JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ENERGY-AWARE CLUSTERING APPROACH FOR SECURED DATA TRANSMISSION IN WIRELESS SENSOR NETWORK

[1]Saziya Tabbassum, [2]Sanjeev Bangarh

Department of Computer Science,
OPJS University Churu, India
Email: saziyatabassum@gmail.com; sanjeevbangarh2012@gmail.com

Abstract : In Wireless Sensor Networks (WSNs) large number of sensor nodes is deployed in the required region for getting the information about the environment related to a particular application. These sensor nodes have limited battery source in most of the cases, therefore extending network lifetime in WSNs becomes one of the major challenge. WSNs have distributed nature, multi-hop data forwarding, and open wireless medium they are vulnerable to security attacks at various levels. For routing in WSNs hierarchical clustering based routing protocol LEACH is a successful protocol which utilizes energy of sensor nodes evenly. However, there exist some flaws in this protocol which can attract intruders and can cause serious damage to the network. In this paper, a secured version of energy-aware clustering approach is proposed to minimize the risk of attacks by the intruders either from outside or inside of the network. Furthermore, we propose a clustering approach in which the overall load of cluster head is balanced in each round and the intruders are detected before transmission of data to the base station so that information are safe. Simulation and analysis result shows a significant improvement in proposed work over other protocols like DEEC, LEACH in terms of various parameters i.e. lifetime of network, nodes death, network connectivity.

Keywords-WirelessSensorNetwork,LEACH,Attacks,Security,IntrusionDetection

I. INTRODUCTION

Wireless sensor networks (WSNs) consist of sensors used to monitor various physical and military applications such as inventory control, environmental monitoring, disaster management, target field imaging, etc. Due to the technological advancements in micro electrical mechanical systems (MEMS), wireless communication and digital electronics have proved low-cost, low-power multi-functional sensors with capabilities of sensing, data processing, and wireless communication within short range. Sensors are equipped with radio transceivers radio chip, embedded microprocessors and various sensors. These sensors are deployed based on the requirements of the applications either manually or can be scattered randomly in the required region without planning and should operate unattended for long period of time. Sensors have limited battery power and it is impossible to replace or recharge the battery in most of case therefore, energy of sensor nodes should be utilized very efficiently. Moreover, the sensors node sense data in the deployed region and then transfer those data to the base station either directly or via other sensor nodes which act as relay nodes if base station is not within communication range of sensor nodes. Furthermore, there comes some security related threats which may compromise the privacy of data, resources, network structure, and many more. There exist various kinds of threats which can modify or drop the information that is being transmitted to the BS from sensor nodes. Such threats to the network or data from outside of the network is done by outsider attacker but some threats like data modification of replication kind of attack can be done from inside the network by insider attackers. Security in WSNs mainly deals with data confidentiality, data integrity, authentication, non-repudiation, data freshness and availability. Hence, these networks require more effective and energy efficient schemes for secure routing and processing of information.

In recent years, various routing protocols have been proposed in order to minimize energy usage and prolong lifetime of network with energy aware protocols in WSNs [1, 2, and 3]. The main goal of designing routing protocol is to extend the lifetime of network by achieving higher energy conservation for transmission of data packet to the base station. The energy consumption for transmission of data packet from source node to the sink is square of transmission distance between source node and sink in case of single hop, but in case of multi-hop it is four times the transmission distance between source node and the sink [4]. The data packet received from the sensor nodes is aggregated by the cluster head to eliminate redundant data transmission. Various hierarchical routing protocols are proposed for balancing the load among the networks, efficient energy utilization [4, 5, and 6]. The main goal of these works is distribute whole load among the entire cluster by properly choosing cluster head so that early death of cluster head can be avoided hence, resulting in extended lifetime.

In recent years, it has been observed that various securities related threats may compromise the privacy of data, resources, network structure, and many more. Generally, attacks are classified as active and passive attacks. Active attacks used to misdirect, temper, or drop packets where Spoofed, altered or replayed routing information, selective forwarding, sinkhole attack, Sybil attack, wormhole attacks, HELLO flood attack are some of the routing attacks in sensor network [7]. In passive attacks, monitoring and listening of the communication channel by unauthorized attackers are done. The attacks against privacy are passive in nature where monitor and eavesdropping, traffic analysis, camouflage adversaries are some of the passive attacks. A wide variety of security mechanisms can be invented to counter these malicious attacks and some of which can be categorized as high and low level of security mechanisms. In a high-level category secure group management, intrusion detection and secure data aggregations are some of the mechanisms [8]. Key Establishment and Trust Setup, Secrecy and Authentication, Privacy, Robustness to communication, denial of service, Secure Routing, Resilience to Node Capture are some of the low-level security mechanisms [9].

Due to the advancement in communication, there are certain kinds of threats in the network related to data as well as resources too. To prevent from launching such attacks, security services such as authentication, integrity and freshness checking mechanism should be added to the LEACH sub-phases. Also, Trust-based variants of various protocols prevent these attacks by using reputation management methods which rely on the history of nodes before actions. For providing more security, hybrid trust-based schemes apply both cryptographic and trust management methods to protect LEACH against internal and external attackers [10, 11, and 12]. Adding security to cluster-based communication protocols for homogeneous WSNs, a security solution for LEACH is proposed in which building blocks from SPINS is used [13]. It is a suite of highly optimized security building blocks and relay solely on symmetric- key methods. In [14], authors aim to provide an improved secure and more energy efficient routing protocol called Light-weight Secure LEACH (LS-LEACH). The authors in [15] propose an Intrusion Detection System (IDS) mechanism to detect the intruders in the network which uses LEACH protocol for its routing operation. To compute the intrusion ratio (IR) by the IDS agent, authors use the detection metrics such as number of packets transmitted or received. The computed value shows the normal or malicious activity. Whenever the sinkhole attack is captured, the IDS agent alerts the network to stop the data transmission. Thus, it can be a resilient to the vulnerable attack of sinkhole.

II. METHODOLOGY

A. Basic Idea

In cluster based routing utilization of various methods are done to perform energy efficient routing in WSNs. Here, higher energy nodes are used to process and send the data and low-energy nodes are used to perform the sensing in the proximity target. Hierarchical routing is an efficient way to lower energy consumption within a cluster, performing data aggregation and fusion in order to decrease the number of transmitted messages to the BS. Hierarchical routing is mainly two-layer routing where one layer is used to select cluster heads and the other for routing as shown in fig 1.

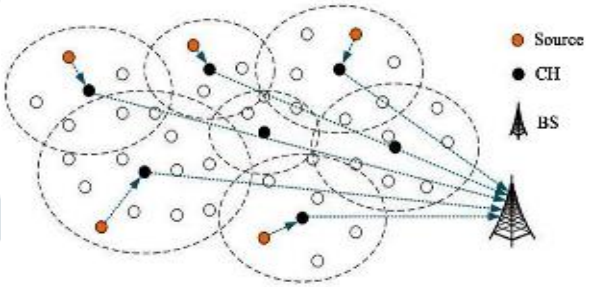

Figure 1: Clustering

LEACH (Low Energy Adaptive Clustering Hierarchy) is one of the hierarchical routing protocols, which is a cluster-based protocol for data transmission from the environment to the base station [4]. The operations of LEACH are divided into a number of rounds and each round consists of two phases: set-up phase, in which clustering is done and the steady state phase, in which data is being sent to the base station from all the sensors. Initially, when the clusters are formed in the set-up phase all sensor nodes decide to become a cluster head or not in the current round. This decision is made by node *n*, choosing a random number between 0 and 1. If the number is less than threshold value *T (n)*, then it becomes a cluster head (CH) for the current round where *T (n)* is given by

$$T(n) = \begin{cases} \frac{P}{1-P*(r mod \frac{1}{P})}, & if\ n \in G \\ 0, & otherwise \end{cases} \quad (1)$$

Where, *P* is the desired percentage of cluster head, *r* is the current round and *G* is the set of nodes that have not been cluster head in the last $\frac{1}{P}$ round.

