International Journal of Computing Science and Information Technology, 2016, Vol.4, 05-08
ISSN: 2278-9669, January 2016 (http://ijcsit.org)

PREDICTION AND LOAD BALANCED CLUSTERING FOR MOBILE DATA GATHERING IN WIRELESS SENSOR NETWORK LIFETIME EXTENSION

R.SHANMATHI1, J.DEEPIKA2
[1]PG Scholar, SONA COLLEGE OF TECHNOLOGY
[1]ravichandranshanmathi@gmail.com
[2]AP/IT, SONA COLLEGE OF TECHNOLOGY
[2]jdeepikait@gmail.com

Abstract

A three types of layer is proposed for Mobile data collection in wireless sensor networks, which includes the sensor layer, mobile collector layer, and mobile cluster head layer. The sensor layer is the bottom and basic layer. At the sensor layer, load balanced clustering algorithm is proposed for sensors to self-organize themselves into clusters. At the cluster head layer, Cluster head is selected with the LEACH protocol. Right after the cluster heads are elected, the nodes synchronize their local clocks via beacon messages. The multiple cluster heads in a CHG coordinate among cluster members and collaborate to communicate with other CHGs. At the mobile collector layer, SenCar collects the data from the clusters. Upon the arrival of SenCar, each CHG uploads buffered data through MU-MIMO share and synchronizes its local clocks with global clock on SenCar through acknowledgement messages. To gather data as fast as possible, SenCar should stop at points inside a cluster that can achieve high capacity. Since SenCar has pre-knowledge about the place of polling points, it can find a good trajectory by attempt the shortest route that visits each polling point exactly once and then returns to the data sink. Suppose if the SenCar turns out to be an intruder then the network is subject to security attacks therefore go for Elliptic Curve Cryptography algorithm. This can achieve high security in CHGs by Elliptic Curve Cryptography algorithm.

Key Words: Wireless Sensor Networks, Low Energy Adaptive Clustering Hierarchy, Elliptic Curve Cryptography, Cluster Head Groups

1. . Introduction

WSNs are composed of set of tiny sensor nodes, which can effectively monitor their all-around environment. Due to the wide potential applications in environmental monitoring, healthcare, battlefield surveillance, other forecasting.

WSNs have advantages over wired networks, such as simple, ease of deployment, extending transmission range, and self-organization. A distributed algorithm organize sensors into clusters, where each and every cluster has many cluster heads. In contrast to clustering techniques balances the load of intra-cluster aggregation and activate dual data uploading between multiple cluster heads and the SenCar. Second, multiple cluster heads within a cluster can collaborate each other to perform energy efficient. Different from other hierarchical schemes, in this algorithm, cluster heads does not relay data packets from other clusters, which effectively make the burden of each cluster heads. Instead, forwarding the paths among clusters are only used to route small number identification of cluster heads to the mobile collector for effective use of the data collection.

LAYERS IN MOBILE DATA COLLECTION

A three types of layer is used for gathering mobile data's in wireless sensor networks, they are

- Sensor layer,
- Cluster head layer, □ Mobile collector layer.

II. PROBLEM DEFINITION

1. Small storage capacity,
2. Limited computation
3. Low communication bandwidth,
4. Limited device energy.

In terms of energy, all nodes in a sensor network are battery-driven. Therefore reducing the energy consumption in sensor nodes and thereby increasing the network lifetime has become as major issue in WSN.

III. CLUSTER BASED ROUTING PROTOCOL

The protocol divides the number of nodes of ad hoc network into a number of overlapping or disjoint multi hop diameter clusters in a distributed manner. A cluster head is choose to maintain cluster membership data's. Inter cluster routes are dynamically using the cluster membership data kept at each cluster head.

By clustering nodes into groups, the protocol minimizes the traffic during route discovery and speeds up this process as Cluster Formation.

The target of Cluster Formation is to force some kind of structure or hierarchy in the otherwise completely not controlled ad hoc network. The algorithm is a difference of the simple lost ID clustering algorithm in which the node with a lost ID among its neighbors is elected as the Cluster Head.

