INTEGRATION OF ASSEMBLING NODES USING MASTER SLAVE

Kowsik Siddarth.1, Natarajan Shruthi2, Sibi Aman3, Aishwarya.D4

1234SRM INSTITUTE OF SCIENCE AND TECHNOLOGY, CHENNAI

johnpaulreddy875@gmail.com

Abstract: Clustering is one important method for extending the network energy in WSNs. It mires grouping of sensor nodes into clusters and recruiting cluster Head (CHs) for all the clusters. CHs rally the data from relevant cluster’s nodes and forward the accumulated data to cluster Master. WSN are inclusive to various attacks in which Blackhole a kind of Denial of Service (DoS) attack is very crucial to encounter and defend the mechanism. The attackers elect a set of neighbor nodes in the network and reconstruct the route to downfall the received packets instead of forwarding them to the sink node, which will emerge in a situation where packets enter the blackhole area but never reaches the destination resulting in higher end-to-end delay and decline in the throughput. In this paper, We use SHA(Secure Hashing algorithm) Cluster based Futuristic Method for detecting black hole attack in WSNs. By using the proposed technique we adapts filtering technique to the attacker and prevent from the BlackHole attacker and improving the performance such as throughput, delay and packet delivery ratio.

Keywords- Dos, Support vector machine, futuristic method of prevention, Secure hash algorithm, Hash function. Malicious node, Black hole, Secure energy efficiency.

1. Introduction

WSN are inclusive to various attacks in which Blackhole a kind of Denial of Service (DoS) attack is very crucial to encounter and defend the mechanism as it collects the data and drops the packet instead of forwarding which in turn creates a black hole region. In order to detect the attacker, we better have to collect sensory data from all nodes. However, this strategy requires much more energy consumption and its not secure. Traditional routing protocols rivet on choosing the optimal path to destination, unlike the conventional routing protocols which derogate delay. Most of the routing protocols for WSNs strive to optimally utilize the minimal resources with the network nodes. One way to transfer the data among the nodes efficiently is by using “cluster master” method. Clustering is an approach using which we can ease the implementation of routing and resource management in WSN.

We have proposed a Secure Energy Efficient algorithm for efficient transmission of data which will aid the Detection, Filtering and Prevention of Blackhole attack in Wireless Sensor Network. The novelty of the proposed idea is discussed in section-III which includes 5 phases which includes, cluster formation, election of master and cluster leader. Communication medium, detection and filtering of malicious node followed by a prevention technique. Section - IV shows how a secure transmission is obtained followed by simulation analysis. The work is concluded in section VI with the discussion of future work.

2. Effects of BlackHole attack on WSN

A. Packet delivery ratio (PDR):
It is the ratio of the number of data packets received by the destination to the number of data packets generated by the sources node[1]. When the node is attacked by the black hole malicious attack then the black hole will absorb all the data to itself and will not transmit the data to the destination node.

B. Throughput:
Throughput can be defined as the amount of data transferred from sender[12] to receiver in a given amount of time. It is measured in bits per second or packets per second. When there is a presence of black hole malicious attack then the throughput of the network will be less.

C. Delay:
The time taken by a packet to travel from source to destination is called the Delay. With the presence of a black hole malicious attacker there will be a lot of delay in the packets to reach the destination[2].

D. Denial of Service(DOS):
Denial of Service is meant to shut down a machine or network, making it inaccessible to its intended users. DoS accomplish this by flooding the target with traffic, or sending it information that triggers a crash[12]. It also pulls all the data to itself without sending it to the desired destination.

E. Information loss:
It is the loss of data packets during [3] the transmission of data from its sender to receiver.[15]The black hole malicious node absorbs all the data and so there will a lot of loss of information.

F. Energy Expenditure:
Sometimes sensitive data or the critical information is communicated to the destination node through an insecure medium. Thus,[4] WSN can be easily attacked by Denial-of-Service (DoS) attacks in such medium, which cause loss in information along with large energy expenditure in the network.

