A Relative Analysis of Efficient Cluster-Basedrouting Protocols in Wireless Sensor Network

[1]N.Poornima, [2]M.Mahasree
[1]Assistant Professor,[2]Final Year B.E student,
[1,2]Department of Computer Science and Engineering
[1,2]Valliammai Engineering College
Kancheepuram

***Abstract* — In (WSN) wireless sensor networks, there are many issues related to secure transmission of data, overall energy consumption of network, aggregation of collected data etc. Clustering of nodes in a Wireless Sensor Networks is the efficient way to transmit information with the help of relevant protocols and for prolonging the life of these networks. Though the existing protocols like LEACH, Sec-LEACH, and SET-IBOOS have solutions to security threats and energy constraints, they use more complex scenarios. In this paper, we study an easily feasible protocol named Reliable Cluster Protocol - RCP which serves three purposes. 1) Misbehavior node detection and elimination using Witness table managed by all the sensor nodes in the network. 2) Extension of network's lifetime by assigning two cluster heads for each cluster. 3) Compression of collected data so as to reduce overhead in packet transmission.**

I. INTRODUCTION

Now-a-days, Wireless Sensor Network (WSN) is the emerging area of interest in Network's research field. These networks are widely used in places where direct recording of data is difficult [1]. Examples include detection of seismic activity of volcanoes, climatic conditions, military purposes, monitoring of health–care systems and many other security applications. A Wireless Sensor Network consists of many sensor nodes which are used to collectively sense, gather and aggregate information from their surroundings. There is variety of sensors available.

The aggregated data are transmitted to the user through base station which is the central authority. In order to send the gathered data to base station, the sensor nodes should be organized .Thus, a protocol provides the approach to organize and transmit those collected data. The performances of WSN are based on protocol used. A routing protocol provides the best path between sender and receiver nodes [2].

Clustering is the efficient method for routing protocols to reduce power consumption and extend the network's lifetime. Since sensor nodes are battery operated devices energy consumption should be considered.

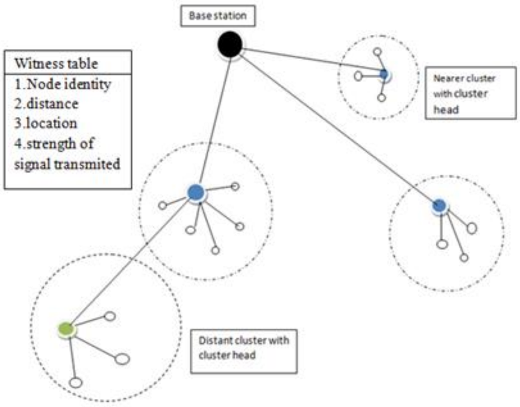

Fig. 1 Cluster formation in WSN

II. TYPES OF ATTACKS

The existing protocol is effective against three types of attacks. They are selective forwarding, sinkhole attack and hello flood attacks [3].

1) Selective Forwarding Attack: In this type of attack, the node may refuse to forward certain packets from other nodes and drop them. So, data is lost during communication.

2) Sink-hole attack: The attacker in the network pretends with high capability resources, by which announces a short path to destination to attract the data packets. After receiving the packets, the attacker node drops them.

3) Hello Flood Attack: Strong hello messages are broadcasted by attackers with high transmission power. Other nodes may think this message is nearest to them and send packets through this node.

So, our proposed protocol defends the network mainly against Sybil attack. The Sybil node is one which presents multiple identities on the same node and attracts all other nodes to send data packets to it.

This paper can be further organized as following: Section II describes the existing protocols with their processing steps and their drawbacks. Section III explains our proposed (RCP) Reliable Cluster Protocol for Sybil attack and aggregation techniques. Section IV shows the experimental analysis of RCP with respect to other protocols and Section concludes the paper.

III. LITERATURE SURVEY

A. LEACH:

Low energy adaptive clustering hierarchy is the first basic protocol proposed by Heinzelman .The main objective is to prolong the lifetime of Wireless sensor network [4]. For this reason, the energy should be spread evenly among sensor nodes in the network. So, the energy of a node or group of nodes may not drain very often. In other words, energy consumption of sensor nodes while communicating with BS is spread to all the nodes in the network. There are two phases in LEACH protocol.