IV. INTER-CLUSTER ROUTING

The cluster formation and routing process added to the protocol:

- Route shortening
- Local repair.

Both features make use of the multi hop topology information enabled by each node through the broadcasting of HELLO messages. The route shortening mechanism continuously shortens the route of the data packet being forwarded and informs about the effective route. Local route repair broken source route and avoids route rediscovery by the source.

1) CLUSTER MEMBER

All nodes within a cluster are called members of this cluster.

2) GATEWAY NODE

In any node a cluster head use to communicate with a next cluster is called a gateway node.

Advantage

- Fully distributed operation.
- Less flooding traffic during the constant change route discovery process.
- Broken routes could be repaired locally without discover again,
- Sub-optimal routes could be make as they are used.

V. METHODOLOGY

An Exponentially Lighted Moving Average (EWMA) is occupied for on-line updating nodal contact probability. Lighting factors which decrease more and more rapid. The lighting for each older data point decreases exponentially, giving importance to recent process while still not discarding older observations entirely. True contact probability. A set of functions includes Sync (), Leave () and Join () are used to form clusters and select gateway nodes based on nodal contact expectation. The cluster table consists of this fields includes, Cluster ID, Time Stamp, and, Node ID Contact Probability. Each entry in the table is inserted upon meeting with another node, by using the online updating scheme. The gateway table used for routing includes Cluster ID, Gateway, Contact Probability, and Time Stamp.

3) NODAL DELIVERY PROBABILITY

The nodal delivery probability indicates the deliver data messages to the sink. The delivery probability of a sensor i, is updated as follows,

$$E_i = \begin{cases} (1-\alpha)[E_i] + \alpha E_K, & \text{Transmission} \\ (1-\alpha)[E_i], & \text{Timeout,} \end{cases}$$

Where E is the delivery probability of sensor i before it is updated, α is the delivery probability of node k and Ei is a constant employed to keep partial memory of historic status.

4) DISTRIBUTED CLUSTERING ALGORITHM

The set of functions in the distributed clustering algorithm including Leave, Sync, and Join is following.

5) SYNC

The Sync () process is call when two cluster members meet. It is designed to exchange and operate at the same time two local tables. The synchronization process is important because each node separately gain network parameters, which may differ from other nodes.

The Time Stamp field is second hand for the information of the network to deal with any conflict.

6) LEAVE

The node with low stability must leave the cluster. The stability of a node is defined to be its minimum communicating probability with cluster members.

It indicates the state of the node will be excluded from the cluster due to low communicating probability.

Use abbreviations in the title or heads unless they are unavoidable.

7) JOIN

The Join () process is employed for a node to connect better cluster or to merge two separate clusters.

A node will merge the other cluster if

- It moves membership check for all ongoing members.
- Its solidity is become well with the new cluster.

By merging new cluster, it will duplicate the gateway table from the other node and update its cluster ID.

8) ONE-HOP INTER-CLUSTER ROUTING

If nodes are not in the same cluster, one node look up gateway information to another node cluster in its gateway table. If an entry is found, the first node send the data message to that gateway. After receiving the data message, the gateway will send to another node.

9) MULTI-HOP INTER-CLUSTER ROUTING

If one Node does not have any information about neighbor Node, the data transmission needs a multicluster routing process. Low connectivity environment, with extremely high packet dropping probability, on-demand routing protocols will not work explicitly. In the protocol, every gateway node builds a Cluster

Connectivity Packet (CCP), and issues it to rest of the gateways in the network.
The CCP of a Gateway comprises its cluster
Identification and a list of clusters to which it serves as gateway along with corresponding communicating probabilities. Such information can be readily get from the gateway table.
Once a gateway node collects an enough set of CCP's, it build a network graph. Every vertex in the graph use for a cluster. A link connects two vertices when there are gateways between these two clusters.

VI. ELLIPTIC CURVE CRYPTOGRAPHY

Elliptic curve cryptography (ECC) is an alternative process for implementing public key cryptography. Public-key algorithms create sharing keys for large numbers of entities in a complex information system. Other algorithms such as ECC, RSA is based on discrete logarithms that is more difficult to challenge at key lengths.

10) ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

ECC depends on the discrete logarithm problem. Let A and B be two points on an elliptic curve such that kA = B, where k is a scalar. Given A and B, it is hard to compute k. k is the discrete logarithm of B to the base A. The main operation is point multiplication. Multiplication of scalar k * A to achieve another point B

11) POINT ADDITION

Point addition is nothing but addition of two points J and K on an elliptic curve to obtain other point L on the same elliptic curve.

12) POINT DOUBLING

Point doubling is known as addition of a point J on the elliptic curve to obtain another point L on the same elliptic curve.

13) ELLIPTIC CURVE DIGITAL SIGNATURE

Algorithm Signing
For signing a message m by sender S, using S's private key d
1. Calculate e = HASH (m),

Where HASH is a cryptographic hash function, such as SHA-1

2. Select a random integer k from [1, n − 1]

3. Calculate r = x1 (mod n), Where (x1, y1) = k * G.

If r = 0, go to step 2
4. Calculate s = k − 1(e + dr) (mod n). If s = 0, go to step 2

5. The signature is the pair (r, s)

14) ELLIPTIC CURVE DIGITAL SIGNATURE

Algorithm Verification
For A to authenticate B's signature, A must have B's public key Q
1. Verify that r and s are integers in [1, n − 1]

2. Calculate e = HASH (m)

3. Calculate w = s −1 (mod n)

4. Calculate x1 = ew (mod n) & x2 = rw (mod n)

5. Calculate (a1, b1) = x1*G + x2*Q

6. The signature is valid if a1 = r (mod n)

15) ELLIPTIC CURVE DIFFIE HELLMAN

A pair of key consisting of a private key (d) and a public key (Q)
Q = d * G
(G is the generator point, an elliptic curve parameter).
Let (dA, QA) be the private key - public key pair of A and (dB, QB) be the private key – public key pair of B. It is not possible to get the shared secret for a third party.

16) PACKET DROP

Drop = (Number of Packets Received) - (Number of packets Sent)

a) VII. CONCLUSION

Mobile data collection employs distributed load balanced clustering for sensor self- organization, adopts collaborative inter- cluster communication for energy-efficient transmissions among CHGs, uses dual data uploading for fast data collection, and optimizes SenCar's mobility to fully enjoy the benefits of MU-MIMO. The sensor nodes are energy constrained and have limited lifetime, energy consumption of sensor nodes research framework is to provide a better approach to reduce the energy consumption in wsn's and to prolong the network lifetime. It is achieved by two main approaches: 1) Clustering-based: sensor nodes form clusters and elect the cluster heads in such a way to improve energy efficiency, and 2) prediction based: energy-aware prediction is used to find trade-off between communication and prediction cost.

B. REFERENCES

[1] Darrel Hankerson, Julio Lopez Hernandez, Alfred Menezes, Software Implementation of Elliptic Curve Cryptography over Binary Fields.
[2] M. Brown, D. Hankerson, J. Lopez, A. Menezes, Software Implementation of the NIST Elliptic Curves over Prime Fields.
[3] Certicom, Standards for Efficient Cryptography, SEC 1: Elliptic Curve Cryptography.
[4] Certicom, Standards for Efficient Cryptography, SEC 2: Recommended Elliptic Curve Domain Parameters.

[5] D.Gong, Y. Yang, and Z. Pan, "Energy-efficient clustering in lossy Wireless sensor networks," J. Parallel Distrib. Comput.

[6] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks".

[7] Jea, A. A. Somasundara, and M. B. Srivastava, "Multiple controlled mobile elements (data mules) for data collection in sensor networks.

[8] K. Xu, H. Hassanein, G. Takahara, and Q. Wang, "Relay node deployment strategies in heterogeneous wireless sensor networks.

[9] Lee, S. Park, F. Yu, and S.-H. Kim, "Data gathering mechanism with local sink in geographic routing for wireless sensor networks.

[10] M. Ma and Y. Yang, "SenCar: An energyefficient data gathering mechanism for large- scale multihop sensor networks.

[11] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol.