Open access Journal International Journal of Emerging Trends in Science and Technology
IC Value: 76.89 (Index Copernicus) Impact Factor: 4.219 DOI: https://dx.doi.org/10.18535/ijetst/v4i8.42

Trust-Based Malicious Node Detection and Routing in Wireless Sensor Networks

M.Rajeshkumar[1], N.Thangamani[2], Dr.G.Dalin[3]
Assistant professor [1], Assistant professor [2],
Department of Computer Applications [1], Department of Computer Science [2]AJK College of Arts and Science,Coimbatore-641 020, India.
[3]Asst Professor & Placement Officer PG & Research Dept of Computer Science Hindusthan College of Arts & Science,

ABSTRACT: Wireless Sensor Networks (WSN) have arisen as a significant innovative area in wireless technology. In the nearby future, WSN are projected to comprise of thousands of sensor nodes, each having sensing proficiency with restricted energy, computational and communication power. In the previous work, Hierarchical Energy-Balancing Multipath routing protocol for Wireless Sensor Networks (HEBM) is introduced to improve the energy consumption and network lifetime. However it does not consider the security of the sensor network. To solve this problem the proposed system introduced a Trust-based Malicious node Detection and Routing (TMDR) approach. Based on the trust calculation the malicious nodes are detected and eliminated from the network. Then an optimal cluster head is selected based on the node weight, remaining energy and distance between sensor nodes and base station. Finally Time Division Multiple Access (TDMA) schedule allocate the time to each cluster member for packet transmission. The experimental results show that the proposed system achieves high throughput, energy consumption and packet delivery ratio.

Key words: WSN, cluster head, direct observation and routing

1. Introduction

Wireless Sensor Network (WSN) contains lot of sensor nodes employed collaboratively to attain a common mission. All the senor nodes in the network are responsible for collect the data from an environmental condition. And then the collected data are forwarded to the sink or Base Station (BS). These sinks establish the interface via which the WSN cooperates with the external world. Although the sensor nodes are responsible to self-organize and collaborate together in order to create and preserve the network [1]. These nodes are regularly tiny in size with restricted dispensation power, limited memory and limited power [2] [3].

Energy efficiency, routing and attacks are major problem in WSN [4].The Quality of service (QOS) is important factor in all routing protocols [5]. These QoS requirements include end-to-end delay assurance, bandwidth storage, energy efficiency, packet loss and the network life time, etc. In WSN, there exist lot of algorithms to investigate the routing problem. But maximum of all try their finest to consider the energy efficiency because the energy is an important to sensor node. Only minimum protocols consist the QoS provision at the same time. Commonly, they can be divided into five categories: they are data-centric approach, hierarchical algorithm, location/ position-based approach, network-flow approach and QoS-constrained algorithm. Those typical protocols consists of include SPIN, Directed Diffusion, LEACH, GEAR.

Security in WSNs is as significant as in other pan aches of systems, particularly in armed forces and safety applications (e.g. intruder recognition) [6]. Attackers may attempt to thwart traffic in sites (i.e. perform a denial of service attack) to network. The attacker nodes in the network may affect the routing process. And also it can alter the transmission packets. In WSNs, lot of attacks is establishing that damages the life time of the network system. In the various attacks, a Sybil attack is the further most hazardous attack that disturbs the whole network.

2. Literature Survey

Gopalakrishnan and Ganeshkumar [7] designed a Secure Routing for Attacker Identification (SRAI) protocol to detect the malicious nodes in the WSN. The designed SRAI protocol computes the threshold value which is based on the successful packet transmission. It considered the threshold value as 50. If the current node packet transmission rate is greater than the threshold, the receiver assumes that the received packet was original. Then compute an acknowledgement and send back to the source node. Else it identified the received packet is modified by an attacker. Finally the destination node computes the misbehavior report and sent it to the source node via the intermediate nodes. The designed SRAI protocol achieves better end to end delay, throughput and packet delivery ratio.