Set-up phase

Steady-state phase

In set-up phase, the CH is elected by the following random method.

$$T = \frac{p}{1-p[n_r \; mod \; 1/(p)]} \text{ ; if n belongs to G}$$

$$T = 0 \qquad \text{; otherwise}$$

T = threshold value

p =probability that a node is selected as a cluster head

n_r = number of round.

G = set of unselected nodes as CH in the last 1/P rounds.

B). STEPS INVOLVED IN LEACH

Step 1): Each node generates a random number between 0 and 1.If this number is less than threshold, then node becomes CH.

Step 2): After becoming cluster heads, the nodes broadcast messages to all nodes to inform their status.

Step 3): On receiving this message, non-cluster head nodes decide which CH to join based on receiving signal strength of these messages.

Step 4): After this, CH create Schedules and send to all the nodes in cluster .the nodes send data to their respective CH then CH aggregate and send data to base station.

Step 5): This completes one round, after this, Ch rotation takes place i.e., CHs are re-generated to form new clusters.

C). DISADVANTAGES:

Since it is a single-hop and no Inter-cluster communication, it fails for large scale networks.

Since cluster head are elected randomly, we cannot assure that each cluster does posses a cluster head. So, possibilities of a node having low residual energy may be elected as cluster head as if the node with higher residual energy.

Repetition of same node as CH

B. Sec-Leach:

Here we use random key pre distribution to enable node- to node authentication in LEACH [5]. Before the network deployment, a large pool of keys and their IDs are generated.

From this key pool, each sensor node is assigned with a ring of keys.

The following are also generated:

(i)ID for each sensor using Pseudo Random Function.

(ii) key pool

(iii)pair –wise key shared with BS.

A). SET UP PHASE:

Step 1): The self-elected CH broadcasts its ID and nonce (number used once).

Step 2): Remaining sensors computes the set of CHs keys IDs and choose the nearest CH and send a join request message.

Step 3): join request messages contains MAC produced by the sharing key, nonce from CHs broadcast, the id of key.

Step 4): so, CH knows which key to use to verify the MAC and send the time slot schedule to the nodes that choose to join their clusters.

B). STEADY STATE PHASE

Step 1): Data communication between nodes-to-CH is protected using the same key they use it for join request message.

Step 2): To prevent replay attacks, nonce (number once) is included in the MAC.

Step 3): CH can verify the sensed MAC's reports and perform aggregation.

Step 4): The results along with a MAC including counter is sent to Base Station protected by symmetric key shared between them.

C. SET-IBOOS:

This protocol namely Secure and Efficient Transmission-Identity Based Online and Offline Signature involves four operations for authentication and secure transmission [6].

A) STEPS

Setup: The BS gives a Master Key MK and parameters for the private key generator to all sensor nodes.
Extraction: With an Id, a sensor node generates a private key Pk using Mk
Offline signing: With public parameters and time stamp t, the CH node creates an offline signature OffSig, and reports it to the leaf nodes in its cluster prior to communication.
Online signing: From the private key Pk, OffSig and message M, a sensor node generates an online signature OnSig.
Verification: Given Id, M, and OnSig, CH node outputs "accept" if OnSig is valid, and outputs "reject" if OnSig is invalid.

B) DISADVANTAGES IN EXISTING SYSTEM:

Public key operations may be applicable in wireless sensor networks. But, private key operations are still too expensive in terms of computations and energy cost to accomplish in a sensor node.
Symmetric key cryptography is superior to public key cryptography in terms of speed and low energy cost. But key distribution schemes are not perfect. They lack in efficiency and flexibility. Also they increase complexity of networks.

PROPOSED PROTOCOL

To detect any misbehavior in sensor nodes, we propose the method of monitoring sensor nodes by its neighbor sensor nodes. This can be achieved by maintaining a table called Witness table that contains abnormal activities of sensor nodes. It contains information about IDs, distance, location and signal strength of each and every sensor in a wireless network. This table will be updated periodically.

