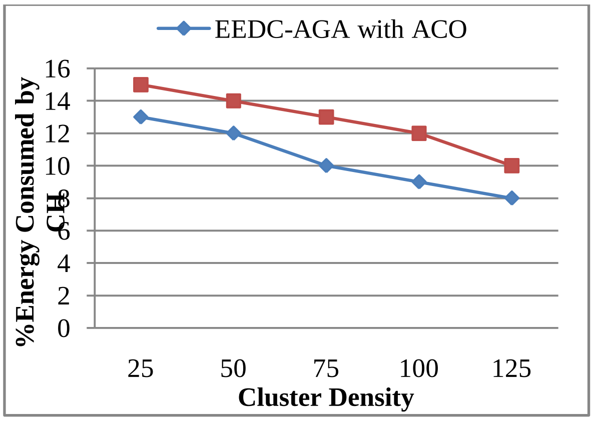


Fig.6. Average energy consumption of cluster head over cluster density

Fig. 5 shows the average energy consumption of sensor nodes following different network size. It is observed that with the increase number of nodes from 50 nodes to 250 nodes and the number of attackers from 10 to 20, the energy consumption of the EEDC-AGA protocol with ACO is slightly higher when compared with EEDC with ESKMS. Notice that the gap between EEDC with ESKMS and EEDC-AGA with ACO is extremely low and practically identical. Therefore, it could provide an energy efficient technique is improved in the proposed approach. Fig. 5 also shows that in EEDC-AGA with ACO as well as in EEDC with ESKMS, the energy of sensor nodes remains almost unchanged for all network sizes. This result was expected because in this model, cluster members communicate only with the cluster head, each ordinary node sends one message and receives one message. Fig.6 shows the average energy consumption of cluster head over cluster density. See that with the increase of the cluster size from 25 to 50 nodes in a network of 250 sensors, the average energy consumption of CH increases in EEDC with ESKMS than the proposed EEDC-AGA with ACO.

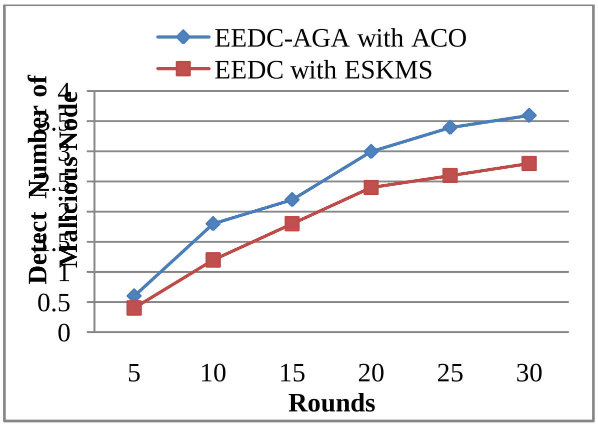


Fig.7. Number of malicious nodes Detection Comparison

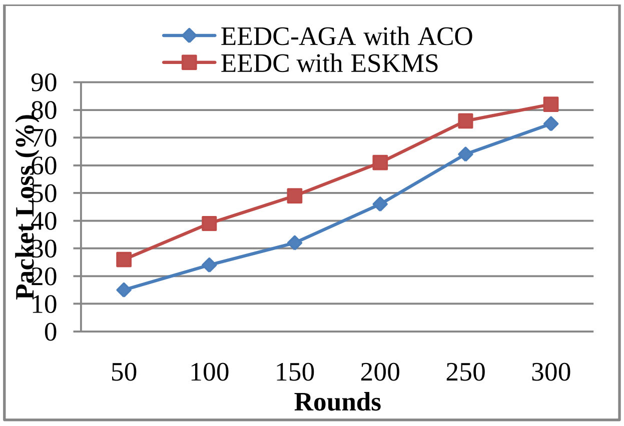


Fig.8. Packet Loss Comparison

The performance of EEDC-AGA with ACO algorithm compared with and EEDC with ESKMS algorithm with respect to the number of rounds and detection of Sinkhole nodes. As Fig.7 shows, the EEDC-AGA with ACO method detects all the Sinkhole nodes after about 8 rounds. These quality service parameters can be defined in terms of the network capacity in detecting the events during the network lifetime. A network manages to report events (or the less it loses the events) the higher is its reliability. In Fig. 8 comparisons between EEDC-AGA with ACO and EEDC with ESKMS methods in terms of the number of lost packets is shown. Obviously, the fact that a graph is higher shows that fewer packets are missed by the EEDC with ESKMS algorithm. As the Fig.8 indicates, it is evident that the EEDC-AGA with ACO algorithm is more reliable than EEDC with ESKMS algorithm in terms of packet loss.

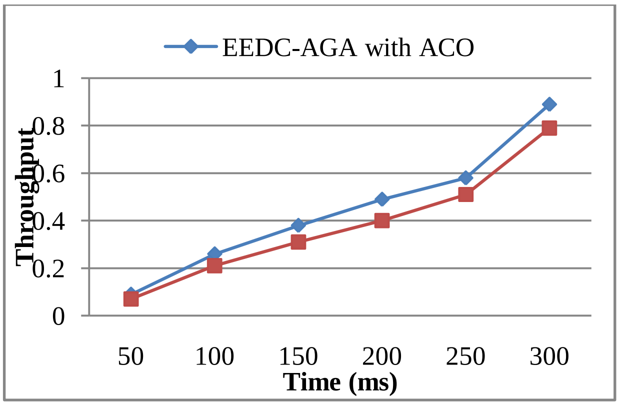


Fig.9. Throughput Comparison Results

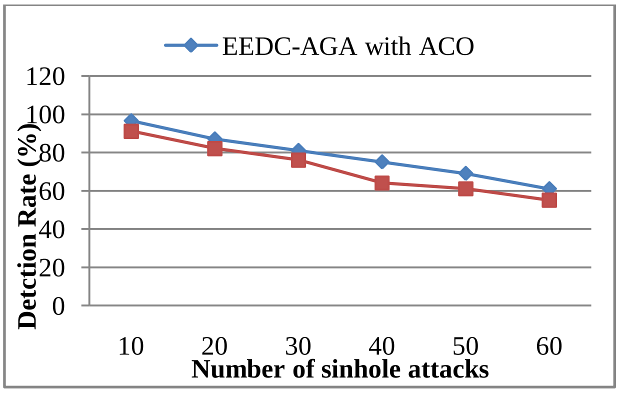


Fig.10. Detection Rate Comparison Results

Fig. 9 indicates the throughput comparison between EDC-AGA with ACO and EEDC with ESKMS methods in terms of time. As the Fig.9 depicts, when a node acts maliciously its average throughput drops compared to when it acts normally. The reason behind increase in the throughput over time is that the convergence speed of packet throws in proposed work is higher than the existing algorithm. Fig.10 depicts the percentage of malicious node detection by EDC-AGA with ACO and EEDC with ESKMS methods. When there is a more malicious nodes (sinkhole node) present in the network the success rate of EEDC with ESKMS methods degrades. This is due to the fact that the proposed work prefers to maximize its own utility and so it has to lower the rate of false positives and false negatives detection and eventually it misses more malicious nodes.

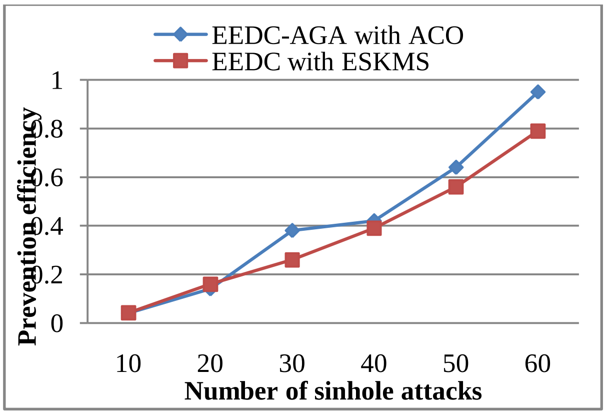


Fig.11. Prevention Efficiency Results

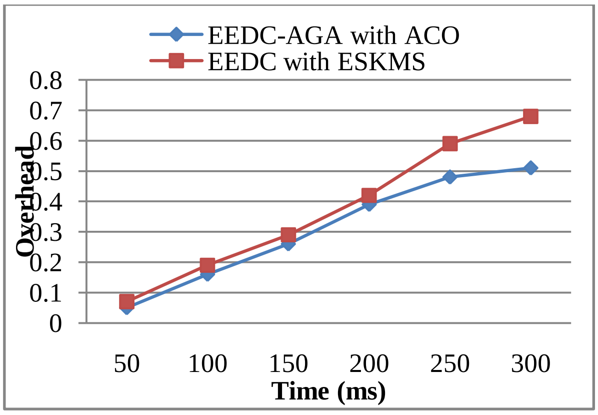


Fig.12. Overhead Comparison Results

Fig.11and Fig.12 depicts the prevention efficiency and an overhead comparison between EDC-AGA with ACO and EEDC with ESKMS methods. When there is sinkhole attack the prevention rate of the proposed work is higher than the EEDC with ESKMS method. The overhead of the proposed work is lesser and also node failure in proposed work is lesser than the existing protocol.

