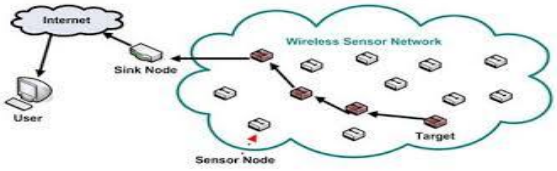
A NOVEL APPROACH FOR DETECTION AND PREVENTION OF INTRUSION IN WSN

Zarana Shah[1], Riddhi Patel[2]
[1]PG Scholar, [2]Assistant Professor, Department of Computer Engineering,
Swaminarayan College of Engineering & Technology, Kalol, Gujarat, India

Abstract: Wireless Sensor Network (WSN) has a great potential to be deployed in wide range of applications like consumer, industrial and defense sectors. The WSNs consists of thousands of sensor nodes which are battery-powered and one or more sinks or base stations which collect data from the nodes. These sensor nodes are battery-powered with a limited lifetime and additional energy can be harvested from the external environment. Wireless sensor networks are vulnerable to different kinds of attack. Misdirection attack is one of the Denial of Service Attack in which malicious node misdirect the packets to other nodes but not to the intended recipient. So it can reduces the network throughput and also increase end to end delay.
Keywords: Wireless sensor network, Cluster head selection, Misdirection Attack, Security

I. INTRODUCTION

In, wireless sensor network it consist multiple base station, sink nodes, and Sensor nodes, which are more prone to failure and energy drain, and their battery sources are usually not replaceable or rechargeable. In WSNs there are two other components, called 'base station' and 'aggregation points ' , which are more powerful resources than other normal sensors. Aggregation points collect information from their neighbors sensors, integrate them and then forward to the base stations according to multi-path routing to process gathered data. The below figure 1 explain basic working of Wireless Sensor Network.



A. Issues and Challenges of Wireless Sensor Network:

- Scalability: In wireless sensor network number of sensor node deployed in sensing area may be increase in the order of hundreds, thousands or more and routing scheme must be scalable enough to respond to the events.
- Fault tolerance: In wireless sensor network, in such cases sensor nodes may blocked or be fail due to physical damage ,lack of power or environmental interference, ability to sustain sensor network functionality without interruption due to sensor node failure.
- Computational capabilities: Embedded processors in sensor nodes generally do not as powerful as they are in wired network.
- Quality of service (Qos): Quality of service required in terms of length of life time, data reliable, energy efficiency and location awareness collaborative processing data within certain period of time form the sensor.
- Communication range: The communication range is limited so actual transmission range is achieved from a given transmission signal strength that generally depend on various environmental factors.
- Random deployment: Random deployment means setting position of wireless sensor network randomly an independently in target area. Sensor nodes are randomly deployed and generally do not fit into any regular topology. Once deployed, they usually do not require architectures, internet of things, outsourcing, etc. That is the reason why cloud is mistaken for any human intervation. Hence, the setup and maintenance of the network should be entirely autonomous.
- Security: Security is the most important challenge in wireless sensor network.In network some confidential data are pass through different node,so that must be secure in network.

B. Different types of attacks in wireless sensor network:

There are various types of attacks in wireless sensor network. Which are categorized below:

List of Attacks	Description of Attacks
Black Hole Attack	The intruder node listens to the route requests and then replies to the intended node informing that it has the shortest path to the base station.
Hello Flood	In a WSNs intruder node send Hello packets just to announce themselves as neighbor to the sensor nodes.
Sybil Attack	Intruder node can behave to be more than one node at the same time using the identities of other nodes. Sybil attack nodes means kind of multiple fake identity.
Selective Forwarding	A intruder node during transmission through routing acts as a normal node,that simply by forwarding messages but selectively drops secure packets which are very hard to detect.

 Copyright 2016.All rights reserved.

False Identity Broadcast Flooding	Similar to simple broadcast flooding except the attacker deceives with wrong source ID.
False Identity Target Flooding	The intruder uses wrong source ID.
Misdirection Attack	Intruder node can misdirect the packet to different nodes instead of destination node.

Table: Threats And Attacks in Wireless Network [5]

C. Denial of Service Attack:
There are different types of Dos attacks in WSN, which can distrupt the whole network. The main goal of this attack is to overloading targeted network with traffic. Misdirection attack is one of the Dos attack which can decrease the performance of network and increase the end to end delay.

D. Misdirection Attack:
Misdirection attack is the most popular Denial of Service Attack. In this attack, instead of passing packet to the intended node intruder node redirect it to other direction.

