Secure and Energy Efficient Data Aggregation Technique for Cluster Based Wireless Sensor Network

Ashwini V. Sisal[1]
[1]M.E. Computer Network
[1]G.H.R.C.E.M.Wagholi,
[1]Pune,India
[1]*Ashwini.sisal@gmail.com*

Prof. Simran Khiani[2]
[2] Assistant Prof.(I.T.)
[2]G.H.R.C.E.M.Wagholi,pune
[2]Pune, India
[2]simran.khiani@raisoni.net

Abstract— In the past few years secure transmission of data along with efficiency is a serious issue for wireless sensor networks (WSNs).Clustering is a powerful and convenient way to enhance performance of the WSNs system. In this project work, a secure transmission of data for cluster-based WSNs (CWSNs) is studied, where the clusters are formed dynamically and infrequently. Basically protocols for CWSNs, called SET-IBS (Identity-Based digital Signature)scheme and SET-IBOOS (Identity-Based Online / Offline digital Signature)scheme, correspondingly. In SET-IBS, security relies on the hardness of the Dill-Hellman difficulty in the pairing area. Data aggregation is the process of abbreviation and combining sensor data in order to reduce the amount of data transmission in the network. This paper investigates the relationship between security and data aggregation process in wireless sensor networks. In this paper propose SET-IBS and data aggregation techniques for secure and efficient data transmission. For energy consumption using DRINA algorithm. DRINA means Data Routing for In-Network Aggregation, that has some key aspects such as high aggregation rate, a reduced number of messages for setting up a routing.

Keywords- *Cluster, Data aggregation, WSN, Security*

*****

I. INTRODUCTION *(HEADING 1)*

In recent years, Wireless sensor network (WSNs) plays a very important role in various application domains such as object detecting, medical caring, forest monitoring and so on. In Wireless Sensor Networks energy ability and scalability are two greater challenges. For example, the number of nodes in a randomly illuminate network needs to be enough high to ensure connectivity. As a result, when using its maximum transmission power, a node may have very massive of neighbors. Having more neighbors than the necessary leads is redundant for energy consumption in the network. This complexity can be overcome by using topology control which restricts the set of neighbors of given node. The transmission power can be reduced along power consumption by carefully choosing the set of neighbors. Lack of energy efficiency which delays the lifetime of the network is one of the serious issues in the Wireless Sensor Network (WSN). The main characteristics of a WSN include Power consumption, Ability to arrive up with node failures, Mobility of nodes, Failure in communication, multiplicity of nodes. The individual nodes are capable of sensing their environments ,processing the information data nearby, and sending data to one or more collection points in a WSN Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can achieve the corresponding private keys without secondary data transmission, which is efficient in communication and saves energy.

Data aggregation reduce the number of transmission thus improving the bandwidth and energy consumption in WSN. Aim to combine the data packets of numerous nodes so that amount of data transmission is reduced. The intelligent way to combine and reduce the data belonging to a single cluster is known as data aggregation in cluster based environment. It is a process of grouping the sensor nodes in a closely deployed large-scale sensor network.

II. RELATED WORK

In-network data aggregation acts an important role in energy constrained WSNs, since data correlation is demoralized and aggregation is performed at intermediate nodes to reducing size and the number of messages exchanged across the network. In data gathering-based application, number of communication packets can be reduced by in network aggregation, resulting in a longer network lifetime. In most cases, tree-based protocols build a traditional shortest path routing tree. For instance, the Shortest Path Tree (SPT) algorithm [9] uses a very simple strategy to build a routing tree in a distributed fashion. In this approach, every node that detects an event reports its collected information by using a shortest path to the sink node. Information fusion occurs whenever paths overlap.

