Secure and Efficient Energy Consumption System in WSN

Miss Harshala Mahajan. Prof. Dr. S. J.Wagh
1PG student, Computer department, 2 Professor, Computer department,
KJCOEMR, Pisoli, Pune-48
harshala.mahajan2@gmail.com, sjwagh1@yahoo.co.in

Abstract:- For cluster-based WSNs (CWSNs), secure data transmission, where like dynamically and periodically the clusters are shaped. The analysis problems associated with WSNs security and knowledge aggregation with reference to the protection and security analysis against various attacks, we show the quality of being usable of the SET-IBS and SET-IBOOS protocols. For a fuzzy approach and SET-IBS formula employing a combination in our planned system, for WSNs a replacement routing technique to extend network amount of sometime from the supply to the destination by affirmative the best remaining battery power. The proposal is to envision an optimum routing path, minimum vary of hops, and minimum traffic load in terms of leveling energy consumption and for some time maximization of network quantity for the planned technique. To demonstrate the effectiveness, in two completely different topographical areas using similar routing criteria with the A-star search formula we tend to match our approach and fuzzy approach.

Keywords—*ID-based digital signature, secure data transmission protocol, Cluster-based WSNs, Fuzzy Approach, Minimum Energy Consumption.*

*****

I. INTRODUCTION

InWireless sensor networks, have used in several areas like surroundings, health, setting observance and industrial functions at the beginning for themilitary for various application. With the recent breakthrough of "Micro Electro Mechanical Systems (MEMS)" technology [2] whereby sensors became smaller and extra versatile at intervals, the term WSN guarantees many new application areas.

To conservation of energy, packets transmitted to the lowest station leading information aggregation reduces the redundant information that in turn minimizes the quantity to the top purpose. Since data aggregation transmits exclusively the useful or resultant information, the matter of network congestion, traffic implosion, and overlap are usually overcome [3]. Aggregated data transmits securely. For security reason the digital signature is used at the source node as well as destination node. Aggregated data is encrypted at the source node and embed with the digital signature. This encrypted data with digital signature transmit to the destination. So that in network third party should not decrypt this data. Digital signature is obtained combining public key and the ID of the node, which are generating digital signature.

The data transmission is one in all the foremost necessary issues. Many Wireless Sensor Networks are deployed in hard, abandon, and with trustless surroundings typically adversarial physical environments certainly applications, like military domains and sensing tasks. Secure and efficient information transmission (SET) is use in many such smart Wireless Sensor Networks notably necessary and is demanded.

However, for Secure and Efficient transmission (SET) use not onlyfor device networks, specifically in-network aggregation and information management throughout this project but also we have a tendency to tend to focus on another necessary side for procedure quality. These approach change to trade off communication. In cluster Wireless sensor networks secure data transmission with minimum energy consumption is needed. In thedata transmission, the more energy is used then thenode may not send whole data to the destination. The node will be dead due to lack of energy. So we want to transmit more data in less energy consumption.

For sending data from source to thedestination we have to form a cluster. We can form a cluster by using clustering algorithm.Clustering algorithms are different by the architecture and node deployment. The clustering algorithms are developed with respect to the application. Because of cluster formation the life of node increases,as there is no bulk messages send to nodes which are not in communication. In acluster, we select the cluster head by any election algorithm. And then cluster head will aggregate the data from the leaf node. Leaf nodes are the remaining node in the clusters i.e. all node excluding cluster head.

Apply security to the node very challenging task with adigital signature. So we are applying all parameters to the node in starting required for the digital signature

I. LITERATURE SURVEY

To improve the scalability of network and the management of network the researches develop the cluster based data transmission.

TiNA [4] Temporal coherency-aware in-Network Aggregation [4] (TiNA) works on highest quality of a routing tree (i.e., TAG or panther) having the information gathering purpose (sink) at its root. For the aggregate information by suppressing those values that don't have an effect on the expected quality for device readings to scale back energy consumption. It also balances the energy efficiency in the network

In an SQL statement by Modulus Addressing (DADMA), DADMA(Data Aggregation and Dilution by Modulus Addressing) [5] for device networks where nodes mixture or dilute detected values accordingto theinformation aggregation and Dilution [5] technique, as a distributed relational database DADMA treats a wireless device network.