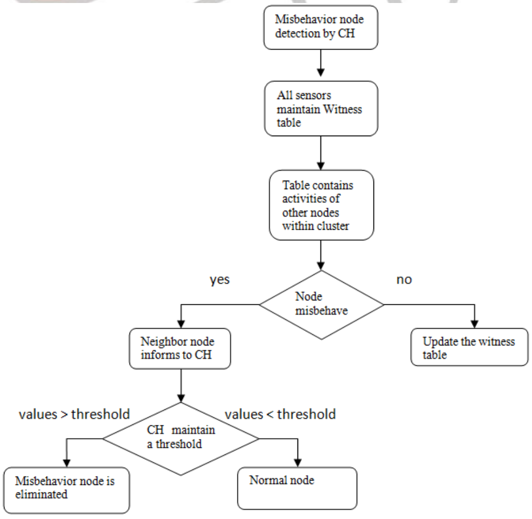
Misbehavior node detection by CH
All sensors maintain Witness table
Table contains activities of other nodes within cluster
yes
no
Node misbehave
Neighbor node informs to CH
Update the witness table
values > threshold
values < threshold
CH maintain a threshold
Misbehavior node is eliminated
Normal node

Fig.2. Data flow diagram of RCP

A) FEATURES

In our proposed protocol, the security threat for Sybil attacks is studied and measures are taken to reduce the effect of such attacks on node so as to show the compatibility of our proposed protocol against the existing protocols [7] .The Sybil attack is said to be happened in a Sensor Network, when a node pretends to be another node by using many identities (IDs) to access the control over the network and creates lots of misinterpretation by other sensor nodes in the network. However, the physical position of any Sybil node is same irrespective of number of identities that it claims to be. Therefore it is absolute to doubt any sensor node in the Wireless Network as malicious nodes category (Sybil node). In addition to absoluteness of Sybil node, we can confirm the presence of such Sybil node when count of node identities is greater, which is rare for a sensor network to consists of many sensor nodes in one place.

In a wireless sensor network of homogeneous nodes, a node is assumed to be observing neighbor nodes within its cluster. This is possible by calculating the node’s location, distance and whether the node is within the transmission range or not [8].

B) STEPS

Step 1): Whenever data is sent to a destination node, the receiving node examine whether it can monitor the sending node or not.

Step 2): Let us denote the transmission range of selected node as T_R, the accurate distance between node that is being observed and the observer node as D, location of node as L and the signal strength of the node that is being observed as SS_N.

Step 3): The distance between two nodes can be estimated as follows:

$$D = \sqrt{(\mathrm{x}_2 - \mathrm{x}_1)^2 + (\mathrm{y}_2 - \mathrm{y}_1)^2}$$

Where $(x_{1,}y_1)$ and $(x_{2\,,}y_2)$ are the co-ordinates of the source and destination nodes.

Step 4): With this distance D and location of the node in the form of co-ordinates, we can calculate the SS as follows:

$$SS_r = \frac{SS_s * C}{D^b}$$

C =constant, b= attenuation factor (if any loss).

Thus based on this location of a node and its distance, if the values of both parameters are unique then location and distance of those nodes are true and they lie within the transmission range R [9].

C). DUAL CLUSTER HEADS

Within a cluster we assign two cluster heads: One in sleep mode and another in active mode. Whenever the CH1 loses energy it sends request message to CH2 to awake it. Now, CH2 takes the position of CH1 and sends broadcast message about changes in CH, to all other nodes in the network.

D). DATA AGGREGATION

(i). Data aggregation is the combination of data from different sources and can be implemented in a number of ways [10]. Example: if node A and node B are sending same or similar kind of data, CH will not transmit both copies to the base station. This is known to be duplicate suppression in Wireless Networks.

(ii). Energy during packet transmission is saved by data aggregation. The number of transmissions depends on diameter of set of sensor nodes. Using these methods redundant data can be removed. So, energy and bandwidth are saved.

