A Review On Energy Efficient Secure Routing For Data Aggregation In Wireless Sensor Networks

K.Sasikala[1], M.Geetha[2]

[1]M.Phil Scholar, [2]Associate professor,
Dept. of Computer Science, Muthayammal College of Arts &Science, Rasipuram, TN, India

Abstract: **- Wireless sensor nodes challenges are supply maximum lifetime and provide secure communication to network. It has small in size and limited processing capability with very low battery power. This restriction of low battery power makes the sensor network prone to failure. So it conserves battery power or energy with some security considerations. The energy is mainly consumed for three purposes: data transmission, signals and hardware usage. Most of energy consumption happens because of data transmission. The data transmission can be optimized by using efficient secure routing and effective ways of data aggregation. Data aggregation technique maximize the lifetime of wireless sensor network by decreasing the number of packets to be sent to sink or base station. Cluster-heads implement data aggregation for distinct data in encrypted form is transmitted from sensor nodes to the base station via cluster-heads. Cluster heads no need of information about sensor data.**

Keywords: **- Sensor network; secure routing, Data aggregation; Cluster;**

I.INTRODUCTION

A Wireless Sensor Network (WSN) consist group of independent nodes, and one or more base station (BS) or sink. Sensor networks are used many of environments for commercial, civil, and military applications such as surveillance, vehicle tracking, climate and habitat monitoring, intelligence, medical, and acoustic data gathering [1]. Sensor nodes sense the physical environment and send the data in the form of signals to the base station. These nodes can collect and pass data to the sink. Sensor nodes have less amount of energy so energy conservation is the important factor in sensor network [2]. Most of them sense the environment and send the data to the base station and at base station and we have to combine all the information for the desired output. If we aggregate the data before reaching the base station we can potentially decrease the number of packets in the network so we will have to send less number of packets to base station and that can save the energy of sensor nodes.

Data aggregation techniques explore how the data is to be routed in the network as well as the processing method that are applied on the packets received by a Node. They have a great impact on the energy consumption of nodes and thus on Network efficiency by reducing number of transmission or length of packet [3]. Data aggregation is defined as the process of aggregating the data from multiple sensors to eliminate redundant transmission and provide fused information to the base station.

Data aggregation usually involves the fusion of data from multiple sensors at intermediate nodes and transmission of the aggregated data to the base station (sink). Data aggregation attempts to collect the most critical data from the sensors and make it available to the sink in an energy efficient manner with minimum data latency. There are several factors which determine the energy efficiency of a sensor network such as network architecture, the data aggregation mechanism and the routing protocols [4-5].

II. TECHNIQUES OF DATA-AGGREGATION IN WIRELESS SENSOR NETWORKS

To minimize energy consumption, routing techniques proposed in the literature for WSNs employ some well-known routing tactics as well as tactics special to WSNs, e.g., data aggregation and in-network processing, clustering, different node role assignment, and data-centric methods were employed. Depending on the network structure, data aggregation techniques has been classified [6].

A. Flat Networks based data aggregation

Data aggregation in flat network environment implements the data routing such as the sink transmits a query message to the sensor nodes, for instance, via flooding and sensors which have data matching the query send response messages back to the sink.

i). Directed diffusion: It creates for avoid unnecessary operations of network layer routing in order to save energy. It suggests the use of attribute-value pairs (name of objects, interval, duration, geographical area, etc) for the data and query messages the sensor nodes on demand basis by using those pairs. Few directions can be established so that one of the best is selected by reinforcement. The sink resends the original interest message through the selected path with a smaller interval hence reinforces the source node on that path to send data more frequently. Figure. 1 shows the data delivery of Directed Diffusion network.

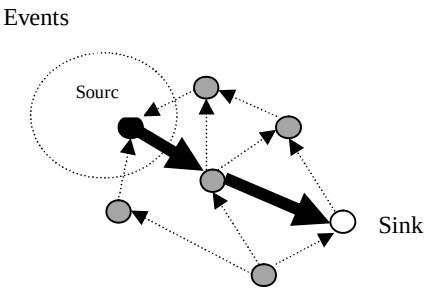

Figure 1: Data delivery

Within the flat network communications are neighbor-to-neighbor with no need for a node addressing mechanism. Each node can do aggregation and caching, in addition to sensing. Caching is a big choice for energy efficiency and delay. The Direct Diffusion is highly recommended for energy efficient. However, directed diffusion cannot be applied to all sensor network applications since it is based on a query-driven data delivery model. [7][8]

