Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

A Detection of Malicious Nodes in HCCT Model for Wireless Sensor Network

Dr.M.S.Nidhya [1], Dr.M.Vanitha [2], Dr.L.Jayanthi [3], Mr.L.Vadivel Kannan [4], Mr.S.Ajay [5], Mr.S.Gowdham Kumar [6], Dr.S.Sangeetha[7]

[1]Associate Professor, Department of Software Engineering, Periyar Maniammai Institute of Science and Technology,Vallam,Thanjavur, Tamilnadu. Email Id:nidhyaphd@gmail.com

[2] Associate Professor, Department of Electronics and Communication Engineering, Saveetha Engineering College, Chennai, Tamilnadu. Email Id: vanitha@saveetha.ac.in

[3]Assistant Professor, Department of Electronics and Communication Engineering, Periyar Maniammai Institute of Science and Technology, Vallam, Thanjavur, Tamilnadu. Email Id: jayanthikesavan50@pmu.edu

[4]Assistant Professor, Department of Mechanical Engineering, PSNA College of Engineering and Technology, Dindigul-624622, Tamilnadu.Email Id:vadivelkannan79@gmail.com

[5] Assistant Professor, Department of Mechanical Engineering, Kongu Engineering College, Perundurai-638052.Tamilnadu. Email Id:ajusuku.405@gmail.com

[6] Training officer, PSG Industrial Institute (PSGCT), Peelamedu, Coimbatore-641001, Tamilnadu. Email id:saigowdham@gmail.com

[7] Assistant Professor, Department of Mathematics, Dhanalakshmi Srinivasan College of Arts and Science for Women (Autonomous), Perambalur-621212, Tamilnadu. Email Id: sangeethasankar2016@gmail.com

ABSTRACT

Detection of malicious node is one of the challenges faced by the sensors in wireless sensor network. Clustered architecture is efficient one for detecting the malicious node and saves energy of the node. Sensors present in the cluster will monitor the information and send the information to cluster head by applying hamming code method. Based on the first cycle transmission, bit position will vary among the sensors. Cycle transmission and forwarding node information are

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

stored as table called cycle table by cluster head. Cluster head will process the received information based on the cycle table. Mismatch in the table and suspicious node count, will leads to the detection of malicious node by the cluster head.

Keywords: Sensor, Cluster, hamming code, malicious, cycle table.

INTRODUCTION

Wireless sensor network (WSN) refers to a group of spatially dispersed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. Three types of architecture is there they are flat, cluster and location. In a flat architecture all the sensor nodes are scattered in the environment and monitor the environment then they send the information to the sink node. Detection of malicious node is difficult one in flat architecture when compared to hierarchical. In Hierarchical architecture scattered sensors are in groups called cluster.

Each cluster has a head which will protect and controls the sensors belong to it. [1] Sensor nodes [2] have limited resources such as power, computation and communication capability, memory, and transmission range, whereas the gateway has an abundance of these resources.

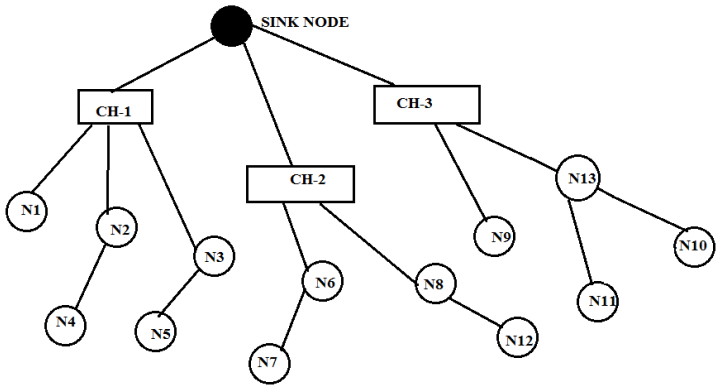

Fig.1: Clustered Architecture

In the above figure it is clearly illustrated clustered architecture. Group of sensors are grouped under three clusters CH-1, CH-2 and CH-3. Each Cluster head will control and aggregate the information from there group sensors.