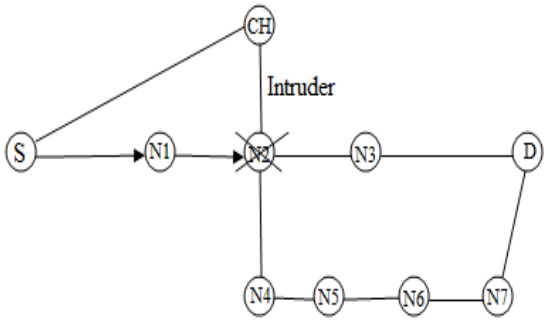


Fig: Intruder node misdirect the packet to other node
Types of Misdirection attack. It can be performed in two ways:[1]

- Packets orwarded to a node large away from the destination: This kind of misdirection attack is very dangerous because all packets are forwarded to a sensor node far away, preventing them to reach the destination so packets will not reach destination. Due to the attack the delay becomes infinite and decrease the throughput.
- Packets forwarded to a node close to actual destination: This kind of misdirection attack is less intense.Because in this, packet is sent to the destination node but via a long route. So network delay is increased and throughput is decrease.

E. Intrusion Detection System (IDS)
In wireless sensor network security is an important issue. So in order to opeate in secure way, it is necessary to detect intrusion before attacker can damage the network. Intrusion Detection system is required in Wsn because it can detect the intruder node from network and prevent other sensor nodes from the attacks.“Intrusion is an unauthorized (unwanted) activity in a network that is either achieved passively or actively.

II. LITERATURE SURVEY

A. “A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN”. [1].
In this paper a novel Cluster Based Intrusion Detection and Prevention Technique is used for Misdirection Attack. In this paper they selected a cluster head for particular cluster.Sensor nodes users the buffer for store the information.And regarding this information cluster head detect the intruder node.

B. “An algorithm to detect Malicious Nodes in Wireless Sensor Network using enhanced LEACH protocol” [2].In this paper LEACH approach is used.this protocol balance the energy consumption in sensor network.In the working principle of LEACH CH node is randomly selected. They can use the secret key for check the authentication.Sensor nodes compute MAC with this secret key over message and destination address and then send it to cluster head.CH has its own database key which are preshared with its nodes and base station. CH makes MAC address of received message using this secret key.If it is matched then send message to the node otherwise send back to the sensor node. And they use different types of technique for detection of intruder node.

C.“Preventing Denial service of attack in wireless sensor network ” [3].In this paper they present a method for detection and prevention of Dos attack. In detection method they are used special control nodes for monitoring the throughput of traffic in cluster. In this technique cluster head are selected using recursively LEACH clustering algorithm. If one node transmit packets more than threshold value then node consider it as a intruder node. When this malicious node is detected in network, All the packets which are sent by this sensor node are blocked and broadcast it as a intruder node in all the cluster.

D.“Intrusion Detection Based Security Solution for Cluster Based WSN” [4].In this paper they have illustrated MAC address, IP address, Port Number based intruder tracking system for cluster based wireless sensor networks. This proposed system is very energy-efficient for early detection and prevention of security threats and different attacks. Early detection and prevention of the intruder node by efficient security system can prevent many problems like slowing down of the network, sending of forged data, etc. By designing a security system in which the Base Station (BS) keeps track of the security of the Wireless network, high security can be ensured without any significant energy overheads on individual nodes and cluster heads.

E.“Detection and prevention of misdirection attack by third party monitoring in WSN ” [5].In this paper they have illustrated detection and prevention technique for misdirection attack.They are created CH-buffer database and receiver-buffer database for each source and destination transmission. They consist three module, which are Cluster head election, path identification, malicious node detection.Ch selection is done by energy model. Sensor Node

 Copyright 2016.All rights reserved.

which have highest energy is selected as a Cluster head. Path identification can be done using DSDV protocol. In implemented intruder detection source node maintains CH-buffer database and destination node maintains a received-buffer database. After transmission of packet, compare both database if both matches then transmission take place else intruder node is identified.