By means that of Feedback management information Aggregation [6], on information delivery and minimizing the energy consumption. The authors of [6] outline a technique to tune the degree of knowledge gathering whereas maintaining such latency bounds. To the delivery of device measurements with period applications,they think about time-constrained reference eventualities dealing that impose specific time constraints. On the delivery time, information is sorted into completely different categories related to different bounds. For all information at the minimum energy value. The aim is to ensure the delivery whereas satisfying all time constraints. Consequently to fulfill these necessities the information aggregation degree is tailored.

A recent resolution to the information aggregation drawback has been projected in Synopsis Diffusion Framework [7]. Within the information aggregation method, multiple times (double-counting problem) to outline aggregation functions and information structures that are sturdy to considering equivalent device readings is that the main contribution of the paper. With multi-path routing schemes in conjunction, this is often crucial once information aggregation is employed.

In [8], the problem of temporal order once aggregating in Wireless device network has explain by the author. Theyneed to be shown, during a WSN by reducing the number of knowledge transmitted through each mathematical analysis and simulation that their projected protocol will save energy.

In [9], for temporal order in information aggregation algorithms,this paper evaluates the impact by process information because it flows from sources to sinks for In-network aggregation attains energy-efficient information recreation.

Data-centric routing and compare its performance by using traditional end-to-end routing schemes [10]. It was examined the impactwith information aggregation on the energy prices and delay associated with source-destination placement and communication network density. It was shown that across a good vary of operational eventualities data-centric routing offers important performance gains.

Since within the literature for the Steiner tree drawback is found it's an NP-hard drawback, some heuristics. Approximate solutions to the matter are given in [11] and [12]. However, for resource-constrained networks, these solutions don't seem to be applicable. For WSNs, since for messages exchange their distributed implementation need an oversized variety once in high energy consumption putting in the routing tree and, consequently resulting.

Related to information transmission ways, recently in [13], Carman initial combined the advantages of IBS and key redistribution set into WSNs.The signatureprocess to scale back the computation and storage prices. The security is provided using ID- Based signature[14],[15],[16]. The IBOOS theme has been projected by S. Even for constructing online/offline signature [17] general methodology schemes was introduced.In online/offline signature, no need to store the key anywhere or have to calculate the key first. In IBOOS scheme the keys, which are used for encryption and decryption created online.

For the key management in Wireless Sensor Networks,theIBOOS theme may be effective. Specifically, on a device node, the offline section is dead or to communication at the previous, whereas the net section is to be dead throughout thecommunication. For WSNs after Some IBOOS schemes are designed for AODV and DSR routing security [18],[19]. The offline signature in thisstrategy, a third party and lacks reusability is precomputed, therefore for CWSNs they're not appropriate.

The remainingof this paper arrange as follows: section III describe the motivation, problem definition and our proposed system architecture. Section IV describe the hardware requirement and the result to be expected and finally, section V conclude the paper.

II. Proposed Approach Framework and Design

3.1 Motivation

The two secure data transmission protocols SET-IBS and SET-IBOOS that are economical and powerful for wireless sensing element networks. In communication SET-IBS and SET-IBOOS for CWSNs applying the ID-basedcryptosystem that attains security requirements, furthermore with the symmetrical key management as resolved the orphan node drawback inside the secure transmission protocols. Overall in WSNs exploitation ancient these two protocols solve the protection issues or for data aggregation and management existing ways. The routing performance exploitation SET-IBS is must be improved.

3.2Problem Definition

Nodes in the network should have the maximum energy. If the node has the lowest energy level, then in between the transmission of data, the energy will be low. Because of that, the data transmission will be terminated in between and destination didn't get all data. And network will be partition in two network. So it will be confirmed that node should not die during data transmission.