It is assumed that all sensors deployed contain equal initial energy and sink is not limited by power supply. Based on [4], we use following energy model to calculate the energy consumption of sensors due to transmission (E_{Tx}) and reception (E_{Rx}) of data of size *k*-bit and distance *d* are given by:

$$E_{Tx}(k,d) = \left(E_{elec} + \mathcal{E}_{amp} \times d^2\right) \times k \quad (2)$$

$$E_{Rx}(k,d) = E_{elec} \times k \quad (3)$$

Where, E_{elec} , $\mathcal{E}_{amp}$ be the energy required by the electronics circuit and by the amplifier.

B. Algorithm Description

In the beginning we assume following assumption about the underlying network:

- All the sensor nodes are randomly deployed and base station is at the center.
- All sensor nodes are having similar functionalities and at the time of deployment they have same initial energy depending on the batteries they are equipped but base station is not limited by power source.
- All communications are over a wireless link which is established between two nodes only if they are within communication range of each other.
- Communications are bi-directional.
- The sensor nodes sense data and send it to the base station located at the center of the region.

The implementation of our proposed work can be divided into five phase and all those phases are executed in each rounds. Here, Phase 1and Phase 5 is very similar to the LEACH protocol whereas, Phase 2, 3, and 4 protects the network from external as well as internal attackers. The proposed work begins with round 1 and each round contains all of these five phases.

Phase1: Setup Phase

With the beginning of each round, sensor nodes which are deployed calculates its remaining energy based on equation (2), and (3), then transmits its location information within its communication range. Based on the equation (1) cluster heads are selected. Once the cluster heads are chosen complete network is divided into various clusters forming a hierarchy from sensor node at low level, cluster head in the next level and at last level of hierarchy is the base station as shown in figure 2.

Phase 2: Authentication

As all sensor nodes have assigned unique id while deployment, it id's of trusted nodes are maintained in the table of neighbor nodes and updated in each round.

Phase 3: Intrusion Detection

In this phase all sensor nodes are monitored for malicious node in each cluster. If any malicious node is detected it is marked as default and all the communication is declined from that node.

Phase 4: Encoding / Decoding Data for transmission / reception

In this phase, data to be send from cluster head to the base station are encoded so that any intruder if present cannot make any changes in the data. Similarly, decoding of data is done at the receiver end.

Phase 5: Routing

This phase is the last part of each round in which data collected from sensing region by nodes in cluster are transferred to the cluster head. The cluster head then aggregates the data, encode it, and then transmit it to the base station.

III. SIMULATION AND ANALYSIS

An extensive experiment is performed in our proposed work in this section using Matlab. Moreover, the performance of our proposed work is compared with similar protocols like LEACH, DEEC. Experiments of these protocols are done with varying number of sensors in simulation based environment. The simulation results shows that the proposed work have improvement over previous work in terms of lifetime of the network, overall system throughput.

A. Environment:

In our proposed work experiments were conducted on a diverse number of sensor nodes between 100 and 500 and cluster heads ranging between 15 and 50 in an area of 300 m × 300 m of target region. The initial energy of all the sensor nodes is assigned 2J and the base station have uninterrupted energy supply which is located in the center. For the energy model, the parameters are set as follows: E_{elec}= 50nJ/bit, $\mathcal{E}_{fs}$= 10pJ/bit/m^2, $\mathcal{E}_{mp}$0.0013pJ/bit/m^4. Energy consumption is calculated while data transmission from sensor nodes to CH within clusters and from CH to the BS either directly or via relay nodes based on equation (2) & (3). The sensor node deployment, cluster set-up and communication within network are shown in figure 2.