3. PROPOSED WORK.

A. Secure Energy Efficient Algorithm:
In this algorithm, We use SHA(Secure Hashing algorithm) a Cluster based Futuristic Method for detecting black hole attacks in WSNs. The Cluster Head [13] is intended to generate the secure packet by using SHA algorithm. It is helpful for secure data forwarding and data receiving via Cluster Master Futuristic Method, which prevents the cluster from the attacker then the SVM-Naive technique is employed to filter the records, and predict the attacker id in the Wireless Sensor Networks. The objective of this algorithm is to improve the transfer efficiency and to prevent the attack in the wireless sensor network[11]. The algorithm comprises of 5 phases they are,

A. Cluster formation.
B. Master node and Cluster Leader election.
C. Communication Phase.
D. Detection and filtering of malicious node.
E. Prevention of attack in WSN.
B. Cluster Formation:

Since the clustering principle is used, the nodes need to be organized / grouped which is done on based on the properties of the nodes (ie..) nodes with similar properties are grouped together. For practical implementation we have chosen Wsn in Healthcare Department. In the network a total of 6 clusters with 8 nodes each is created with the help of ospf- open shortest first algorithm a an Interior Gateway Protocol, used to distribute[9] IP routing information throughout a single Autonomous System in a network.
In the healthcare department, we have considered 6 departments that represent 6 clusters which are named as patient, doctor, department head, cleaning, managing and nursing. The node ID for the nodes in the cluster are given accordingly which helps us [11] to check the node status of a particular node. For each cluster in the network a particular range is set depending upon its placement in the network. The figure shows how the cluster is formed and the network is created with the help of a network simulation tool.

![Network Layout](image)

**Fig.4: Network layout**

C. *Master node and Cluster Leader election:*

Once we have created the network the next step is to elect the Cluster leader and Master node, which is done with the help of distributed cluster based algorithm, where each node sends a beacon message for checking the node status. Then using the protocol we divide the time into three different slots. Once the cluster is formed, we construct the routing Cluster based upon the limit [7] value of the network id. Out of all the 49 nodes, the node with the highest energy level is elected to be the Master Node using this protocol. Once the master is selected we then elect the cluster leader which is the leader node. The Cluster Head is selected based on the Energy level of the node among all the other nodes in the cluster.
If signature is not verified drop the index, return; else
{
    printf("Inter Node: Signature verified at %d! \n", index);
    rq->sign = index + 5;
    printf(" Inter Node: At node %d Sign: \n", index, rq->sign);
}

END OF DIGITAL SIGNATURE

STEP 3: Create a HASH FUNCTION by initializing temp variable that takes random has values during the check for the following condition;
for (i = 0; i < rq->max_hop_count; i++) Temp *= RANDOM_SEED *
    RANDOM_SEED;
    if (temp == rq->top_hash)
        printf("Hash function verified at %d\n", index);
    Else
        printf("Hash function not verified at %d\n", index);

D. Communication phase:
Now the Source node generate the packet based upon the interval time and the Source node calculates the neighbor node based upon the energy parameters. This protocol is used to define Node status i.e., whether the node is ‘sleep’ node or ‘wake up’ node (nid), and it also sends the RTS/CTS message for getting the channel status. Once the channel status is received and the [14] node status is active SHA is used for securing the communication. SHA stands for Secure Hashing Algorithm. It takes an input and produces a 160-bit (20-byte) hash value or known as hexadecimal number. SHA algorithm is used for node to node data transmission and reception. Source node send a hash packet to a sink. By using SHA Algorithm message should be transmitted in secure way[12] The Algorithm shown below shows how the secure hash algorithm works to secure the communication channel in the network.

Algorithm 1: SHA

STEP 1: Cache the broadcast ID
    id_insert(rq->rq_src, rq->rq_bcast_id);

STEP 2: Set up a SHA DIGITAL SIGNATURE
    if(( (ih->src_.addr_)+5)! = rq->sign)
        { printf("Inter Node: Signature not verified! at \n", index);
    
STEP 4: END OF HASH FUNCTION.

