Intrusion Detection System For Mitigating Sinkhole Attack on Leach Protocol In Wireless Sensor Network

Sudarshan Suryawanshi[1], Amutha Jeyakumar[2]
VJTI, Mumbai

Abstract- *In wireless sensor network (WSN), the sensors are deployed and placed uniformly to transmit the sensed data to a destination periodically. Major threat of the WSN is sinkhole attack and it is still challenging issue on the sensor network, where the malicious node attracts the packets from the other normal sensor nodes and drops the packets. In this paper a new Intrusion Detection System (IDS) mechanism to detect the intruder in the network is discussed, which uses Low Energy Adaptive Clustering Hierarchy (LEACH) protocol for its routing operation. In this new detection method, a Watchdog Timer is active in each Sensor. If sensor is not forwarding packets to destination, then watchdog timer expires. If watchdog timer expires greater than the threshold, then it is a malicious node. After detection, an alert message is sent to all sensors and malicious node blacklisted from network permanently. For the Simulation of this method TETCOS NETSIM Simulation Software is used. Simulation results is proven to be efficient compared with existing work in terms of fast detection and mitigation.*

Keywords: *WSN, IDS, Sinkhole attack, LEACH, Cluster Head (CH).*

I. INTRODUCTION:

Wireless sensor network (WSN) a group of spatially distributed and dedicated sensors for monitoring and recording the physical conditions of the environment and organizing the collected data at a central location. WSNs measure environmental conditions like temperature, sound, pollution levels, humidity, wind, etc. Wireless sensor devices are used in a broad range of applications such as defence, farming, medicine, and industries. WSNs deploy an array of micro sensors that senses the activities of a physical phenomenon and sends the information to the base station (BS). It faces a lot of security issues that arise due to their low Operating energy and minimal computational capabilities. There are so many attacks in different layer of wireless sensor network. One of those is a Sinkhole Attack which takes place in Network Layer. Sinkhole attack is active attack resulting in a successful intrusion and high data loss rate of the real time data.

Intrusion Detection System (IDS) is a high level security mechanism. Encryption methodologies and authentication system prove to be inefficient in the case of insider attacks. The main objective of this paper is to detect and mitigate the sinkhole attack in a WSN.

II. SINKHOLE ATTACK IN WSN:

Sinkhole attack is an insider attack where malicious node attracts all the traffic by advertising wrong information regarding maximum energy.

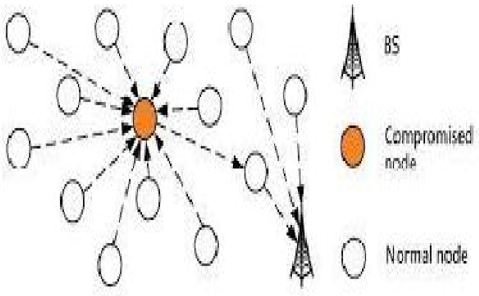


Fig.1: Sinkhole Attack.

Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As shown in fig.1 compromised node attracts all the traffic from its neighbor's by telling its neighbor that it has shortest route to reach to the base station.

III. MOTIVATION:

Network layer is very important layer in wireless communication. Attack on network layer can damage whole network which is very serious issue. The purpose of this attack is to create a serious threat to the network. Sinkhole attack is more vulnerable than the other attacks. Sinkhole attack may introduce new attacks like selective forwarding attack and Wormhole attack. Therefore, detection and mitigation of sinkhole attack is very important.

IV. LITERATURE REVIEW:

Security domain and intrusion detection system are considered as an active research area in WSNs. Based on data consistency and network traffic analysing, the authors in [4], proposed an IDS for detecting a sinkhole attack. Rasheed and Mahapatra [5] proposed a multi-tier framework using a pre distribution pair wise key scheme. This framework uses any a pre-distribution pair wise key scheme and needs two separate key pools, one for the mobile sink, and the other for pair wise key establishment between the sensors Eschenauer and Gilgor [6] proposed a robust probabilistic key pre-distribution scheme. In this scheme each sensor node chooses randomly a set of keys from a key pool before deployment in this scheme each sensor node chooses randomly a set of keys from a key pool before deployment. This idea is further extended in [7] and [8] using two key pre-distribution schemes. Using polynomial pool-based key pre-distribution protocol [10], Liu and Ning [9] designed another enhanced framework for pair wise key establishment.