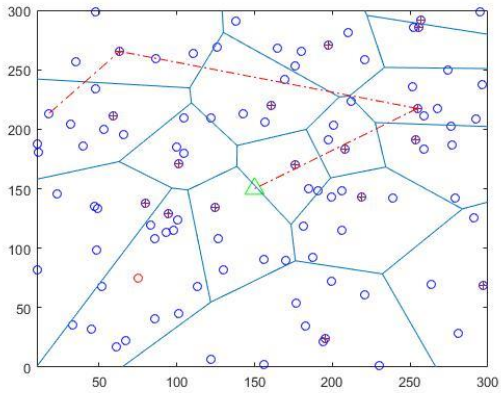

Figure 2: Sensor node deployment in the region

B. Performance:

Our proposed work is a clustering approach for secure data transmission in a WSN using energy efficient efficiently. Therefore our proposed approach consists of two parts: utilization of energy efficiently and secured routing approach in WSN. The performance of proposed approach is compared with DEEC and LEACH in terms of network lifetime, remaining energy of nodes. We compare various protocols on the basis of last node dead and number of dead sensor nodes with respect to number of rounds.

Figure 3 shows network lifetime with different number of sensors. The simulation result shows that the performance of proposed work is improved as the number of dead sensor nodes are less at particular round. It is because in this work we have considered the remaining energy of nodes in each round before selection of cluster heads and selecting only those nodes as cluster head which have higher residual energy hence, the utilization of energy in each round is balanced.

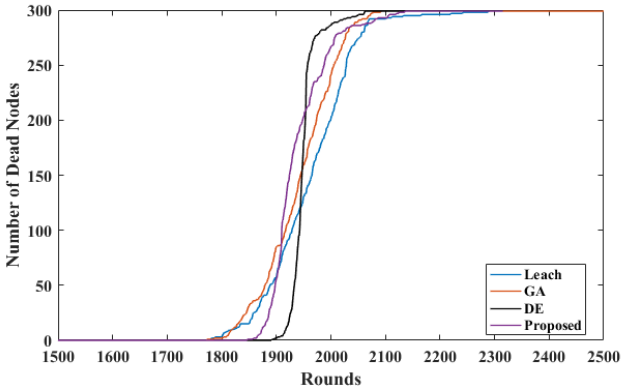

Figure 3: Network Lifetime

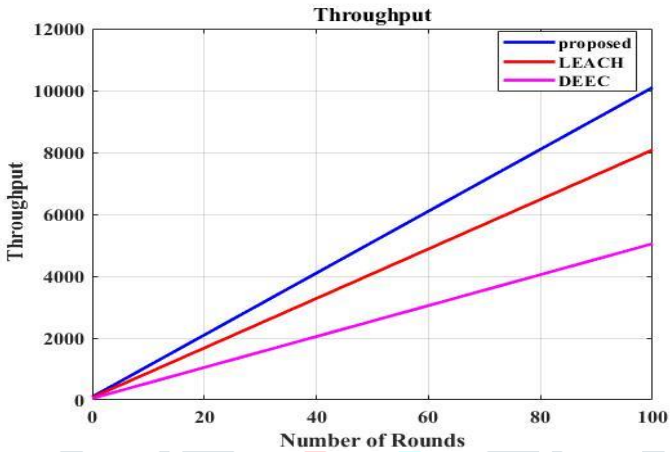

Figure 4: Overall system throughput

Furthermore, in our proposed work we have considered secured transmission of data from sensor nodes to cluster heads and from cluster heads to the base station. For secure data transmission, the network and data are protected from the intruders for which we have used intrusion detection system along with authentication of nodes in the network. Figure 4 shows the overall throughput of the system in which it shows successful transmission of data from sensor nodes to the base station safely. The simulation result shows that the proposed protocol has the highest throughput with respect to number of rounds when compared with LEACH and DEEC. In the proposed approach has higher packet delivery ratio and lower packet drop ratio because the intrusion detection system finds out intruders if any present in the system which may cause Sybil attack, selective forwarding attack, and HELLO flood attack.