E. Detection and filtering of malicious node:
Generally, the sink is made to receive all the data from the nodes simultaneously. So the sink requires a lot of time to identify the corrupted data and to filter them out, hence an ideal method is required to reduce the load and traffic which can be done by [15] creating a set of clusters and bringing up a management system where the load is distributed. Hence all the leader nodes elected, collect the data from its respective cluster. After collecting the data from its respective clusters the
leader node sends the data to the “CLUSTER MASTER” which is placed near to the sink. Now in case of an attack for instance a BLACK HOLE ATTACK, where the attacker [9] collects all the data that is flowing within its range and intermediate range, In that case we need to come up with an algorithm to detect the presence of the attacker and to filter him out of the system. We have proposed a supervised machine learning technique to detect and filter the malicious node out of the network.

**SVM:** A Support Vector Machine (SVM) is a supervised machine learning technique that can be used for both classification and regression based problem. By using this technique we filter the node status and find the blackhole attackers and the normal user. The algorithm takes the node status as an [6] input and outputs a line that separates those classes if possible. Given below is the algorithm of how the svm in implemented to create a output which includes a hyperplane that differentiates two classes output if possible. Using the node’s database we feed the input the machine, in case of any anomalies present or a malicious presence in the node the svm can detect [11] it and filter it out of the network. Blackhole attacks occur when an intruder captures and reprograms a set of nodes in the network to block the packets they receive instead of forwarding them towards the base station. As a result any information that enters in the blackhole region is captured and doesn't reach destination. In this case the periodic database that is fed to the svm can detect the variation of that particular node in the network. Given below shows the algorithm of how svm is implemented to detect and filter the malicious node.

---

**Algorithm 2: SVM**

STEP1: Create a test case for all the input
STEP2: For each instance a predicted value and corrected value is initialised
STEP3: A fix for handling the test case StarIx:
for (int i = startIx; i < thesesInstances.numInstances(); i++){
  SparseInstance sparseInst = new SparseInstance(thesesInstance.instance(i));
  SparseInst.setDataset(thesesInstances);
}
STEP4: Print comparison of the two values for ‘not the same test case’
double correctValue = (double)sparseInst.classValue(); double predicted Value = this Classifier.classifyinstance(sparseInst);

---

**F. PREVENTION OF ATTACKS IN WSN:**

Wireless sensor networks is and will always be prone to various attacks due to its presence in the environment. The most used applications of [12] wsn lies in personal and environmental monitoring. Some data are critical for instance the wireless health monitoring where there is no place for compromises in the integrity of the system as the data is critical. A small change would put the entity in a bad state, hence the Wsn should have the capacity to prevent various types of attacks that compromises the network. One such attack which is difficult to defend is the BlackHole Attack which causes delay in the packet delivery and brings down the throughput of the system. We have implemented a **Futuristic method** of detection and prevention against blackhole attack.
that detects attacker node and prevents it before it affects the sensor network. This method has two step.

1. Validation process
2. Response process

**G. Validation Process:**

The cluster head(CH) sends a validation packet to every cluster member that contains node id and validation packet.

**H. Response Process:**

All the cluster member response with response packet after receiving the validation packet. If cluster member sensed the data packet but it consumes the data and act like a blackhole instead of forwarding to the Cluster Head. The Cluster Head detects the blackhole by its id.