Wu et al [8] designed a new malicious node detection approach which is based on trust based authentication algorithm. At first the nodes in the network are randomly initialized. Based on the fuzzy theory and revised evidence theory the malicious nodes are detected. The continuous observation and incorporation of the behavior of computed nodes are assists to find out the attacker nodes in a network. In addition Neighbor Node Trust approach is used to detect the malicious node. In this algorithm, the trust value of its neighboring nodes is computed. Based on this value, the neighboring node is classified as risky, malicious or trustworthy. It can able to detect the HELLO flood attack, selective forwarding attack, and jamming attack with high packet delivery ratio.

Lu and Valois [9] designed a Dynamic Directed Backbone (DDB) to constructs a backbone in WSN. The sensor nodes are initialized in the network. The backbone is consists of leader and gateway nodes. Each leader node groups the neighboring nodes to form a cluster. By using the gateway nodes the leader nodes are communicate with each other. The gateway nodes finish the connectivity of the backbone structure. The sink is connected with the backbone and the packet transmission is done over the backbone. Modifying the designed backbone arrangement to evade hotspots has relatively low overhead since only the intermediate nodes have to be informed if a backbone node switches roles with a regular node . However it does not suitable for large area network.

Yi et al [10] designed a power efficient and adaptive clustering hierarchy (PEACH) protocol to improve the network work lifetime in WSN. In this designed work, the nodes can be able to predict the source and destination of packet transmission. These packets are transmitted by hearing intermediate nodes. Without consideration of ACK, joining, leaving and scheduling messages the protocols forms the clusters according to the heard information. To achieve an adaptive multilevel clustering PEACH is introduced to work on probabilistic routing protocols. If the position details of each node is unavailable on the network the location-unaware PEACH protocol is utilized. The location-aware PEACH works while the localization approaches such as a GPS is obtainable on sensor nodes. The experimental results achieves high network lifetime, packet transmission ratio with lower communication overhead.

3. Proposed Methodology

The proposed system designs a Trust-based Malicious node Detection and Routing (TMDR) approach to improve the network performance.

The flow diagram of the proposed system is shown in figure 1.

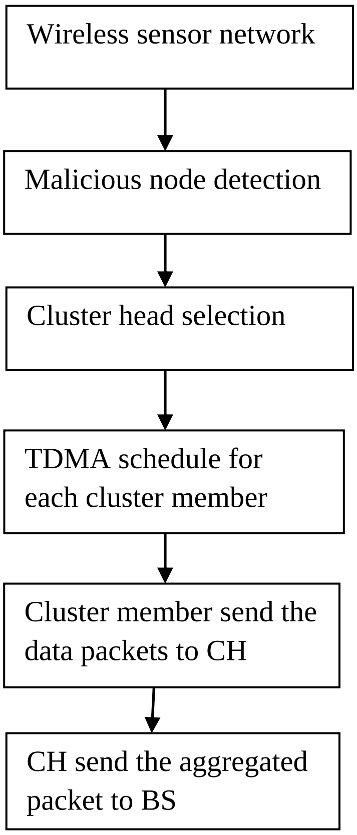
Wireless sensor network
Malicious node detection
Cluster head selection
TDMA schedule for each cluster member
Cluster member send the data packets to CH
CH send the aggregated packet to BS

Figure 1. Flow diagram of the proposed methodology

3.1.System model

In homogeneous WSN, the nodes are uniformly dispersed throughout the area. All the nodes in the network are communicates with Base Station (BS). They can utilize various power levels for communications. The BS is positioned far away from the monitoring field. Within the cluster range all the nodes are communicated with each other. The system divides the whole network operational time into a number of rounds. At first the cluster is formed and then data gathering, aggregation and transmission are performed. In this system the Cluster-Head (CH) is alive in all the time of a round and cluster member nodes are in sleep mode.