Cluster head position is a rotational basis, a node which is having a good energy level will be considered as a next cluster head. During cluster head rotation information about the cycle table will also be handed over to the new cluster head.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

Security[3] in the Wireless Sensor Networks has various difficulties, some common are: dynamically changing topology, wireless communication among the sensor nodes, infrastructure-less framework, and limited physical resources like energy source, memory capacity and very low communication bandwidth. A malicious node is defined as node seeking to deny service to other nodes in the network. The node which modifies data before transmission or after transmission is known as malicious node.

Generally [4] malicious node detection is a difficult one because a node which listen the entire network it absorbs every activity of the network. Then it will start to corrupt the data inside the network.

Malicious node will corrupt the data which it received from the other node then it will forward the corrupted information. Messages will also be dropped by it. If the trust mechanism is used to find the malicious node then it will act as a normal node and score good trust then it will start to drop or modify the packets in the network and maintain a good trust level.

The essential work of cluster head is to aggregate data from the sensors in its group. The role of Cluster Head usually rotates between nodes in the cluster. Hamming code is a set of error-correction codes that can be used to detect and correct the errors that can occur when the data is moved or stored from the sender to the receiver. An error during transmission is also being corrected in this paper.

To secure the network, cryptography concept is used. But the node's memory capacity is very low and energy will be consumed for this process.

RELATED WORK

[5] Reviewed a number of algorithms which finds a malicious node in wireless sensor networks and concluded that Genetic cryptography algorithm is a best one for detection of malicious node. [6] Trust mechanism is used to detect a malicious node that acts as a sink hole. Packets dropped by malicious node are recovered by a transport protocol. [7] Proposed EERN algorithm and introduced two nodes called vigilant node and aggregator node which finds malicious node, faulty node and dead node also.

[8] Proposed ERLEN model find a reliable node to forward a packet and eliminate malicious node from packet routing [9] Discuss the usefulness of two-dimensional distance based localization algorithms when the number of malicious sensors is equal to or greater than a certain threshold. They proved that some algorithms are able to detect the location of the malicious nodes if the number of malicious nodes is under $(n – 2)/3$, where n is the number of nodes in the network.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

[10] Detecting malicious node using Hamming code residue method. Security code is generated by sensors but in prescribed time to live (TTL). Malicious node will take more time to analyse the security code. So the time will exceed the (TTL). By using this method, malicious node can be detected, not only detection of malicious node, it improves the packet delivery ratio (PDR) and reduces the delay in the network. Hamming residue method, this method is responsible for providing security to WSNs beside the malicious attacks without any key distribution mechanism.

[11]Proposed decentralised malicious node detection technique based on receiver signal strength indicator. This technique will localise and detect the malicious node in a small covered area.[12]Proposed an algorithm which selects a shortest path and deterministic strategies that regularize the power consumption, and cares different routing methods to secure the data. But, this strategy will fail because it is not considering the energy of the node in WSNs.

[13] Proposed graph theory concepts to overcome from the node failure or compromised node and find out the shortest reliable path from sender node to sink node. [14] Comparison between flat and hierarchical architecture in power consumption and the lifetime of the network. Comparative study states that hierarchical architecture has more advantage than flat architecture like well structured, easy management, less power consumption, high lifetime and flood problem is avoided.

HAMMING CODE AND CYCLE TEST MODEL (HCCT)

Sensor nodes are deployed in the monitoring environment. Sensors are grouped into number of clusters. This group of sensors are governed by cluster head. Cluster head position is rotational basis. Depending on the energy level of sensor nodes in the group, head position is assigned to the sensor.

Based on hamming code method data can be send from sender node to cluster head. A senor node will send information by appending parity bit based on the cycle which it sends the information to destination. Only four cycles are allowed per sensor. If the sensor complete it’s forth cycle then it starts from first cycle.

Cycle information and hop number is maintained as a table by the cluster head. Whenever the cluster head position changed the table will be forwarded to the forth coming cluster head. Then the new cluster head will continue the process.

Generally malicious node send a data before that it will listen the transmission medium then it send the data. If it listens the medium every time data will be changed by each one of the cluster it will take a time to understand. In the meantime the cluster head will find the malicious node and eliminate it.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

If the node is too farther from the cluster head then the data send by that node will be forwarded by the intermediate node.