V. NEW METHOD OF INTRUSION DETECTION SYSTEM:

In WSN sensors are placed uniformly in the network and transmit the sensed data to the destination. LEACH protocol is used for routing data packets as it is a very energy efficient protocol.

To mitigate sinkhole attack proposed method proves very efficient in terms of energy consumption, throughput and efficiency. In this method a Watchdog timer automatically gets activated whenever a packet sent. If that packet does not reach to destination in specified time, the acknowledgement won’t receive before timer expires. If the timer expires up to a threshold no of times for packet transmitted to a particular node that means this node is a malicious node. This is how malicious node detected. An alert message is sent to all the sensor nodes in that cluster. All sensors stop sending data to that node and blacklist that node permanently from further cluster Head election process. It saves data loss. The Timer based simulation has been done in TETCOS NETSIM Simulator.

VI. Flow Chart:

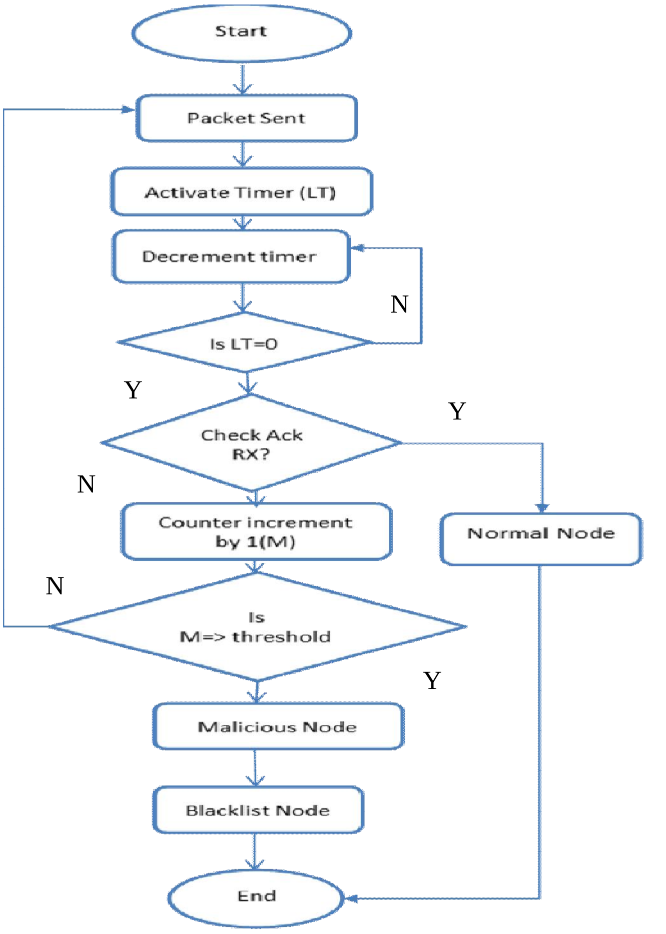


Fig.2: Flow of new method.

Fig.2 Shows flow chart for the Intrusion detection using watchdog timer by a particular node. Watchdog Timer with lifetime (LT) will be active whenever packet starts routing. Node checks acknowledgement received within the set time in the timer. If packet receives acknowledgement, then it is normal node. Sensor allows transmitting some packets (M), even if the acknowledgement not received. A counter count no of non-Acknowledged packets. If count is greater than M, then that node is declared as malicious node. After detection of malicious node an alert message is sent in the network and all sensors blacklist that malicious node from the network permanently. The simulation results are proven to be efficient compared with the existing work in terms of fast detection and mitigation.

VII. SIMULATION:

A scenario is created in NetSim having 64 sensors. Each sensor is connected to sink node through an Ad hoc link. In this network Node 11 is defined as malicious node. So that it attracts all the packets initially but after detection node 11 blacklisted from network.