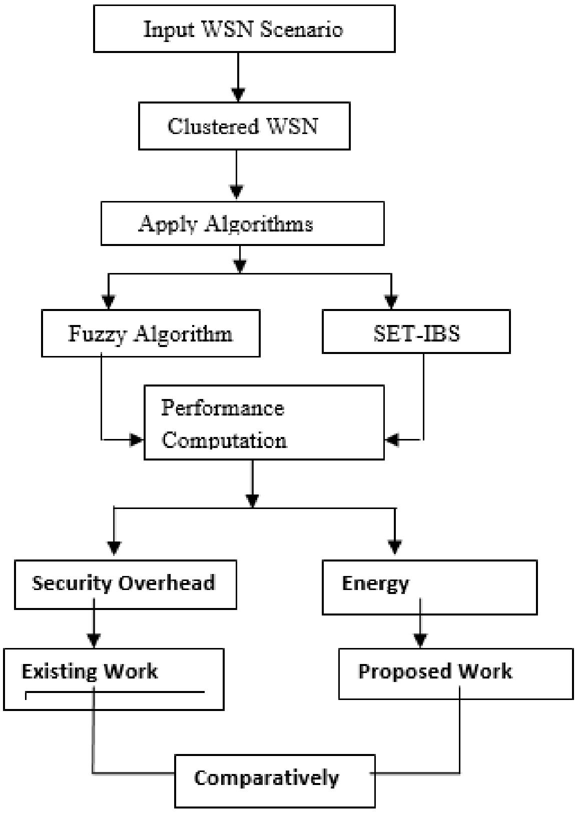

Figure 1: System architecture

3.2 Proposed Work:

When we use the fuzzy approach in SET-IBS protocol,it will increase the time period of the network.The new routing technique for WSN to increase network period and an SET-IBS algorithmic rule.Byfavoring the best remaining battery power, theminimum range of hops and minimum trafficloadfrom the source to the destinationthe approach is to determine an optimum routing path. To determine the potency of the proposed technique,with the A-star search algorithm and fuzzy approach we compare our approach using equivalent routing criteria in two completely different geographical areas.

3.3 Mathematical Model:

Our input and output is as follows:

I= {N, E,D}

Where N- Node, E- Energy,D-data

O= {N,D,RE}

Where D- data, RE- Remaining Energy

In the Proposed model, we calculate the node cost(Cn) of each node in the network. Because of which we come to know that remaining energy so that network partition avoided due to lack of energy or dead node. So the cost of node is calculated by

$$Cn=\frac{\sum_{i=0}^{n} RB_i * C_i}{\sum_{i=0}^{n} RB_i}$$

Where

RB_i- Rule based output i.

C_i - Centre of the output membership function.

Let U is universe of communication, fuzzy set S in universe of communication i.e. U is given by

$$S= \{(u, \mu_A(x)/u \in U\}$$

Where u is the object of theuniverse of communication U.

After calculatingthecost of thenode we create the network using nodes which have more cost i.e. more energy level. Then after we do the following steps:

Step 1: sink ->N_s

In this step, the sink sends all information including its ID to all its node for theelection of Cluster Head.

Step 2: CH_i -> N_s

The Cluster Head which is elected and send their information to all nodes for theformation ofthecluster.

Step 3: Leaf N_j->CH_i

Then nodes excluding Cluster Head i.e. Leaf Nodes joins the cluster Head to form a cluster

Step 4: CH_i ->N_s

Cluster Head send the message to anode in its cluster for communication.

Step 5: Leaf Nj ->CH_i

A leaf node j in cluster transmits the sensed data to

it'sCluster Head CH

Step 6: CHi ->sink

Cluster Head send all collected information through leaf nodes to the sink

III. Implementation Details

The requirement of hardware and software is given. Also the expected result of proposed system is expain.

4.1Hardware and Software Used

For our proposed system we require Pentium-IV processor with 1.1 GHz. Random access memory should be 256 MB. The Hard disk is required of 20 GB. Also keyboard and SVGA monitor. The above hardware is required

The operating system require for project is Windows XP/7/8. The proposal system will be implement in JAVA. Also for implementation the Eclipse tool is require.

4.2Expected Results of Practical Work

The SET-IBS has a protocol initialization prior to the network deployment and operates in rounds during communication, which consists of a setup phase and a steady-state phase in each round. We introduce the protocol initialization, describe the key management of the protocol by using the IBS scheme. In the proposed system, we are using thefuzzy approach with SET-IBS technology for energy saving. So in proposed system minimum energy consumption will be done. So that the sensor node will transfer more data in existing energy level. And no network partition will be done during data transfer because we are choosing nodes which have high energy level.

IV. Conclusion and Future Work

The SET-IBS and SET-IBOOS protocol is explained in short. Then architecture of our proposal system is given. In this proposal, we are avoiding network partition because of the dead node. Our actual mathematical module explains. The cluster head selection and cluster formation in explain in the mathematical module.Dead nodes are formed in the network due to the lack of battery power or energy.With this, we provide security and data aggregation to address the analysis problems.