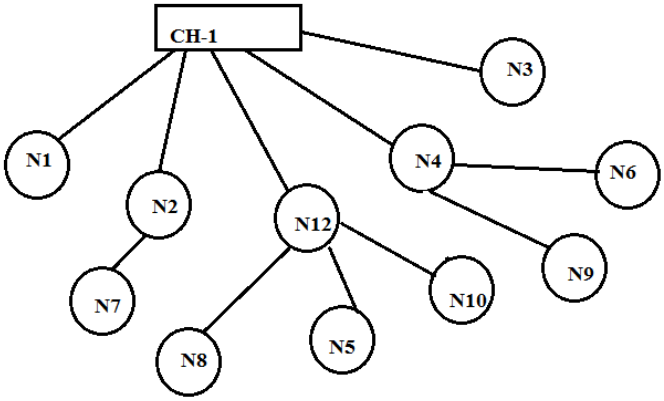

Fig.2: Malicious node in Cluster

CYCLE TABLE

Cycle table is maintained by the cluster head. In this table there three fields init. First one is node id, second one is node cycle and third one is suspicious. Suspicious field is to find malicious node.

Node id	Cycle	Suspicious
N1	2	-
N2	4	-
N3	1	-
N4	8	-
N5	1	1 (fn-n12)
N6	2	Fn-n4
N7	4	Fn-n2
N8	2	1 (fn-n12)
N9	1	Fn-n4
N10	4	1 (fn-n12)
N12	**M**	

Table.1: Cycle table

In this architecture the malicious node can corrupt the data in two ways. First one is it directly send a wrong information to the cluster head by listening one or two transaction by the other sensor node. It will be easily find out by the cluster head based on the cycle and node id.

Second one is, it will act as an intermediate node and corrupt the data then it will send to the cluster head. This act is easily detected by the cluster head through the third field in the table.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

HAMMING CODE BIT POSITION

In the fig-2, cluster head-1(CH-1) has 11 nodes, N1 to N12 nodes information are gathered by the ch-1 send to sink node. Each node will responsible for certain region. If an event occurred, a sensor responsible for that region will send the information to the cluster head. That event is the first event of the region and that is the first information send by the node means they have to send the information in hamming code first bit position.

1	3	5	7	9	11	13	14

Second cycle they are sending means they have to send in second bit position

2	3	6	7	10	11	14	15

Third cycle sensor have to send in 4^{th} bit position

4	5	6	7	12	13	14	15

Fourth cycle 8^{th} bit position

8	9	10	11	12	13	14	15

After completing fourth cycle, node has to enter into first cycle. The node information and cycle information's are stored in the cycle table which is present in cluster head.

In the table it is clearly illustrated that node N5, N8, N10 are denoted as a suspicious node not as malicious node. These three nodes send the information through the intermediate node called N12. It is assumed if a node send more than two times wrong information then that node will be a malicious node. That node information is send to all other node in the cluster. Other node will omit it from the packet routing.

WORKFLOW OF HCCT MODEL

Using the above format, sensors will send the information to the cluster head. Forwarding node will not change the format of the information. It forwards the information to the cluster head or other intermediate node. [15]Sensor which monitors the environment will send the information to the cluster head. So the sender has to follow the hamming code technique for sending the message. Forwarding nodes are not allowed to apply hamming code. Originator of the message is allowed to covert the message into hamming code. Sender information and receiver information is stored in header of the message. In addition to that, intermediate node information is also stored in the header.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

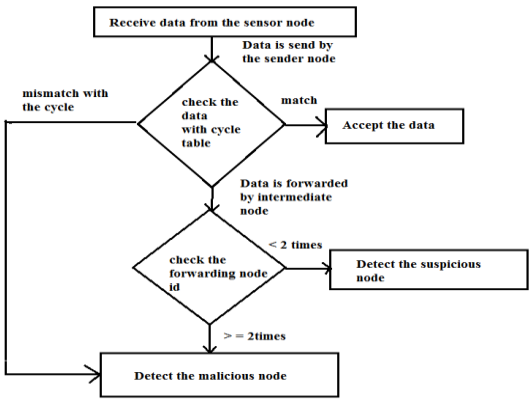

Fig.3: Detection of malicious node by cluster head using hamming code and cycle table

IMPLEMENTATION

Above fig-3 explain the work flow of cluster head to detect the malicious node. A cluster head receives data from sensors then it check with the cycle table whether it send the data in correct format or not. A sensor can send data to the cluster head directly or indirectly. A node sends directly to the cluster head, it checks with the table, match found accept the data. If it is not match that node is detected as a malicious node. A sensor send a data through intermediate node then the cluster head update with table and if the node is suspicious more than 2 times then it is a malicious node or else that node is indicated as suspicious.