ii) SPIN (Sensor Protocols for Information via Negotiation): In this Data transmission are among sensor nodes via a data advertisement mechanism, each node upon receiving new data, advertises it to its neighbors and interested neighbors, which mean those nodes do not have the data, retrieve the data by sending a request message. SPIN used for some important needs such as redundant information passing, overlapping of sensing areas and resource blindness thus, achieving a lot of energy efficiency. SPIN network pass three kind of messages while exchange data between nodes. These are: ADV message for allow a sensor to advertise a particular meta-data, REQ message for request the specific data and DATA message to get the actual data. Figure 2 shows data send and request. [9].

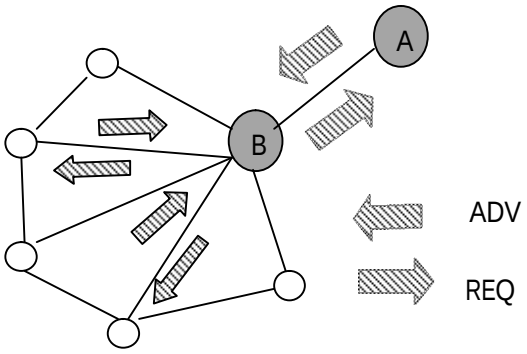

Fig 2: SPIN –Advertise and send request Data within the nodes

iii) Flooding and Gossiping: The flooding sensors receiving a data packets from neighbor node and this process continues until the data arrives at the destination or the maximum number of hops for the data is reached. The gossiping is another version of flooding where the receiving node sends the data to a randomly selected neighbor, picks another random neighbor to forward the data to one another. [10]

iv) Rumor routing: It maintains only one path between source and destination as opposed to Directed Diffusion where data can be sent through multiple paths at low rates. This route passes the queries to the nodes that have observed a particular event within the entire network to retrieve information about the occurring events. Transmission event data packets are long lived manner called as agents. When a node finds an event, it adds found event to its local table and generates an agent. Agents travel the network in order to propagate information about local events to distant nodes. When a node generates a query for an event, the nodes that know the route, can respond to the query by referring its event table. So, the cost of flooding the whole network is avoided. [11]

B. Hierarchical Networks based data aggregation

The hierarchical approach breaks the huge network into clustered layers. Nodes are grouped into clusters with a cluster head that has the responsibility of routing from the cluster to the other cluster heads or base stations. Data travel from a lower clustered layer to a higher one. Although, it hops from one node to another, but as it hops from one layer to another it covers larger distances. This moves the data faster to the base station. Clustering provides inherent optimization capabilities at the cluster heads. This kind of WSN protocols are PEGASIS, HEED, TEEN, and APTEEN [13]

C. Cluster Network based Data Aggregation

In cluster networks, sensors transmit data to the cluster head where data aggregation is performed. In energy-constrained sensor networks of large size, it is inefficient for sensors to transmit the data directly to the sink. The cluster heads can communicate with the sink directly via long range transmissions or multihoping through other cluster heads.

LEACH (Low Energy Adaptive Clustering Hierarchy): role of the cluster head is periodically transferred among the nodes in the network in order to distribute the energy consumption. It provides a conception of round. LEACH protocol runs with many rounds. Each round contains two states: cluster setup state and steady state. In cluster setup state, it forms cluster in self-adaptive mode; in steady state, it transfers data. The time of second state is usually longer than the time of first state for saving the protocol payload. The performance of LEACH is based on rounds. Then, a cluster head is elected in each round. For this election, the number of nodes that have not been cluster heads and the percentage of cluster heads are used. Once the cluster head is defined in the setup phase, it establishes a TDMA schedule for the transmissions in its cluster. This scheduling allows nodes to switch off their interfaces when they are not going to be worked. The cluster head is the router to the sink and it is also responsible for the data aggregation. The cluster head controls the sensors located in a close area, the data aggregation performed by this leader permits to remove redundancy [14].