---

**Algorithm 3: Futuristic method for prevention**

STEP1: Check all the instances of the input periodically

STEP2: Maintain a request table

STEP3: Create a structure and set the delay period and create a soft state for route requests

STEP4: Create a `rp_dst` function which is the destination of the data packets

STEP5: Initiation

```c
#ifdef DEBUG
fprint(stderr, "%d - %s: received a REPLY\n", index, _FUNCTION_);
#endif //DEBUG
```

STEP6: Check for reply if a reply in obtained, reset the “soft state” maintained for route requests in the request table. We don't really have a separate request table. It is just a part of the routing table itself

```c
rt = rtable.rt_lookup(rp->rp_dst);
```

STEP7: If the `rt` entry is not in the host then, `rt = rtable.rt_add(rp->rp_dst);`

---

4. BLOCK DIAGRAM:

![Block Diagram](image.png)
5. SIMULATION RESULTS AND ANALYSIS

5.1 DELAY:
The simulation result shown below depicts how the delay which is the amount of time it is taken to push all the packets through the line, has considerably decreased which results in efficient transmission.

![Fig.5: simulation result (delay)](image)

5.2 THROUGHPUT:
The successful data rate of the packets transmitted has considerably increased in the simulation result shown below. A Comparison result which plots Time X Throughput of two algorithms DBCA and SEEA.

![Fig.6: simulation result (throughput)](image)

A. PACKET DELIVERY RATIO:
The simulation results shown below shows us the data packets received by the destinations to those generated by the source. The xgraph illustrates how the packet delivery ratio is improved by Secure energy efficiency algorithm against the Distributed cluster based algorithm.
6. CONCLUSION:

In this paper a Secure Energy Efficiency algorithm is proposed with with the nodes in the wireless sensor network can communicate securely and efficiently. We are concluding that the SEEA algorithm performs better than the distribution based cluster algorithms based on the simulation results. The futuristic prevention technique used here uses validation and response which prevents the blackhole attack. In future the scope for secure transmission can be enhanced by proposing deep learning techniques that can prevent the attack on the wireless sensor network by exploiting how the nodes in the network are managed so that they respond efficiently without compromising the resources.

7. REFERENCES:

[1] Energy-Efficient Abnormal Nodes Detection and Handlings in Wireless Sensor Networks, by Fei lei, Deng Zhao and Yucong Duhan.

[2] An Effective Energy-Harvesting-Aware Routing Algorithm for WSN-based IoT Applications by Thein D. Ngyuen, Jamil Y.Khan and Duy T.Ngo.

[3] Fuzzy-Logic-Based Clustering Approach for Wireless Sensor Networks Using Energy Prediction by Jin Syan Lee and Wei Lang cheng.

[4] Applying Intrusion Detection Systems to Wireless Sensor Networks by R.Roman, J.Lopez and Jianying Zhou.

[5] Tree based Distributed Clustering Routing Scheme for Energy Efficiency in Wireless Sensor Networks by Pradnya M.Daflapurkar, Meera Gandhi and Bhagwan Patil.

[6] A Security Framework for Cluster-Based Wireless Sensor Networks against the Selfishness Problem by Zeba Ishaq, Seongjin Park and Young Wan Yoo.

[7] Energy Efficient IOT based on wireless sensor Networks for Health care by Youngbok Cho, Minkang kim and Sung Hee woo.

[8] An Efficient Protocol for load balancing multipath routing in mobile ad-hoc networks. by Anshuman Bhattacharya and Koushik Sinha.

[9] Detection of black hole attack in wireless sensor network using UAV by Maryam Motamedi and Nasser Yazdani.
[10] Protocols and Architectures for Wireless Sensor Networks by Holger Karl.

[11] Detection and isolation of black hole attack in wireless sensor network using hybrid techniques (Received packet and time delay) by Arshdeep Kaur.

[12] Security against Black Hole Attack in Wireless Sensor Network by Binod Kumar Mishra, Mohan C. Nikam, Prashant Lakkadwala.

[13] Modified Ant-AODV-VANET Routing Protocol for Vehicular Ad Hoc Network by Atreyee Datta.

[14] Support vector machines by M.A. Hearst, S.T. Dumais, E. Osuna, J. Platt, B. Scholkopf.

[15] Secure Hash Algorithm based on Efficient Chaotic Neural Network by Nabil Abdoun, Safwan El Assad, Mohammad Abu Taha, Rima Assaf, Olivier Deforges, Mohamad Khalil.