3.2.Trust Calculation Mechanism

In direct observation, the sensor nodes in the network are provides its trust worthiness using previous history. In this proposed work, according to the history of information that one sensor nodes collect the details about other nodes in the network. The trust value computed for direct observation collected from all the neighbor nodes, DT(x) is computed using the following equation.

$$T(x) = D(x) + TCH(x) \qquad (1)$$

Where,

Each sensor nodes direct observation D(x) is computed using the following:

$$D(x) = (CR - CD) + (DR - DD) \qquad (2)$$

Where, CR = Communication Packet Received, CD = Communication Packet Dropped , DR = Data Packet Received and DD = Data Packet Dropped . Based on the direct observation the malicious nodes in the network are detected. And finally the detected nodes are eliminated from the network.

3.3.HEBM initialization phase

Generally the sensor nodes are arbitrarily deployed in the network. Due to the longer distance transmission the sensor nodes are depleting their energy fastly. Once nodes are deployed there is no probability to change their position. In this initialization phase, BS broadcast the announcement message BS-Msg to all nodes in the network. Based on the received signal strength each node computes distance from BS. The calculated parameter is set as following: D (N, BS). Theoretically, the signal strength is inversely proportional to squared distance, and a known radio propagation model can be used to convert the signal strength into distance.

3.4.Neighbors' discovery phase

Neighbors Discovery (ND) is a significant in the initialization phase of WSN. Due to the limited energy the sensor nodes are sometimes go to sleep mode. Every node in the network execute at least one neighborhood discovery while WSN Construct. The main goal of this phase is collect more information to select the neighbor. The different form of the message is swapped between discoverer and nearest node to achieve transmission and to report the selected neighbors.

The neighbors table is constructed at the end of neighbor node discovery phase.

To compute the node weight each node sends a Discov-neigh-msg which has its identifier. Every nodes in the network are receives the message and reply Discov-neigh-msg message of similar type. The neighbors with a better link quality are important to select a neighboring node. The retransmission is required because of neighbors with bad link quality. Due to the retransmission lot of energy is exhausted and the consistency of the network function is reduced. So the energy efficiency is important factor to achieve a reliable transmission.

At starting the designed protocol send a Discov-neigh-msg. Then the time the discoverer sends the first broadcast, and a timer ts-discov is started concurrently. The nodes are receiving or wait for broadcast received messages when the timer is running. It includes the source as neighbor'(s) of the neighbor and send an acknowledgment (ack) back to the discover.

3.5.Cluster head selection phase

In order to improve energy efficiency the clustering is an important factor. Each cluster consists of Cluster Head (CH) and cluster member. Each CH collects the data from cluster member and it transmits to Base Station (BS). In this work an efficient CH is selected based on the combination of following factors,

(i) The distance among node and BS
(ii) Remaining energy of the node and its neighbouring nodes
(iii) The distance among the nodes neighbouring nodes.
(iv) Weight of the Node

$$\beta_1(i,j) = 1 - \alpha_1\left(1 - \frac{D_{Bs,i}}{D_{Bs,j}}\right) \quad (3)$$

Where, D_{Bs},i: the distance between the node "i" and BS, $D_{Bs,j}$: the distance between the node neighbor "j" and BS.

$$\beta_2(i,j) = 1 - \alpha_2(1 - \frac{NW_i}{NW_j}) \quad (4)$$

Where, Nw_i: Node-weight of node i, Nw_j: Node-weight of node neighbor j

$$\beta_3(i,j) = 1 - \alpha_3(1 - \frac{E_i}{E_j}) \quad (5)$$

Where, $E_{r,i}$: Residual energy of node i , $E_{r,j}$: Residual energy of node neighbor j

$$P_{ch}(i,j)=\text{Max}\ \left[1 - \sum_{i,j=1}^{n} \beta_1(i,j), \beta_2(i,j), \beta_3(i,j)\right] \quad (6)$$

Based on the P_{ch}(i,j) value an efficient CH is selected. After the CH selection, data transmission occurs between cluster member and CH. The main goal of the each CH is having three responsibilities. The first one is collect the data from cluster member nodes continuously. Second one is, it compute the Time Division Multiple Access (TDMA) schedule. By using this time scheduling process each cluster members are having separate time period to send the data for CH. Finally each CH sends the aggregated data to BS.