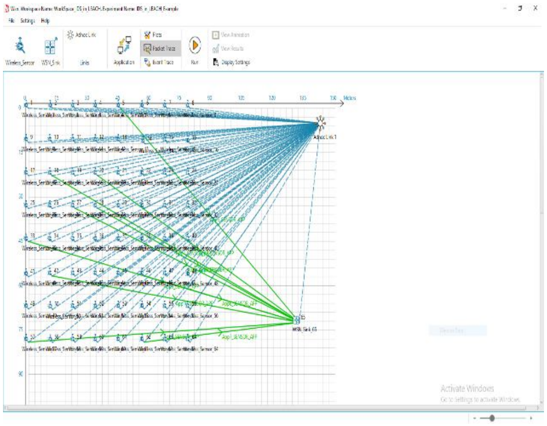
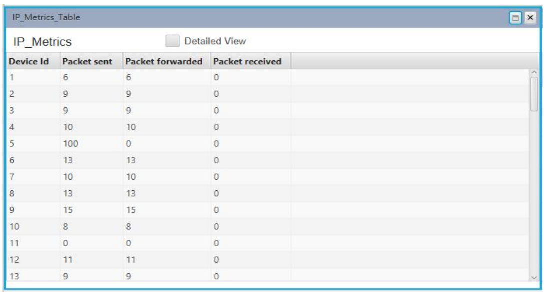


Fig.3: Network scenario.

After simulating this network for 100 sec following results are obtained:

VIII. RESULTS:



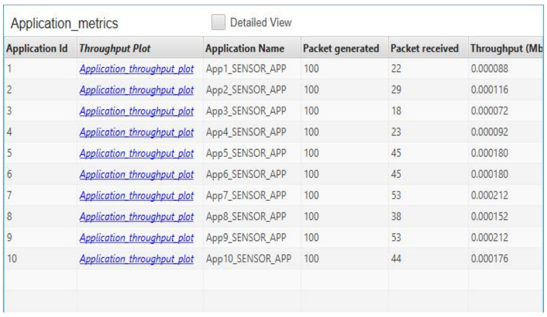
IP_Metrics_Table

IP_Metrics ☐ Detailed View

Device Id	Packet sent	Packet forwarded	Packet received
1	6	6	0
2	9	9	0
3	9	9	0
4	10	10	0
5	100	0	0
6	13	13	0
7	10	10	0
8	13	13	0
9	15	15	0
10	8	8	0
11	0	0	0
12	11	11	0
13	9	9	0

Fig.4: IP metrics table.

As observed in IP metrics table node 11 does not forward any packet because it is a malicious node.



Application_metrics ☐ Detailed View

Application Id	*Throughput Plot*	Application Name	Packet generated	Packet received	Throughput (Mb
1	*Application_throughput_plot*	App1_SENSOR_APP	100	22	0.000088
2	*Application_throughput_plot*	App2_SENSOR_APP	100	29	0.000116
3	*Application_throughput_plot*	App3_SENSOR_APP	100	18	0.000072
4	*Application_throughput_plot*	App4_SENSOR_APP	100	23	0.000092
5	*Application_throughput_plot*	App5_SENSOR_APP	100	45	0.000180
6	*Application_throughput_plot*	App6_SENSOR_APP	100	45	0.000180
7	*Application_throughput_plot*	App7_SENSOR_APP	100	53	0.000212
8	*Application_throughput_plot*	App8_SENSOR_APP	100	38	0.000152
9	*Application_throughput_plot*	App9_SENSOR_APP	100	53	0.000212
10	*Application_throughput_plot*	App10_SENSOR_APP	100	44	0.000176

Fig.5: Throughput Metrics

By observing throughput metrics table (fig.5) it is clearly seen that Application throughput for Application id 1,2,3,4 is less as compared to other application id. Because application id 1, 2, 3, and 4 are the applications from the malicious node cluster that's why they have low throughput. As malicious node detects throughput increase.

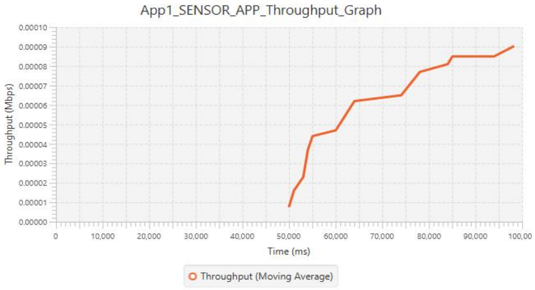


Fig.6: Throughput of malicious cluster node application

Fig.6 shows the throughput of malicious cluster node. Throughput is zero up to 46 secs because Throughput increases gradually after attack detection.