In [2]paper, Data aggregation, as a typical operation in data get-together applications, can cause a lot of energy wastage since sensor nodes, when not receiving data, may keep in the listen state during the data collection method. To save this energy wastage, sleep scheduling algorithms can be used to turn the nodes to the sleep state when their radios are not in use and wake them up when required. In this paper, identify the contiguous link scheduling problem in WSNs, in which each node is assigned repeated time slots so that the node can wake up only once in a scheduling period to fulfill its data collection duty. Also proposed centralized and distributed algorithms with hypothetical performance bounds to the optimum in both homogeneous and heterogeneous networks.

In [3]paper focus on constructing a Load-Balanced Data Aggregation Tree (LBDAT) under the PNM. Accordingly, approximation algorithms and inclusive theoretical analysis of the approximation factors are presented in the paper. Three problems are investigated, namely, the Load-Balanced Maximal Independent Set (LBMIS) problem, the Connected

Maximal Independent Set (CMIS) problem, and the LBDAT construction problem LBMIS and CMIS are well-known NP-hard problems and LBDAT is an NP-complete difficulty. In this paper, address the fundamental problems of constructing a load-balanced DAT in probabilistic WSNs. First solve the CMIS problem, which is NP-hard, in two phases.

In [6] paper provide a resolution for node capture attack. Node capture attacks result from the combination of active, passive and physical attacks by an intelligent challenger. In Proposed System, to avoid data loss initially sensor network is separated into different clusters , each cluster is headed by an aggregator and directed connected to sink. So, this idea basically isolated data processing measures to save the power and minimize the medium access layer disagreement in wireless sensor networks. It proposed the distinct Structure and Density Independent Group Based Key Management Protocol (DGKE) propose a method for countering node capture attacks for hierarchical data aggregation in wireless sensor networks.

In [12] paper, studied the major problems in applying SlepianWolf coding for data aggregation in cluster-based WSNs, including the CSWC problem, the optimal intra cluster rate-allocation problem, and the joint intra-CSWC and inter cluster precise entropy coding problem. Proposed the DOC protocol, which can be used to select a set of disjoint potential clusters that maximize the global compression gain of SlepianWolf coding.

III. EXISTING SYSTEM

The existing system is absence of the symmetric key management for secure data transmission. They existed secure and efficient data transmission protocols correspondingly SET-IBS and SET-IBOOS. In the estimation part, they provided feasibility of the proposed SET-IBS and SET-IBOOS with respect to the security requirements and analysis against routing attacks. SET-IBS and SET-IBOOS are efficient in communication and applying the ID-based crypto-system, which achieves security requirements in CWSNs, also solved the orphan node problem in the secure transmission protocols with the symmetric key management. Finally, the comparison as well as calculation and simulation results show that, the proposed SET-IBS and SET-IBOOS protocols have better performance than existing secure protocols for CWSNs. With respect to both computation and communication costs, pointed out the behavior that, using SET-IBOOS with less supporting security overhead is preferred for secure data transmission in CWSNs. The key scheme of both SET-IBS and SET-IBOOS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security.

IV. PROPOSED SYSTEM

Data Aggregation WSNs are data driven networks, where the information that need to be routed are formed in large amount in a multi hop fashion, toward a sink node ,which works as a gateway to a monitoring center DRINA plays an very important role in the data gathering process. Data aggregation forwards only smaller number of data, reducing the redundant data, which leads to lower energy saving ,communication cost and thus improves the lifetime of the network. When the nodes forward the aggregated data packets to the sink node, if a lose in the packet occurs, then this cause server impact on data analysis in the monitoring center. So the algorithm used provide an important role in aggregated data forwarding and capable of providing assured service even in the case of node failure circumstances. In typical wireless sensor networks, sensor nodes are usually resource-constrained and battery-limited. In order to save resources and energy, data must be aggregated to avoid irresistible amounts of traffic in the network. The aim of data aggregation is that eliminates redundant data transmission and enhances the lifetime of energy in wireless sensor network.