HCCT model is implemented in Math Lab with n number of nodes. N number of nodes are scattered in a x and y plane. By sending and receiving the data from the node. Cluster head will detect the malicious node based on HCCT model.

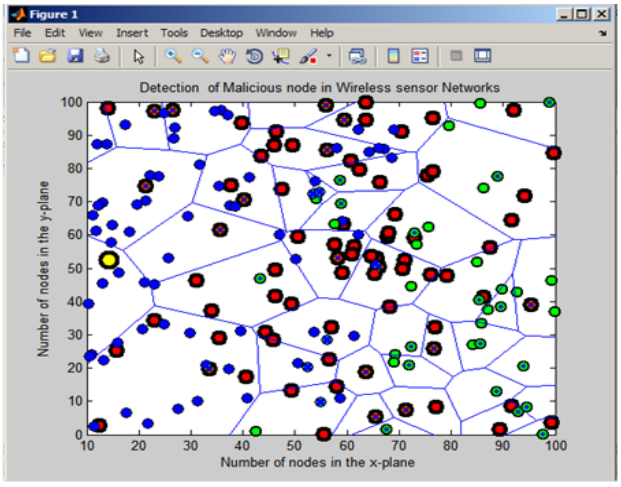

Fig.4: Nodes deployed in an environment

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

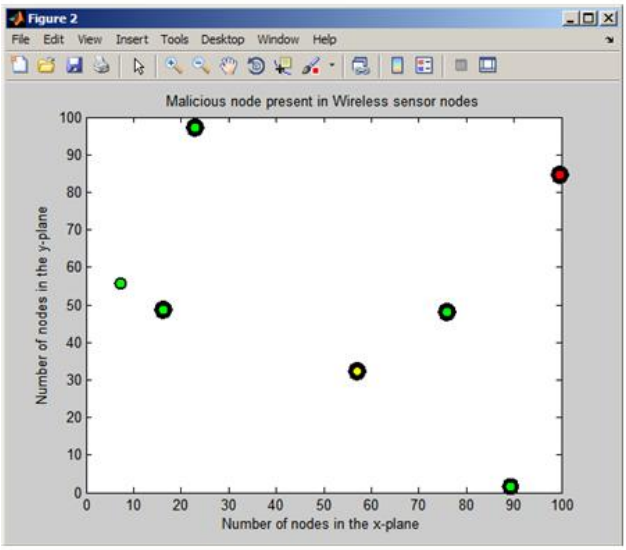

Fig.5: Detection of malicious node using HCCT model

PACKET DELIVERY RATIO

Moreover Packet delivery ratio will also be increased by using HCCT model. Packet Delivery ratio means number of packet delivered to the Number of packets send. In the below figure it is clearly illustrated that Packet delivery ratio is high if the clusters use HCCT model. Result shows HCCT model give good packet delivery ratio than other approaches.

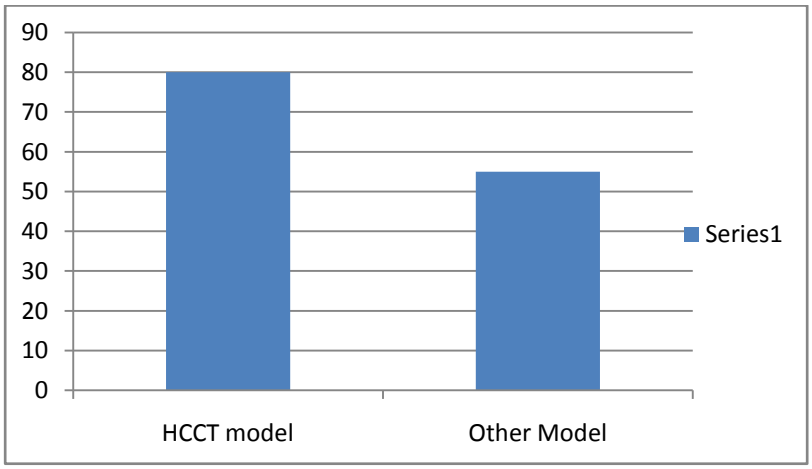

Fig.6: Packet delivery ratio

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

CONCLUSION

Using hamming code and cycle table a cluster head can efficiently detect the malicious node in the network and compared to other approach it shows high packet delivery ratio. HCCT model will work efficiently in clustered architecture. HCCT find the malicious node which wrongly sends the information, corrupt data during forwarding and drop data by malicious node. In future it will be extended to work in flat architecture.