(iii). Robust aggregation-Robust aggregation technique is followed by taking values of all sensor nodes consecutively in batches for several times. In first stage, observations of two parameters are calculated .one parameter is bias while another parameter is variance.

These observed values are then subtracted from actual sensor node’s readings.

In this technique, the malicious node tries to apply another compromised sensor node. For making the simple average of every sensor node readings and to skew these values, the attacker makes use of x-1 sensor nodes to sequentially form the outlier readings.

A wrong value closer to the average skewed value is included by the assumption that the last sensor node indicated is x-1. Thus, these kinds of attacks make Iterative Algorithms to take up a wrong value as the average value.

To avoid confusions with accuracy in iterative algorithms, we propose a method of tabulating several sets of data in different values of different compromised sensor nodes.

By this method aggregation is done effectively and accurately without including the data from malicious nodes.

One important factor to note in this method is that similar to few calculation techniques of aggregation; our proposed method also uses 0 as initial assigned weight.

IV. IMPLEMENTATION

A.NETWORK SIMULATOR

Network simulator (version 2.34) is known as NS2 is simply an open-source event-driven tool that has useful for dynamic nature of communication networks. It provides way of specifying network protocols and simulating nodes and their corresponding behaviors. NS2 has continuously gained tremendous interest from industry, academia and government. Now it contains modules numerous network components such as routing, transport layer protocol, and application.

B. ADVANTAGES OF NS2

It does not require costly equipment

Complex scenarios are tested easily.

Results can be quickly and more ideas can be tested in a short time frame.

It has more supported protocols and platforms.

Most popularity and modular among all simulator tools.

C. PERFORMANCE METRICS

To analyze the performance of the proposed protocol RCP, we take into account the important metrics-Number of packets delivered and networks energy consumption. With these metrics, we evaluate and compare RCP with SET-IBOOS protocol.

Number of packets: The time period with which packets are delivered.

Lifetime of a sensor node

Network's energy consumption:

This metric defines the total amount of energy that is consumed in a Wireless Sensor Network. We produce the energy consumption of sensor protocols thus showing the variations.

D. SIMULATION RESULTS

In the simulation experiments, 100 nodes are created with two cluster heads in each cluster. BS is fixed in the same area all the sensor nodes sense the events periodically and transmit the data to cluster head and then forwarded to the BS.

Fig. 3 shows network lifetime i.e. the time for delivering data packets is taken as measuring factor. In our experiment we define a round as period when the Base Station successfully receives the sensed data from its cluster heads and sensor nodes.

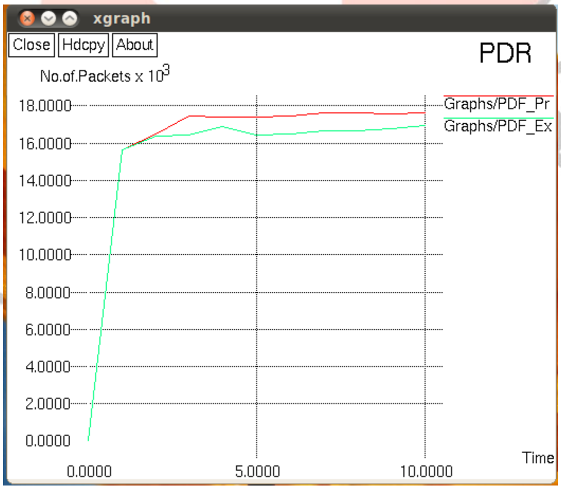

Fig.3. Graph for Time Vs No. of packets

The comparison is made for system lifetime using RCP versus SET .The results demonstrate that the network lifetime of RCP is mentionably longer than others .The time of first node loses its energy is shorter for LEACH because of security overhead in computation cost.

Fig.4. demonstrates the energy consumption of all sensor nodes in the network and its balancing capacity. Here RCP outperforms SET-IBOOS protocol.