III. PROBLEM STATEMENT

Wireless sensor networks collect sensitive information from sensor nodes. Sometimes some confidential information is exchange between nodes. This information can be leaked or altered because many attacks are possible. Therefore, securing information is important in designing a sensor network. For example, one of the most challenging security threats is denial of service attack, whose goal is to disrupt the whole operation of sensor network. This can be done by different types of attacks, one of it is a misdirection attack, which is the most popular type of Dos attack. Misdirection attack can be perform in different ways. In misdirection attack intruder node misdirect packets away from the intended destination. Misdirection attack in wireless sensor network reduces the throughput of network along with the introduction of large end to end delay. So, there is some technique required for detection and prevention of intruder in wireless network to protect it from miss direction attack and also maintain network performance. To develop this technique we have to select cluster head for protecting cluster from misdirection attack.

IV. PROPOSED WORK

We can select the cluster head using energy efficient model.So highest energy level node is selected as a cluster head.Source node maintains buffer corresponding to each packet. This buffer contains entry of each sent packet with time stamp value corresponding to each packet sequence number. Source node also shares this buffer to the cluster head. Cluster head compares all sequence numbers of packets stored in its buffer to the sequence numbers of packets stored in buffer of all intermediate nodes with stamp value. If packet mismatch or empty entry is found in the buffer at a particular node, then the previous node will be omitted. The detection process again starts right from the beginning. It again searches for another optimum route for the secure communication. Thus any misdirection attack is easily detected and prevented with the proposed technique.

A. Cluster Head Selection Method

During the selection of cluster head
First Compute energy level of each node in the network
if
Sensor nodes energy level >= average energy level,
then Sensor node suitable for cluster head selection process
If
Sensor node with highest energy level work as a CH
Else
Not eligible for cluster head selection process.

B. Explanation of algorithm

- Select cluster head based on energy parameters.If node has highest energy in the network then select as a cluster head else not eligible for cluster head selection process.
- After that highest energy level node is selected as cluster head and broadcast it to whole network.
- Cluster head containing all the details regarding send & receive packets of all nodes in another matrix.
- Packets are passed from one node, source node to next node till destination node is reached.
- After the packet is send from source node to next node,source node will send acknowledgment to cluster head and when the packet isreceived by receiver it will send acknowledgment to cluster head.
- When the acknowledgment is received from receiver node cluster head set the flag value 1.Means the packet is successfully deliver to next node.
- Cluster head continuously check the matrix details.If sender node send the acknowledgment and receiver node not sending acknowledgment within some period it will wait for some time because of network traffic.
- After that time if acknowledgment is not received it declare that node as a intruder node.
- Cluster head broadcast the message to whole network & changed the route of packet transmission and continuous detection process.

C. Flow chart of the proposed algorithm

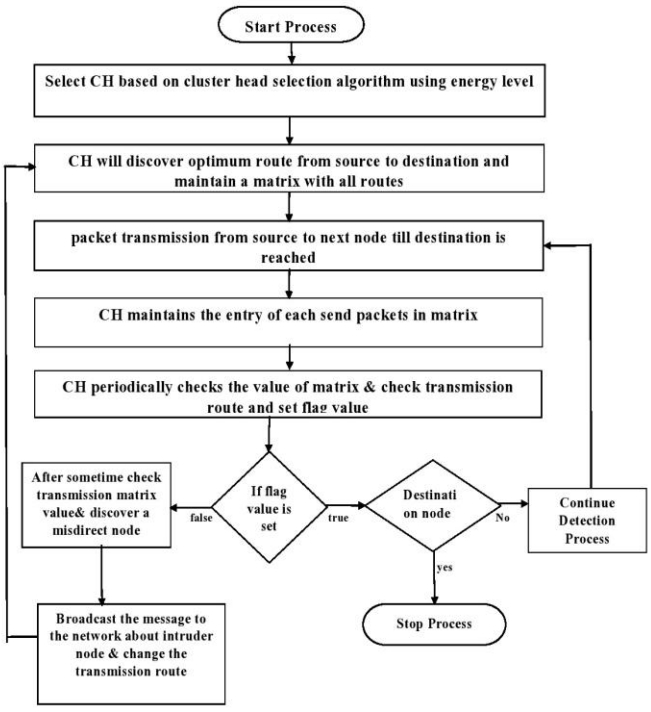


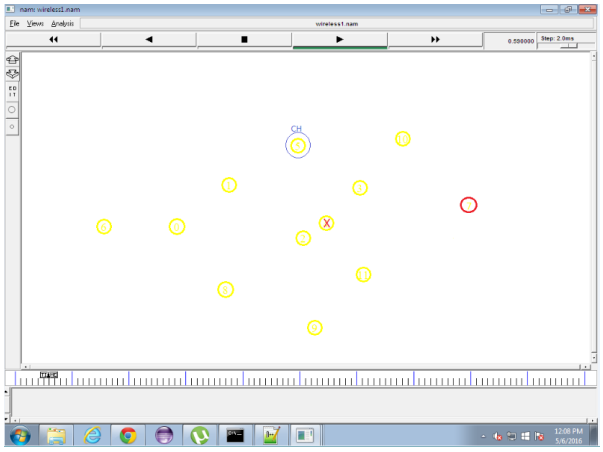
Fig: Proposed Algorithm Flow Chart

 Copyright 2016.All rights reserved.