REFERENCES:

[1] C. Karlof D. Wagner Secure Routing in Sensor Networks: Attacks and Countermeasures Proc.1st IEEE Int'l. Wksp. Sensor Network Protocols and Apps.2003.

[2] Y. Zhou, Y. Fang, Y. Zhang, Securing wireless sensor networks: a survey. IEEE Commun.Surv.Tutorials. 10(3) 6–28 (2008)

[3] R. Di Pietro, L.V. Mancini, C. Soriente, A. Spognardi, G. Tsudik, Data security in unattended wireless sensor networks. IEEE Trans. Comput. 58(11), 1500– 1511 (2009)

[4] H. Song S. Zhu G. Cao Attack-Resilient Time Synchronization for Wireless Sensor Networks Proc. 2nd IEEE Int'l.Conf.Mobile Ad Hoc and Sensor Sys. 2005

[5] P.Poornima, Dr.M.S.Nidhya," A Survey On Malicious Node Recognition In Wireless Sensor Network" Journal of Emerging Technologies and Innovative Research (JETIR), JETIR May 2019, Volume 6, Issue 5(338-344).

[6] M.S.Nidhya, Dr.R.Chinnaiyan "Improving the Reliability of data transfer against sinkhole in Wireless SensorNetworks–a Review." International Journal of Applied Engineering Research, Vol. 10 No.82 (2015).

[7] M.S.Nidhya, Dr.R.Chinnaiyan "Reliability Evaluation of Wireless Sensor Networks Using EERN Algorithm"https://doi.org/10.1007/978-981-10-8681-6_78 2019.

[8] M.S.Nidhya, Dr.A.Kannagi, Dr.R.Chinnaiyan "Evaluating Reliable Node in Wireless Sensor Network Using ERLEN Model" Jour of Adv Research in Dynamical & Control Systems, Vol. 11, No. 2, 2019.

[9] M. Jadliwala, S. Zhong, "Secure Distance-Base Localization In The Presence of cheating Beacon Nodes," in Mobile Computing, IEEE Transactions on vol.9, no.6, pp.810-823,Iune 2010

[10] MajidAlotaibi "Security to wireless sensor networks against malicious attacks using Hamming residue method" Alotaibi EURASIP Journal on Wireless Communications and Networking (2019) 2019:8 https://doi.org/10.1186/s13638-018-1337-5

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 1570 - 1579
Received 15 April 2021; Accepted 05 May 2021.

[11] Alaa Atassi, Naoum Sayegh, ImadElhajj, Ali Chehab, Ayman Kayssi "Malicious Node Detection in Wireless Sensor Networks"DOI: 10.1109/WAINA.2013.135

[12] D. Tang, T. Li, J. Ren, J. Wu, Cost-Aware Secure Routing (CASER) protocol design for wireless sensor networks. IEEE Trans. Parallel. Distributed Syst. 26 (4), 960–973

[13] M.S.Nidhya, Dr.R.Chinnaiyan "Shortest Reliable path for Wireless Sensor Network" International Journal of Pure and Applied Mathematics (IJPAM) Vol 117, No.20, pp.105-108, 2017.

[14] Hassan Oudani, Salah Ddine Krit "Energy Consumption in Wireless Sensor Network: Simulation and comparative study of flat and hierarchical routing protocols" IADIS International Journal on Computer Science and Information Systems vol.12, No. 1, pp.109-125.

[15] M. Mathankumar, S. Karthikeyani, S.Gowdham Kumar, N. Mahesh, N. J. Savitha and R. Rajaguru, "An Efficient Dynamic Key Generation Architecture for Distributed Wireless Networks," 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Tirunelveli, India, 2021, pp. 157-160, doi: 10.1109/ICICV50876.2021.9388551.