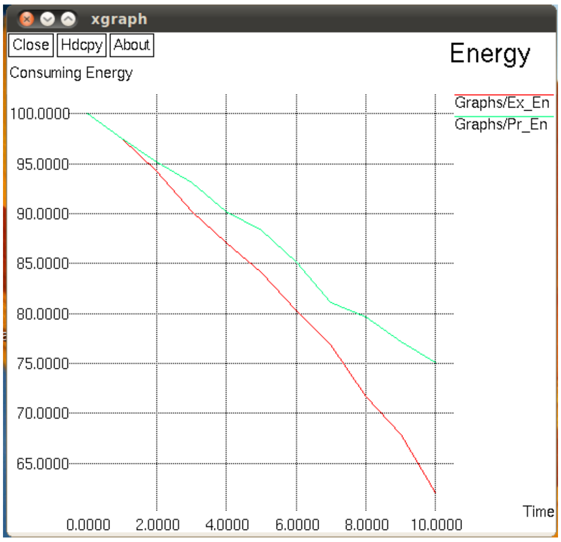

Fig.4. Graph for Energy comparison

We consider a Scenario where the sensor nodes maintain witness table and periodically sends caution messages to sink node.

RCP has average lifetime of network as 90.1 rounds, whereas those of LEACH & SET are 54.2 and 80.7 rounds respectively. Even though SET provides multi-hop communication between cluster heads and Base Station, RCP outperforms it by uniformly distributing clusters with shortest communication distance between node & its CH

Network will not be active when less than 50% sensors are available networks. Our protocol has shortest communication distance with higher possibility of active nodes it improves network's lifetime up 65% compared to LEACH & SET.

V. CONCLUSION

In this paper, we presented RCP, a protocol for securing node-to-CH communication in Cluster-based Wireless Sensor Networks. By the exploitation of node cooperation, we propose to find the position of the suspect node by the SS further group the identities with similar SS together to identify the Sybil attack. Also, we can save lifetime of cluster by the introduction of dual cluster heads in every cluster.

VI. REFERENCES

[1] T. Hara, V.I. Zadorozhny, and E. Buchmann, "Wireless Sensor Network Technologies for the Information Explosion Era ", Studies in Computational Intelligence, vol. 278. Springer-Verlag, 2010.

[2]Nikhil D, Mrs. Smitha ," Reliable Data Transmission for Cluster based Wireless Sensor Networks ", IJTRE., vol. 1 , pp. 1200-1202 ,2014.

[3] K. Pradeepa, W.R. Anne, and S. Duraisamy, "Design and Implementation Issues of Clustering in Wireless Sensor Networks," Int'l J. Computer Applications, vol. 47, no. 11, pp. 23-28, 2012.

[4] Vinoda. B. Dibbad, and C. M Parameshwarappa," A secure data transmission for cluster based wireless sensor netwok using LEACH protocol", ijircce , vol. 2 , pp. 5145-5150, 2014.

[5] A.A. Abbasi and M. Younis, "A Survey on Clustering Algorithms for Wireless Sensor Networks," Computer Comm., vol. 30, nos. 14/ 15, pp. 2826-2841, 2007.

[6] J.Liu et al., "Efficient Online/Offline Identity-Based Signature for Wireless Sensor Network," Int'l .Information Security,vol.9,no.4, pp. 287-296, 2010.

[7] P.R.Vamsi, K.Kant, "A lightweight Sybil attack detection framework for Wireless Sensor Networks," in Contemporary computing(IC3), 2014 Seventh International conference on ,pp. 387-393, IEEE, 2014.

[8] Wei and Y. Guan, "Lightweight location verification algorithms for wireless sensor networks," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 5, pp. 938–950, 2013.

[9] H. Wymeersch, J. Lien, and M. Z. Win, "Cooperative localization in wireless networks," Proceedings of the IEEE, vol. 97, no. 2, pp. 427–450, 2009.

[10] Watfa, M., Daher, W. & Al Azar, H., "A sensor network data aggregation technique", International Journal of Computer Theory and Engineering, vol. 1, no. 1, 2009, pp. 19-26.