4. Experimental Results And Discussion

The performance of the newly introduced Trust-based Malicious node Detection and Routing (TMDR) system is compared with the already available HEBM protocol. The experiments are carried out employing an NS-2 simulator. The comparison of the already prevalent and the newly introduced techniques are carried out in terms of energy consumption, throughput and Packet Delivery Ratio (PDR).

Energy Consumption

Energy consumption is defined as the average energy required for the transmission, receipt or forwarding operations of a packet to a node present in the network during a given period of time.

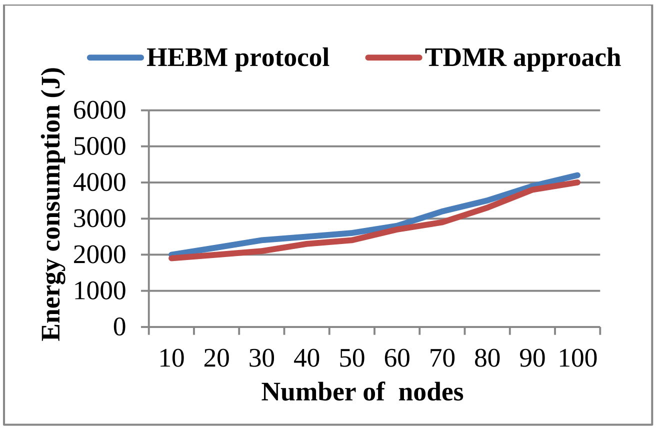

Figure 2: Energy consumption

Figure 2 depicts the comparison made in terms of energy consumption between the already HEBM method and designed TDMR methods. In this research, first the adversarial nodes are identified by employing trust based mechanism. The identified nodes are eliminated from the network. Each of the sensor nodes present in the cluster transmit their information to the CH. Then this CH transmits the gathered data to the BS. Thus, it enhances the network's energy efficiency. It is evident from the graph that the TDMRscheme yields lesser energy consumption compared to the already available technique.

Packet Deliver Ratio (PDR)

This metric refers to the ratio of the number of successfully transmitted data packets to the sink over the total number of packets produced by every source. A bigger percentage of the packet delivery ratio helps in increasing the network robustness and QoS satisfaction.

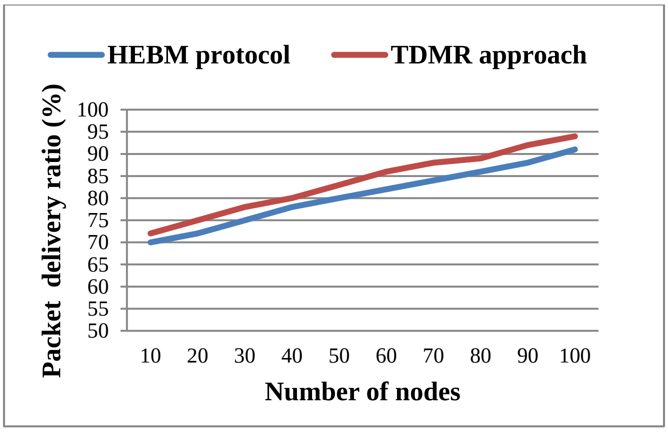

Figure 3: Packet Deliver Ratio (PDR)

Figure 3 provides the comparison made in terms of packet delivery ratiobetween the already available HEBM method and designed TDMR methods. The number of nodes is plotted along the x-axis and packet delivery ratio plotted along the y-axis. For the purpose of improving the packet delivery ratio the designed system took energy, direct observation into account for adversarial node identification. It is evident from the graph that the new TDMR mechanism attains a higher packet delivery ratio in comparison with the prevalent techniques.