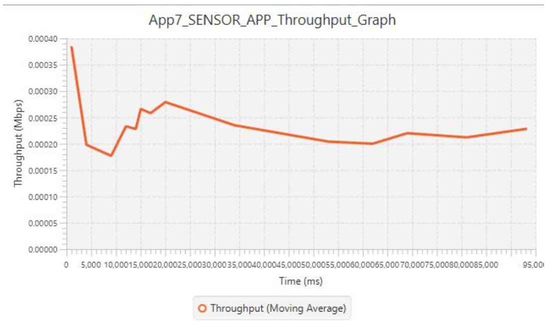
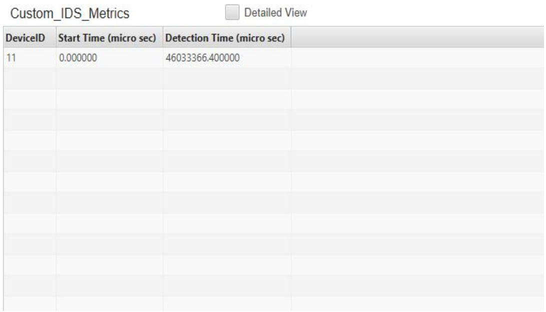


Fig.7: Throughput of normal cluster node application.

In Fig.7 shows the throughput of normal cluster node as it doesn't have any malicious node.



Custom_IDS_Metrics ☐ Detailed View

DeviceID	Start Time (micro sec)	Detection Time (micro sec)
11	0.000000	46033366.400000

Fig.8: Custom Metrics table.

In Fig.8 custom metrics table Detection time is the sinkhole attack detection time. Sinkhole attack is detected and mitigate in just 46 sec.

IX. CONCLUSION:

WSNs are easily prone to security breach like sink hole attack. A new Method of intrusion detection system mechanism has been simulated and tested on LEACH protocol. In this method Detection and mitigation of sinkhole attack is done successfully. After detection Node alerts all other sensor nodes to reduce the data loss rate and fast detection and mitigation. The TETCOS NETSIM software is used for simulation and analysis.

REFERENCES

[1] S. Athmani, D. E. Boubiche, and A. Bilami, "Hierarchical energy efficient intrusion detection system for black hole attacks in WSNs," in Proceedings of the World Conference on Computer and Information Technology, pp. 1–5, June 2013.

[2] I. Krontiris, T. Dimitriou, T. Giannetsos, and M. Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor network," in Proceedings of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (Algo Sensors'07), vol. 4837, pp. 150–161, Wrocław, Poland, 2007.

[3] Ranjeeth Kumar Sundararajan and Umamakeswari Arumugam Research Article "Intrusion Detection Algorithm for Mitigating Sinkhole Attack on LEACH Protocol in Wireless Sensor Networks" Journal of Sensors Volume 2015, Article ID 203814.

[4] S. H. Lee, S. Lee, H. Song, and H. S. Lee, "Wireless sensor network design for tactical military applications: Remote large-scale Environments," In Proceedings of IEEE Military Communications Conference, MILCOM'09, pp. 1-7, Oct 2009.

[5] E. C.H. Ngai, J. Liu, M.R. Lyu, "An efficient intruder detection algorithm against sinkhole attacks in wireless sensor Networks," Computer Communications 30 (2007) 2353–2364.

[6] A. Rasheed and R.N. Mahapatra, "The Three-Tier Security Scheme in Wireless Sensor Networks with Mobile Sinks," IEEE Transactions On Parallel and Distributed Systems, Vol. 23, No. 5, May 2012.

[7] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," Proc. of the ACM Conference Computer Communication Security (CCS'02), pp. 41-47, 2002.

[8] H. Chan, A. Perrig, and D. Song, C. S. Raghavendra, K. M. Sivalingam, T. Znati, Norwell, MA: Kluwer "Key distribution techniques for sensor networks," Wireless Sensor Networks Academic, pp. 277-303, 2004.

[9] H. Chan, A. Perrig, and D. Song, "Random key pre-distribution schemes for sensor networks," Proc. of the 2003 IEEE Symposium on Security and Privacy, pp. 197-213, 2003.

[10] D. Liu, P. Ning, and R. Li, "Establishing pair wise keys in distributed sensor networks," The 10th ACM Conference on Computers and communication security (CCS 03). pp. 52-61, Oct 2003.