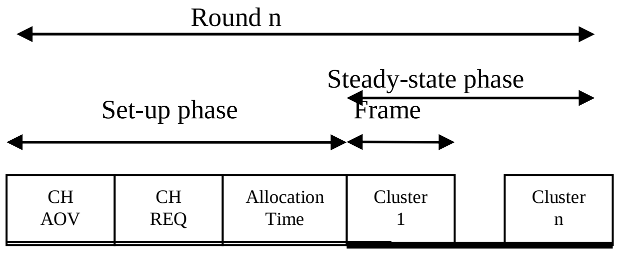
Data aggregation is the process of one or several sensors then collects the detection result from other sensor. The collected data must be processed by sensor to reduce transmission trouble before they are transmitted to the sink or base station. The wireless sensor network has consisted three types of nodes. Regular sensor nodes sense data packet from the environment and send to the aggregator nodes basically these aggregator nodes collect data from multiple sensor nodes of the network ,aggregates the data packet using a some aggregation function like sum, average ,count, max min and then sends aggregates result to upper aggregator node who generate the query, DRINA that has some key aspects such as a reduced number of messages for setting up a routing tree, maximized number of overlapping routes, high aggregation rate, and reliable data aggregation and transmission.

The main goal of our proposed the DRINA algorithm is to build a routing tree with the shortest paths that connect all source nodes to the sink while maximizing data aggregation. The proposed algorithm considers the following roles in the routing infrastructure formation:

- Collaborator
- Coordinator
- Sink
- Relay

SET-IBS

Secure and Efficient data Transmission (SET) protocols for CWSNs is proposed, called SET- IBS, by using the IBS scheme respectively. The key idea of both SET-IBS is to authenticate the encrypted sensed data, by applying digital signatures to message packets, which are efficient in communication and applying the key management for security. Pairing parameters and Secret keys are distributed and preloaded in all sensor nodes by the BS initially. Secure communication in SET-IBS relies on the ID-based cryptography, in which, user public keys are their ID information. Thus, users can obtain the corresponding private keys without auxiliary data transmission, which is efficient in communication and saves energy. IBS Method planned for CWSNs, consists of the following four processes:



- Setup at the BS: The BS creates a master key mk and public parameters Pprm for the private key generator (PKG), and provides these to every sensor nodes in network.
- Key extraction: Given an ID string, a sensor node creates a private key skID related with the ID by means of mk.
- Signing of signature: Given a time-stamp t, signing key and message M, a signature SIG is created by the sending node.
- Verification of the data receiving nodes: Given the SIG, ID and M, the receiving node yields accept if SIG is legal, and outputs reject if not.

A. *DRINA Algorithms :*

The DRINA algorithm can be divided into three phases. In Phase 1, built hop tree from the sensor nodes to the sink node. In this phase, the sink node starts building the hop tree that will be used by Coordinators for data forwarding purposes. Phase 2 consists of cluster formation and cluster-head determination among the nodes that detected the occurrence of a new event in the network. Lastly, Phase 3 is responsible for both setting up a new route for the updating the hop tree and reliable delivering of packets.

Algorithm 1:Hop Tree Configuration :

This phase is started by the sink node sending the Hop Configuration Message (HCM) to all network nodes. The HCM message contains two fields: ID and HopToTree, where ID = Node identifier that started or retransmitted the HCM message and HopToTree = Distance, in hops, by which an HCM message has passed

Algorithm 1: Hop Tree Configuration Phase

```
1. Node sink sends a broadcast of HCM messages with the value of HopToTree = 1.
2. For each u ∈ R do
        If HopToTree (h) > HopToTree (HCM) and First Sending (h)
        then
        Next Hop ← IDHCM;
        HopToTree ← HopToTreeHCM + 1;
3. Node u updates the value of the ID field in the message HCM.
        IDHCM ← IDh;
4. Node u updates the value of the HopToTree field in the message HCM
        HopToTreeHCM ← HopToTree;
5. Node u sends a broadcast message of the HCM with the new values;
        FirstSending h ← false;
6. End
7. Else
        Node u discards the received message HCM;
8. End
9. End
```

Cluster formation algorithm:

When an event is detected by one or more nodes, the leader election algorithm starts and sensing nodes will be running for group coordinator (leadership). For this election, all sensing nodes are eligible. If this is the first event, the leader node will be the one that is closest to the sink node. Otherwise, the leader will be the node that is closest to an already established route. Determines the node with max energy from the nodes. Another possibility is to use the energy level as a tiebreak criterion. At the end of the election algorithm only one node in the group will be declared as the leader (Coordinator). The remaining nodes that detected the same event will be the Collaborators. The Coordinator gathers the information collected by the Collaborators and sends them to the sink. A key advantage of this algorithm is that all of the information gathered by the nodes sensing the same event will be aggregated at a single node (the Coordinator), which is more efficient than other aggregation mechanisms .Then status update,Marks the status of the node as active or inactive

The resulting route is a tree that connects the Coordinator nodes to the sink. When the route is established, the hop tree updating phase is started. The main goal of this phase is to update the HopToTree value of all nodes so they can take into consideration the newly established route. This is done by the new relay nodes that are part of an established route.

Algorithm 2: Cluster formation and leader election

```
1. Input: S
        S - Set of nodes that detected the event.
2. Output: h
        A node of the set S is elected leader of the group.
3. For each h ∈ S
        do
        Role h ← coordinator;
        Node h sends message MCC in broadcast
        Announcement of event detection;
        Nu is the set of neighbors of node h ∈ S
4. Node u retransmits the MCC message received from node w;
        For each w ∈ N u do
        If HopToTree (h) > HopToTree (w) then
                Role h ← collaborator;
5. End
6. Node u retransmits the MCC message received from node w;
        Else if
        HopToTree (h) = HopToTree (w) ^ energy_max() (h) > energy_max() (w)
        then
                Role h ← collaborator;
7. End
8. Else
```

```
        Node u discards the MCC message received from w;
9. End
10. End
11. End
12. End
```

Algorithm 3: Route establishment and hop tree update

```
1. Leader node v of the new event sends a message REM to its NextHop v;
2. Repeat
3. h is the node that received the REM message that was sent by node v.
        If h = NextHop v then
        HopToTree h ← 0;
        Node h is part of the new route built
        Role h ← Relay;
        Node h sends the message REM to its
        NextHop h;
        Node h broadcasts the message HCM with the value of HopToTree = 1;
        Nodes that receive the HCM message sent by node h.
4. End
5. Until
        Find out the sink node or a node belonging to the routing structure already established.
6. Repeat
7. s_h is the number of descendants of u
        If s_h > 1 then
8. Aggregates all data and sends it to the NextHop h;
        If Role h = Relay then
        Execute the mechanism
9. End
10. End
11. Else
        Send data to NextHop h;
12. If Role h = Relay then
        Execute the mechanism
13. End
14. End
15. Until The node has data to transmit/retransmit;
```

B. *MATHEMATICAL MODEL*

Formation of Hop Tree Hop Configuration message (HCM) is used to build the Hop-Tree in DRINA. The hop ID and HopToTree are the two fields in HCM.

A)Initial State:-

Sensor nodes will be create and it enables user of the system to send and receive node's.

B)Intermediate state:-

Representation in the form of set theory:-

Let,

I=Input set:

I represents the Sensor node given as input to the further function.

I= {I1, I2 , I3, . . . , In}

n= Total no. of nodes.

K=subset of nodes in network which are neighbors of I

i.e. K is neighborhood of I

Δt =Period of time

Δt =t1-t0

T=No. of packets send

R= No. of packets receive

Formula ::

$\sum R\ (t1) = \sum T\ (t1)$

Functions set:-

It is a set of different functions applied on mobile node like F1, F2, F3, . . . Fn are the set of functions which works sequentially.