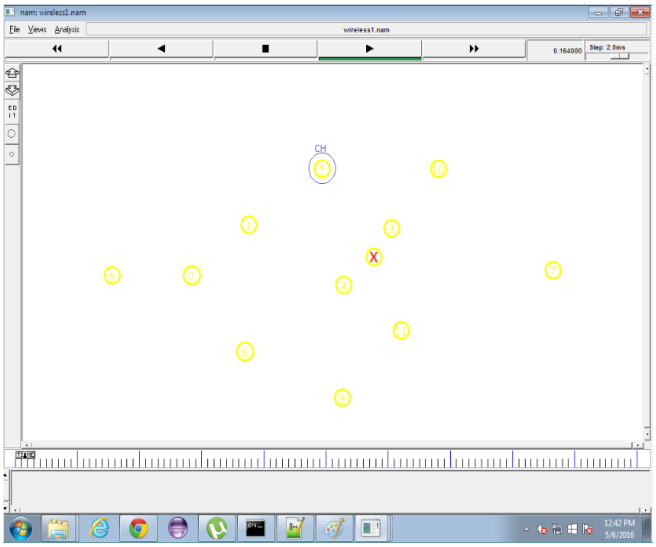
V. SIMULATION SCENARIO OF MISDIRECTION ATTACK

A. Implementation Scenario

In following screen-shot, cluster head is selected from the network and make a channel between nodes. Nodes can send and receive the packets in network. In between intruder node found at node 4, which not pass the packet to destination node but misdirect it.



After Intruder node is identified, discard this node from the network.



B. Common Parameters

Transmission range	250
Inference Range	550
bandwidth	11mb
freq	2.472e9
agent	tcp
routing protocol	dsdv
max packet in queue	50
channel	wireless protocol
simulation	20 nodes

C. Results

In simulation we have taken following statistics of the network: End to end delay (msec), Throughput (bps).In table we can make display the result of normal flow, misdirection flow and proposed algorithm flow.

	Normal Flow	Under Misdirection Attack	Under Proposed Method
End-To-End Delay (msec)	13.65	14.82	13.7832
Throughput (Bps	10868.94	12664.953	12205.12

Table: End to end delay & Throughput

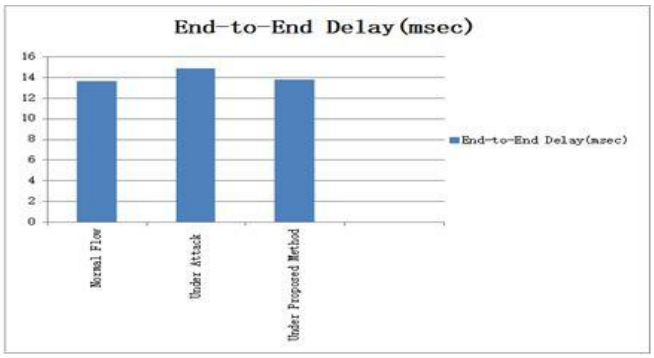


Figure Result of :End-to-end delay

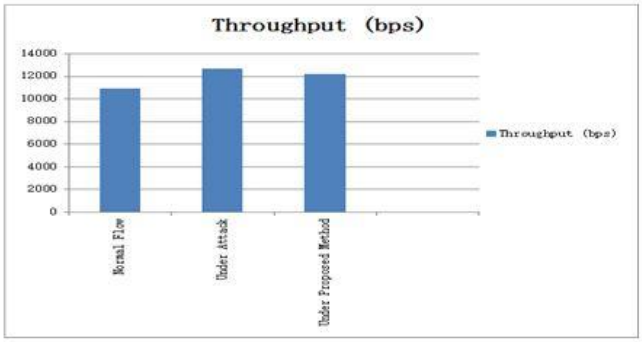


Figure: Result of Throughput

In 1st figure shows end to end delay with normal flow,under attack and under proposed algorithm.In 2nd figure shows throughput with normal flow,under attack and under proposed algorithm.