IV. CONCLUSION

In this paper, we propose an energy-aware clustering approach for secure data transmission in wireless sensor network. In the proposed work we have extended the network lifetime by selecting the cluster head which have residual energy higher than the threshold value in each round so that lower residual energy node does not get exhausted easily hence increase in network lifetime. Moreover we have also authenticated all the sensor nodes at the time of deployment so that network can be secured from the outsider attackers. But if somehow attacker is present inside the network for that we have considered an intrusion detection system which detects malicious node inside the network and protect it from insider attackers. The simulation result shows that proposed protocol outperforms other existing protocols in terms of various metrics.

V. REFERENCES

[1] Md. Solaiman Ali, Tanay Dey, and Rahul Biswas, “Advanced LEACH Routing Protocol for Wireless Micro sensor Networks”, Department of Computer Science & Engineering Khulna-9203, 5th International Conference on Electrical and Computer Engineering ICECE 20-22 December 2008.

[2] Siva D. Muruganathan, Daniel C. F. Ma, Rolly I. Bhasin, and Abraham O. Fapojuwo “A Centralized Energy-Efficient Routing Protocol for Wireless Sensor Networks”, IEEE Radio Communications March 2005.

[3] Arati Manjeshwar and Dharma P. Agrawal, “A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks”, Center for Distributed and Mobile Computing OH 45221.

[4] Heinzelman, W. B., Chandrakasan, A. P., Balakrishnan, H. (2002), “An application specific protocol architecture for wireless micro sensor networks”. IEEE Transactions on Wireless Communications, 1(4), 660.

[5] K. Pratyay, S.K. Gupta, P.K. Jana, “A novel evolutionary approach for load balanced clustering problem for wireless sensor networks”, Swarm Evol. Comput.12 (2013) 48–56.

[6] Pratyay Kuila, Prasanta K. Jana: “A novel differential evolution based clustering algorithm for wireless sensor networks”, Applied Soft Computing, 2014 Elsevier B.V.

[7] Culler, D. E and Hong, W., “Wireless Sensor Networks”, Communication of the ACM, Vol. 47, No. 6, June 2004, pp. 30-33.

[8] Adrian Perrig, John Stankovic, David Wagner, "Security in Wireless Sensor Networks" Communications of the ACM, Page53-57, year 2004.
[9] Pathan, A.S.K.; Hyung-Woo Lee; Choong Seon Hong, "Security in wireless sensor networks: issues and challenges" Advanced Communication Technology (ICACT), Page(s):6, year 2006.
[10] Simplcio Jr MA, Barreto PSLM, Margi CB, Carvalho TCMB, "A survey on key management mechanisms for distributed Wireless Sensor Networks", Journal of Computer Networks 2010.
[11] Jøsang, A and Ismail, R., ''The Beta Reputation System", 15th Bled Electronic Commerce Conference Bled, Slovenia, 2002.
[12] Zhu, S, Setia, S, Jajodia, S, "Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks", 10th ACM conference on Computer and communications security, 2004.
[13] Adrian Carlos Ferreira, Marcos Aur´elio Vila¸ca, Leonardo B. Oliveira, "On the Security of Cluster-based Communication Protocols for Wireless Sensor Networks".
[14] Muneer Alshowkan, Khaled Elleithy, Hussain AlHassan, "LS-LEACH: A New Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks", Department of Computer Science and Engineering, University of Bridgeport, USA.
[15] Ranjeeth Kumar Sundararajan and Umamakeswari Arumugam, "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks", School of Computing, SASTRA University, Tirumalaisamudram, Thanjavur, Tamil Nadu 613401, India.