F= {F1,F2,F3,F4, . . ., Fn}

Identify the Function

F= {Set of Functions}

F= {F1,F2,F3,F4, . . ., Fn} and

F1 = {e1, e2, e3, e4}

Where,

{e1=Find the Sensor nodes in the network}

{e2=Provide the Packet delivery ratio in the network}

{e3= End to end delay }

{e4= Throughput }

O= Output set

O={O1, O2, O3, . . ., On}

F1=Hop Tree Configuration in the network.

F2=Cluster formation and leader election process

F3=Route Establishment and hop tree update

C)Final State:-DRINA algorithm provide the best aggregation quality. It can improve lifetime of network by reducing energy consumption.

V. EXPERIMENTAL RESULT

Analyzed the data transmission issues and the security issues in CWSNs as well as the solved the orphan node problem in the secure transmission protocols with the symmetric key management. Finally, the comparison results shows that the proposed protocols have better performance than the existing secure protocols for CWSNs. With respect to both computation and communication costs the system efficiency is moderately good. SET-IBS and SET-IBOOS are efficient in communication and applying the ID based cryptosystem, which achieves security requirements in CWSNs.

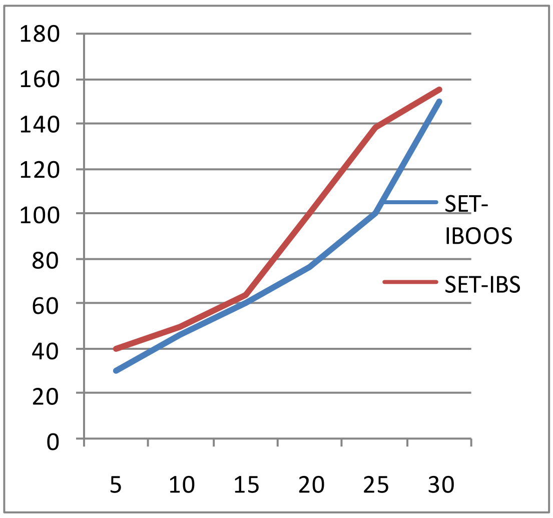


Fig. Energy Consumption Graph of three protocols

In the above Fig. Shows the energy consumption graph. X-axis denotes number of nodes. Y-axis denotes energy consumption is taken.The low-energy adaptive clustering hierarchy (LEACH) protocol is presented which is a generally known and effective one to reduce and balance the total energy consumption for cluster-based Wireless sensor networks. In the proposed method secure and efficient data transmission (SET) protocols for CWSNs is presented which is called SET-IBS and SET-IBOOS. In this method, the number of nodes is increased, the energy consumption is increased. The results demonstrate that the proposed SET-IBS and SET-IBOOS protocols consume energy faster than LEACH protocol because of the communication and computational overhead for security of either IBS and/or IBOOS process.

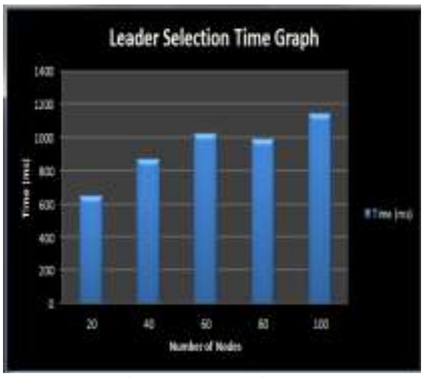


Fig. number of node vs. time for leader selection

Above figures shows the performance analysis of data aggregated algorithms such as DRINA. Fig. show the aggregated rate of transmitted data also shows its corresponding loss probability. It clearly seems that more number of data packets is aggregated with less loss probability.

VI. CONCLUSION

SET-IBS and SET-IBOOS are efficient in communication and applying the ID based cryptosystem, which achieves security requirements in CWSNs also the solved the orphan node problem in the secure transmission protocols with the symmetric key management. In order to reduce the energy of the wireless sensor network also efficient data aggregation is necessary so that to eliminate the redundant data, this method positively give the efficient data aggregation .So that it will provide the energy saving and life time of the network will improve.