VI. CONCLUSION

In wireless sensor network misdirect attack can damage whole network performance and end to end delay. In proposed technique detection and prevention of misdirection attack is efficiently worked. In proposed method we can detect the intruder node by help of cluster head, and create a secured network with minimizing end to end delay and increased network performance. The basic purpose of this proposed scheme is to secure the cluster head from intruder with suitable performance of network parameters during node density variation and preventing the network from misdirection attack.

 Copyright 2016.All rights reserved.

REFERENCES

[1] A Cluster Based Intrusion Detection and Prevention Technique for Misdirection Attack inside WSN, Communications and Signal Processing (ICCSP), 2013(IEEE)
[2] An algorithm to detect Malicious Nodes in Wireless Sensor Network using enhanced LEACH protocol, Computer Engineering and Applications (ICACEA), 2015(IEEE)
[3] Preventing Denial service of attack in wireless sensor network,Communications(ICC),2015(IEEE)
[4] Intrusion Detection Based Security Solution for Cluster Based WSN, International Journal of Advanced Research in Computer Engineering & Technology Volume 1, Issue 4, June 2012
[5] Detection and prevention of misdirection attack by third party monitoring in WSN, R Sowmya1, Mrs. Shoba. M2, Volume: 1 Special Issue: 2(IJRISE)
[6] Wireless sensor networks misdirection attacker challenges and solutions, Information and Automation, 2008. ICIA 2008.(IEEE)
[7] Misdirection attack in WSN: Topological analysis and an algorithm for delay and throughput prediction, Intelligent Systems and Control (ISCO), 2013(IEEE)
[8] RMCHS: Ridge method based cluster head selection for energy efficient clustering hierarchy protocol in WSN, Smart Technologies and Management for Computing, Communication, Controls, Energy and Materials (ICSTM), 2015 (IEEE)
[9] Trust based cluster head selection algorithm for wireless sensor network, Current Trends in Engineering and Technology (ICCTET), 2014
[10] Detecting DoS attacks in WSN based on clustering technique, Wireless Communications and Networking Conference (WCNC), 2013 (IEEE)
[11] Misdirection Attack in WSN Due to Selfish Nodes; Detection and Suppression using Longer Path Protocol,, Volume 4, Issue 7, July 2014(IJARCSSE)
[12] Cluster Head Selection Based On Genetic Algorithm Using AHYMN Approaches in WSN, Volume 3, Special Issue 3, March 2014
[13] Energy efficient and node selection technique for Wireless Body Sensor Network, Communications and Signal Processing (ICCSP), 2015
[14] An Efficient Cluster Head Selection Algorithm for Wireless Sensor Networks –Edrleach, IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 2, Issue 2 (July-Aug. 2012), PP 39-44
[15] Malicious Node Detection Using Confidence Level Evaluation in a Grid-Based Wireless Sensor Network, Received December 19, 2012; revised January 21, 2013; accepted January 28, 2013
[16] Dynamic selection of cluster head in cluster of cluster heads within the cluster in Heterogeneous Wireless Sensor Network, Advanced Communication Control and Computing Technologies (ICACCCT), 2014
[17] J. Kong, Z. Ji, W. Wang, M. Gerla, R. Bagrodia and B. Bhargava,"Low-cost Attacks Against Packet Delivery, Localization and Time Synchronization Services in Underwater Sensor Networks" in 4th ACM Workshop on Wireless Security, 2005, pp. 87-96.
[18] Challenges of Next-Generation Wireless Sensor Networks and its impact on Society, JOURNAL OF TELECOMMUNICATIONS, VOLUME 1, ISSUE 1, FEB 2010
[19] Wireless Sensor Networks: Challenges and Opportunities, Neiyer Correal and Neal Patwari Florida Communications Research Labs,Motorola Labs,8000 West Sunrise Blvd, Rm 2141 Plantation, FL 33322[N.Correal, N.Patwari]@Motorola.com
[20] Monitoring mechanisms for wireless sensor networks: challenges and solutions, Ibrahiem M. M. El Emary & S.Ramakrishnan. Wireless Sensor Networks: Theory and Application, Array, pp.1-30, 2013, 9781466518100
[21] Efficient Clustering for Improving Network Performance in Wireless Sensor Networks, The Hebrew University of Jerusalem, Israel{anker, daniel51, dolev, hodb}@cs.huji.ac.il 2 Marvell Semiconductor, CA, USAtala@marvell.com

 Copyright 2016.All rights reserved.