IV. CONCLUSION

In this work, an algorithm presented for Preventing Sinkhole attack detection in wireless sensor networks. This paper proposes an optimal clustering approach, which, in order to perform the cluster-head election, utilizes two factors: EEDC-AGA with ACO correlates the consumed energy and the distance in the cluster heads. For monitoring the best events in WSNs. By introducing an objective function to carry out dynamic clustering improves the data aggregation, reducing the energy consumption. By this way, provides continuous transmission security in neglecting dangerous attacks from malicious nodes and mitigate the node compromise attack in WSNs communication. In the proposed method, the number of lost packets decreases and the detection of malicious and adversary nodes to be removed from the network occurs more expeditiously. As the number of lost events is decreased, the energy consumption is decreased too.

REFERENCES

[1] Samundiswary. P ,Sathian. D and Dananjayan. P ,"Secured Greedy Perimeter Stateless Routing For Wireless Sensor Networks", International Journal of Ad hoc, Sensor Ubiquitous Computing, vol. 1, No. 2, pp. 9 – 20, 2010.

[2] Kalpana Sharma and M.K. Ghose, "Wireless sensor networks: An overview on its security threats", International Journal of Computer Applications, pp. 42 – 45, 2010.

[3] Rina Bhattacharya, "A comparative study of Physical Attacks on wireless sensor networks", International Journal of Research in Engineering and Technology, vol.2, Issue.1, pp. 72 – 74, 2013.

[4] Heinzelman, W. B, Chandrakasan, A.P, H. Balakrishnan, "An application-specific protocol architecture for wireless micro sensor networks," IEEE Transactions on Wireless Communications, Vol. 1, Issue 4, pp. 660 – 670, 2002.

[5] Younis O, Fahmy, Sonia, "HEED: A hybrid, energy-efficient, distributed clustering approach for ad hoc sensor networks," IEEE Transactions on Mobile Computing, Vol. 3,Issue 4, pp. 366 – 379, 2004.

[6] Haowen Chan, Adrian Perrig, "ACE: An Emergent Algorithm for Highly Uniform Cluster Formation," in Proceedings of the First European Workshop on Sensor Networks (EWSN), Vol. 29 (20), pp. 154 – 171, 2004.

[7] Murat Demirbas, Anisha Arora,Vineet Mittal, "FLOC: A fast local clustering service for wireless sensor networks," in Workshop on Dependability Issues in Wireless Ad Hoc Networks and Sensor Networks (DIWANS/DSN), 2004.

[8] Rajesh.P, Priya.S, Priyanka.R, "Modified Energy Efficient Backup Hierarchical clustering algorithm Using Residual Energy for wireless sensor networks,"International Journal of Soft Computing and Engineering, Vol. 3. Issue 2, pp. 1–5, 2012.

[9] Sang Hak Lee,June Jaa Yoo and Tae Choong Chung, "Distance-based energy efficient clustering for wireless sensor networks," Proceeding of the 29th Annual IEEE International Conference on Local Computer Networks(LCN'04), pp. 567–568, 2004.

[10] Mao Ye, Chengfa Li, Guihai Chen, Jie Wu, "EECS: An energy efficient clustering scheme in wireless sensor networks," 24 th IEEE International conference on Performance, Computing and Communication Conference, pp. 535–540, 2005.

[11] Wei Zhou, "Energy efficient clustering algorithm based on neighbors for wireless sensor networks," Journal of Shanghai University, Vol. 15,Issue 2, pp. 150–153, 2011.

[12] Ioannis Krontiris,Thanassis Giannetsos, and Tassos Dimitriou, "Launching a Sinkhole Attack in Wireless Sensor Networks; the Intruder Side,"IEEE Computer Society, pp.526 – 531, 2008.

[13] Umashri Karkikatti, Dr. Nalini N,"Detecting Sinkhole Attack in Wireless Sensor Network ",International Journal of Scientific & Engineering Research, Vol. 5, Issue 6, pp.149 – 154, 2014.