Acknowledgement

I am highly thankful to prof. S.J. Wagh for his guidance and constant supervision as well as sharing his wisdom with me and also for his valuable support. I am thankful to my college too, for providing me proper resources to explore my skill.

References

[1] Huang Lu, Jie Li, and Mohsen Guizani, "Secure and Efficient Data Transmission for Cluster-Based Wireless Sensor Networks", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014

[2] RuitaoXie and XiaohuaJia, "DRINA: Transmission-Efficient Clustering Method for Wireless Sensor Networks Using Compressive Sensing", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 3, MARCH 2014.

[3] E. Cohen and H. Kaplan, "Spatially-Decaying Aggregation Over a Network: Model and Algorithms," in ACM SIGMOD 2004, Paris, France, Jun. 2004.

[4] A. Sharaf, J. Beaver, A. Labrinidis, and K. Chrysanthis, "Balancing energy efficiency and quality of aggregate data in sensor networks," The VLDB Journal, vol. 13, no. 4, pp. 384–403, Dec. 2004.

[5] E. Cayirci, "Data Aggregation and Dilution by modulus addressing in wireless sensor networks," IEEE Communications Letters, vol. 7, no. 8, pp. 355–357, Aug. 2003.

[6] T. Abdelzaher, T. He, and J. Stankovic, "Feedback control of data aggregation in sensor networks," in IEEE CDC 2004, Atlantis, Paradise Island, Bahamas, Dec. 2004.

[7] S. Nath, P. B. Gibbons, Z. R. Anderson, and S. Seshan, "Synopsis Diffusion for Robust Aggregation in Sensor Networks," in ACM SenSys 2004, Baltimore, MD, US, Nov. 2004.

[8] F. Hu, X. Cao, and C. May, "Optimized Scheduling for Data Aggregation in Wireless Sensor Networks," Proc. Int'l Conf. Information Technology: Coding and Computing (ITCC '05), pp. 557-561, 2005.

[9] I. Solis and K. Obraczka, "The Impact of Timing in Data Aggregation for Sensor Networks," IEEE Int'l Conf. Comm.,vol. 6, pp. 3640-3645, June 2004.

[10] B. Krishnamachari, D. Estrin, and S.B. Wicker, "The Impact of Data Aggregation in Wireless Sensor Networks," Proc. 22nd Int'l Conf. Distributed Computing Systems (ICDCSW '02), pp. 575-578, 2002.

[11] J. Al-Karaki, R. Ul-Mustafa, and A. Kamal, "Data Aggregation in Wireless Sensor Networks—Exact and Approximate Algorithms," Proc. High-Performance Switching and Routing Workshop (HPSR '04), pp. 241-245, 2004.

[12] G. Robins and A. Zelikovsky, "Improved Steiner Tree Approximation in Graphs," Proc. 11th Ann. ACM-SIAM Symp. Discrete Algorithms (SODA '00), pp. 770-779, 2000.

[13] D.W. Carman, "New Directions in Sensor Network Key Management,"Int'l J. Distributed Sensor Networks, vol. 1, pp. 3-15, 2005.

[14] R. Yasmin, E. Ritter, and G. Wang, "An Authentication Framework for Wireless Sensor Networks Using Identity-Based Signatures," Proc. IEEE Int'l Conf. Computer and Information Technology (CIT), pp. 882-889, 2010.

[15] H. Lu, J. Li, and H. Kameda, "A Secure Routing Protocol for Cluster-Based Wireless Sensor Networks Using ID-Based Digital," Proc. IEEE GLOBECOM, pp. 1-5, 2010.

[16] J. Sun et al., "An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks," IEEE Trans. Parallel & Distributed Systems, vol. 21, no. 9, pp. 1227-1239, Sept. 2010.

[17] S. Even, O. Goldreich, and S. Micali, "On-Line/Off-Line Digital Signatures," Proc. Advances in Cryptology (CRYPTO), pp. 263-275, 1990.

[18] S. Xu, Y. Mu, and W. Susilo, "Online/Offline Signatures and Multi signatures for AODV and DSR Routing Security," Proc. 11th Australasian Conf. Information Security and Privacy, pp. 99-110, 2006.

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