Throughput

Throughput is defined as the rate in which the data packets are transmitted with success over the network or communication links. It is measured in bits per second (bit/s or bps). It is also indicated by units of information that get processed over a specified time slot.

$$\text{Throughput} = \frac{\text{Number of delivered packet} * \text{packet size}}{\text{Total duration of simulation}}$$

(7)

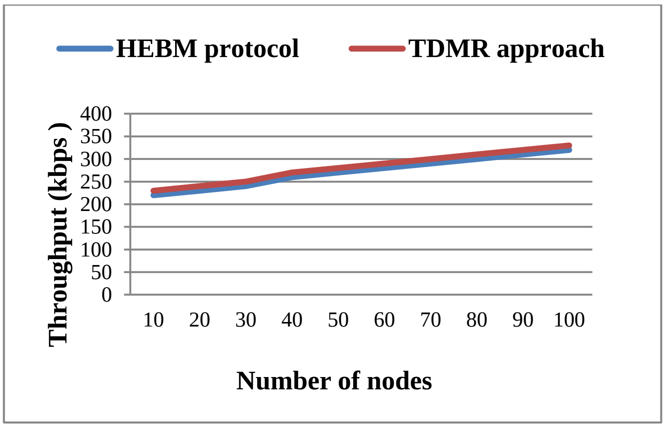

Figure 4: Throughput

Figure 4 indicates the comparison made of performance in terms of throughput for the available already HEBM method and designed TDMR methods. The number of nodes is plotted along the x-axis and throughput is plotted along the y-axis. It is made evident from the graph that the designed TDMR mechanism offers a higher throughput compared to the other prevalent techniques.

5. Conclusion

The proposed system design a Trust-based Malicious node Detection and Routing (TMDR) approach to improve the packet delivery ratio and network life time. The node trust is computed by using trust computation mechanism. An efficient cluster head is selected according to the remaining energy of node, node weight and distance between sensor nodes and base station. The TDMA schedule the time slot to each cluster member for efficient packet transmission. The experimental results show that the proposed system achieves high throughput, energy consumption and packet delivery ratio.

References

1. Liu, M., Cao, J., Chen, G. and Wang, X., 2009. An energy-aware routing protocol in wireless sensor networks. Sensors, 9(1), pp.445-462.
2. Alsaedi, N., Hashim, F. and Sali, A., 2015, Energy trust system for detecting sybil attack in clustered wireless sensor networks. In Communications (MICC), 2015 IEEE International Conference on 12th Malaysia pp. 91-95.
3. Vamsi, P.R. and Kant, K., 2014. A lightweight sybil attack detection framework for wireless sensor networks. Seventh International Conference on Contemporary Computing (IC3), pp. 387-393.
4. Vamsi, P.R. and Kant, K., 2014, Sybil attack detection using sequential hypothesis testing in wireless sensor networks. International Conference on Signal Propagation and Computer Technology (ICSPCT), pp. 698-702.
5. Amuthavalli, R. and Bhuvaneswaran, R.S., 2014. Detection and Prevention of sybil attack in Wireless sensor network employing random password comparison method. Journal of Theoretical & Applied Information Technology, 67(1),pp. 236-246.
6. Shi, W., Liu, S. and Zhang, Z., 2015. A Lightweight Detection Mechanism against Sybil Attack in Wireless Sensor Network. KSII Transactions on Internet & Information Systems, 9(9),pp. 3738- 3750.
7. Gopalakrishnan, S. and Ganeshkumar, P. 2014. Intrusion detection in mobile Adhoc Network using secure routing for attacker identification protocol. American Journal of Applied Sciences 11(8), pp. 1391- 1397.
8. Wu, R., Deng, X., Lu, R. and Shen, X., 2015. Trust-based anomaly detection in emerging sensor networks. International Journal of Distributed Sensor Networks, 11(10), p.363569., 1-14.
9. Lu, J.L. and Valois, F., 2007, On the data dissemination in wsns. Third IEEE International Conference on In Wireless and Mobile Computing, Networking and Communications, 2007(WiMOB 2007), pp. 58-58.
10. Yi, S., Heo, J., Cho, Y. and Hong, J., 2007. PEACH: Power-efficient and adaptive clustering hierarchy protocol for wireless sensor networks. Computer communications, 30(14), pp.2842-2852.