III. SECURE ROUTES IN DATA AGGREGATION

The important considerations of designing wireless sensor network are secure route in data transmission and aggregation. Many of sensor nodes are installed in open places and are susceptible to physical attacks which might compromise the sensor's cryptographic keys. Data transmission security is a challenging task if the data aggregators and sensors are difficult. All sensor nodes have a session key at a time of installation. Initially sensor nodes encrypt the sensed data was applied, which makes the data transmission more secure, and then send encrypted data to gateways. [15-16]. after completing a current session, sink will generate a new session key using current session key and send to the corresponding gateway.

The data communication process session key has change dynamically for every session by the Sink. The gateway broadcast new session key between cluster sensor nodes. It provides data authentication is granted by using periodically changing user specific session keys. These session keys are generated from the Sink and send to the gateways or cluster head (CH) and then gateway broadcast the key to its cluster sensors node for using next session.

A cluster-head is chosen from each cluster to handle the communication between the clusters nodes and the Sink. Cluster-heads (gateways) are resource rich like as they have more computational and communication power comparatively other sensors nodes. Data aggregation is used to eliminate redundancy and to minimize the number of transmissions for saving energy. In our data aggregation methods, gateway receives all the data from sensor nodes and then eliminates the redundancy by checking the contents of the sensor data. In secure route, sensor data, which is identified as non-redundant by the gateways, is transmitted to the Sink in encrypted form [17-18].In each gateways broadcasts a new session key SKb, encrypted using the common encryption key K, i.e. EK (SKch). Sensor nodes receive broadcasted session key SKch and compute their node-specific secret session encryption key (SKi,CH) by XORing the SKb with SKi.

Changing the encryption key(SKi,CH) in each session guarantees data freshness in the sensor network,

moreover, it also helps to maintain the confidentiality of the transmitted data by preventing the use of the same secret key at all times. Ensuring data freshness means that no adversary replayed old messages and data is recent. During the data transmission, each sensor node appends its IDs, time stamp and message authentication code, to the messages to verify data freshness and integrity. Upon receiving a message, base station finds out SKi associated with the IDs on the message, and then decrypts the data using SKi,CH.[12] .The receiving the data from the sensor nodes, the cluster head appends its own IDi before forwarding the data to the base station. Appending cluster-head IDi to each sensor data helps the base station in locating the origin of the sensor data and reduces the search time required to find the Ki associated with originating node IDi. When the base station receives sensor data, it first determines the Ki of the sender node by using sender and cluster-head IDis, and computes the Ki,b to decrypt the data. Then, base station checks the time stamp and Ki,b for the data freshness and calculates MAC(Ki,b, Data) to verify the data integrity. If the data is altered or replayed, then base station requires corresponding sensor nodes to transmit their data again.Figure3 shows Securities Session key b/w Sensor node, Sink and Gateway

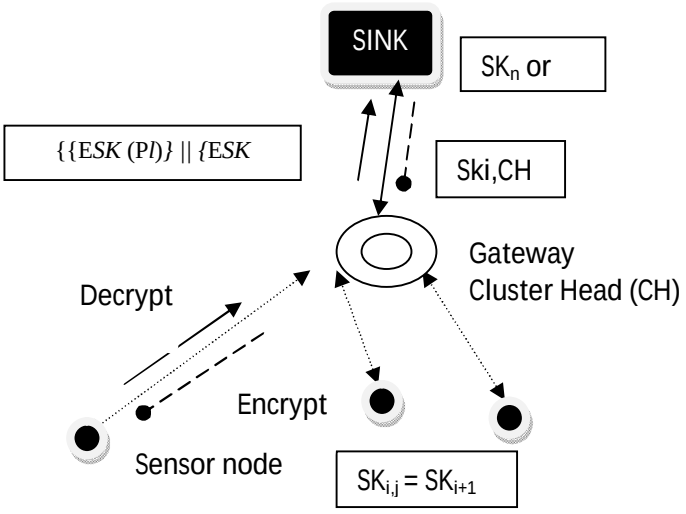

Figure 3: Securities Session key b/w Sensor node, Sink and Gateway

The alternate technique for secure Data transmit from Sensor node to Gateway, A Sensor node S*i* encrypt the packet P*i* using current session key SK, which is built-in at the time of sensors deployments and send to it's a local gateway G*i*. Si *!* Gi E*SK* (P*i*). Gateway to Gateway transmission perform, Gateway concatenates the encrypted packets it received from the sensors in its own cluster and from the other gateways on the path to the sink, Increment the value of logical time stamps T*GS* by one and appends it to the concatenated packets, Concatenate its own IDs and send it to the next Gateway on the path to the Sink. G_h -> G_k. {{E*SK* (P*l*)*}* || *{*E*SK* (P*m*)} where E_{SK} (P_i), E_{SK}(P_m) are encrypted packets from the sensor node l, m,n belonging to the cluster. Transmit the data from Gateway to Sink; it has received concatenated Encrypted packets from the gateway G*k Sink*.

IV.CONCLUSION

The paper provides a short overview of some representative regard secure routing data aggregation in WSN. We focus on optimizing important performance techniques such as network lifetime, data latency, and energy consumption. Efficient organization, routing, and data-aggregation tree construction are the main focus areas of data-aggregation techniques. We also review the security issues in data aggregation in WSN. Combining aspects such as security, data transmission and system lifetime in the context of data aggregation is worth exploring. In the future we will work for an efficient security framework and algorithms.

REFERENCE

[1] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci. Wireless sensor networks:A survey. Computer Networks, March 2002.

[2] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., Cayirci, E. (2002) 'A Survey on Sensor Networks', IEEE Communications Magazine, 40(8), 102-114.

[3] Fasolo E., Rossi M., Widmer J. and Zorzi M. (2007) *IEEE Wireless communication.*

[4] C. Shen, C. Srisathapornphat, and C. Jaikaeo, "Sensor information networking architecture and applications," *IEEE Personnel Communications*, Aug. 2001, pp.52-59.

[5] S. Tilak, N. Abhu-Gazhaleh, W. R. Heinzelman, "A taxanomy of wireless micro-

sensor network models," *ACM SIGMOBILE Mobile Comp. Commun. Rev.*, vol. 6, no. 2, Apr. 2002, pp. 28- 36.

[6] Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera, and Cláudia Jacy Barenco Abbas, "Routing Protocol in Wireless Sensor Networks", *Sensors* 2009, vol. *9*, pp. 8399 -8421.

[7] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: A scalable and robust communication paradigm for sensor networks", Proceedings ACM MobiCom'00, Boston, MA, Aug. 2000, pp. 56-67.

[8] B. Chen, K. Jamieson, H. Balakrishnan, and R. Morris, "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks", Wireless Networks, vol. 8, no.5, Sept. 2002, pp. 481-494.

[9] Braginsky D., Estrin D. (2002) Proceedings of the First Workshop on Sensor Networks and Applications (WSNA), Atlanta, GA.

[10] Schurgers C. and Srivastava M.B. (2001) Energy Efficient Routing in Wireless Sensor Networks. In MILCOM Proceedings on Communications for Network-Centric Operations: Creating the Information Force, McLean, VA.

[11] D. B Johnson et al., "Dynamic Source Routing in Ad Hoc Wireless Networks", in Mobile Computing, edited by Tomas Imielinski and Hank Korth, Kluwer Academic Publishers, ISBN: 0792396979, 1996, Chapter 5, pp. 153-181.

[12] Wendi Rabiner Heinzelman, Anantha Chandrakasan, and Hari Balakrishnan (2000) Energy-Efficient Communication Protocol forWireless Microsensor Networks" Proceedings of the 33rd Hawaii International Conference on System

[13] Perrig A., Szewczyk R., Wen V., Cullar D., and Tygar J. D. (2001) Proceedings of the 7th Annual ACM/IEEE Internation Conference on Mobile Computing and Networking (MobiCom), Rome, Italy, 189- 199.

[14] Hu L. and Evans D. (2003) Workshop on Security and Assurance in Ad hoc Networks.

[15] A. Perrig, R. Szewczyk, J.D. Tygar, V. Wen, D.E. Culler, SPINS: Security protocols for sensor network, Wireless Networks 8 (5) (2002) pp. 521–534.

[16] B. Schneier, Fast Software Encryption, Cambridge Security Workshop Proceedings, Springer, Berlin, 1994. pp. 191–204.

AUTHORS

Sasikala.K, she is pursuing M.Phil (CS), Muthayammal College of arts & Science College. Rasipuram, TN, India. She has received M.Sc., Computer Science in the year 2011. Her main research interest includes wireless sensor networks, Web designing and Databases

Geetha.M, she is currently working as Associate Professor in Muthayammal College of arts & science college, Rasipuram, TN, India. She is having 9 years of teaching experience. Her main research interest includes wireless sensor networks and Data Mining.