REFERENCES

[1] Junchao Ma ,Contiguous Link Scheduling For Data Aggregation In Wireless Sensor Networks, IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 7, July 2014

[2] Huang Lu, “Secure And Efficient Data Transmission For Cluster-Based Wireless Sensor Networks”, IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 3, March 2014

[3] Jing (Selena) He, Constructing Load-Balanced Data Aggregation Trees In Probabilistic Wireless Sensor Networks, IEEE Transactions On Parallel And Distributed Systems, Vol. 25, No. 7, July 2014

[4] Villas L.A, Boukerche A, Ramos H.S, De And Loureiro A.A.F (2013)DRINA: A Lightweight Aggregation In Wireless Sensor Networks, IEEE Trans. ,On Computers, Vol.62 No.4, Pp 676-689.,2013

[5] Antonio Alfredo Ferreira Loureiro, DRINA: A Lightweight And Reliable Routing Approach For In-Network Aggregation In Wireless Sensor Networks, IEEE Transactions On Computers, Vol. 62, No. 4, April 2013.

[6] Shaik Nagul Shareef Secure And Efficient Hierarchical Data Aggregation In Wireless Sensor Networks International Journal Of Modern Engineering Research (IJMER) Www.Ijmer.Com Vol. 3, Issue. 4, Jul - Aug. 2013

[7] Mohsen Rezvani Secure Data Aggregation Technique For Wireless Sensor Networks In The Presence Of Collusion Attacks Ieee Transactions On Dependable And Secure Computing (Tdsc), 2013

[8] Leandro Villas, Azzedine Boukerche1, Heitor S.Ramos, DRINA: A Lightweight And Reliable Routing Approach For In-Network Aggregation In Wireless Sensor Networks Wireless Sensors, 2012

[9] Dan Wu And Man Hon Wong , Fast And Simultaneous Data Aggregation Over Multiple Regions In Wireless Sensor Networks, IEEE Transactions On Systems, Man, And Cybernetics, Vol. 41, No. 3, May 2011

[10] F. Hu, X. Cao, And C. May, Optimized Scheduling For Data Aggregation In Wireless sensor Networks, Proc. Intl Conf.2012

[11] Jaydip Sen ,”Secure And Energy-Efficient Data Aggregation In Wireless Sensor Networks”, Member, ACM Kolkata, INDIA

[12] Jun Zheng, “Distributed Data Aggregation Using Slepianwolf Coding In Cluster-Based Wireless Sensor Networks”, IEEE Transactions On Vehicular Technology, Vol. 59, No. 5, June 2010

[13] Nakamura E.F, Loureiro A.A.F, And Frery A.C “Information Fusion For Wireless Sensor Networks: Methods, Models, And Classifications,” ACM Computing Surveys, Vol. 39, No. 3, Pp. 9-1/9-55,2007

[14] E.F. Nakamura, H.A.B.F. De Oliveira, L.F. Pontello, And A.A. F. Loureiro,” On Demand Role Assignment For Event-Detection In Sensor Networks,” Proc. IEEE 11th Symp. Computers And Comm. (ISCC 06), Pp. 941-947, 2006.

[15] Information Technology: Coding And Computing (ITCC 05), Pp. 557- 561, 2005.

[16] K. Romer And F. Mattern, “The Design Space Of Wireless Sensor Networks”, IEEE Wireless Comm., Vol. 11, No. 6,Pp. 54-61, Dec. 2004.

[17] B. Krishnamachari, D. Estrin, And S.B. Wicker, The Impact Of Data Aggregation In Wireless Sensor Networks, Proc. 22nd Intl Conf. Distributed Computing Systems (ICDCSW 02), Pp. 575-578, 2002.

[18] Heinzelman, W.R.,Chandrakasan, A., Balakrishnan, H. "Energy-Efficient Communication Protocol For Wireless Microsensor Networks". In Proceedings Of The 33rd Annual Hawaii International Conference On System Sciences, Maui, HI, USA, 47 January 2000;Pp.1019