IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-4, Issue-7 E-ISSN: 2347-2693

Result Based approach on Intrusion Detection System against Sinkhole Attack in Wireless Sensor Networks

Rohit Aggarwal [1*], Er. Khushboo Bansal [2]

[1]M.Tech Student, CSE Department, Desh Bhagat University, Punjab, India
[2]Assistant Professor of CSE Department, Desh Bhagat University, Punjab, India

Available online at: www.ijcseonline.org

Received:18/Jun/2016 Revised:26/Jun/2016 Accepted:16/Jul/2016 Published:31/Jul/2016

***Abstract*:** The main problem in the proposed work was the sinkhole attack which was detected and removed by implementing appropriate protocol such as AODV i.e. ad hoc on-demand distance vector (AODV) routing. In this paper, eliminate the sinkhole attack from network by using a novel algorithm for sinkhole detection. The algorithm first finds a list of suspected nodes through checking data consistency and then effectively identifies the intruder in the list through analyzing the network flow information. The algorithm is also robust to deal with multiple malicious nodes that cooperatively hide the real intruder.

Keywords: Wireless Sensor Networks, Routing Algorithm, Malicious Detection Approach

1. INTRODUCTION

A wireless sensor network is a group of specialized transducers with a communications infra-structure for monitoring and recording conditions at diverse locations. Commonly monitored parameters are tempe-rature, humidity, pressure, wind direction and speed, illumination intensity, vibration intensity, sound intensity, power-line voltage, chemical concentrations, pollutant levels and vital body functions.

Wireless Sensor Networks (WSNs1) are applied to various fields of science and technology. To gather information regarding human activities and behaviour such as health care, military surveillance and reconnaissance, highway traffic to monitor physical and environmental phenomena such as ocean, wildlife, earthquake, pollution, wild fire, water quality to monitor industrial sites such as building safety, manufacturing machinery performance.

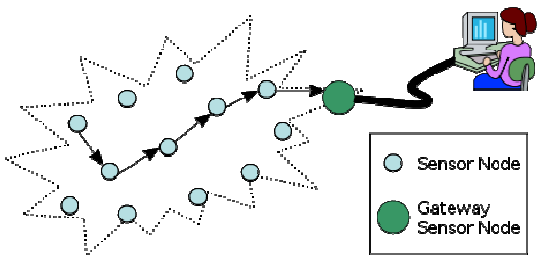

Figure 1: Wireless Sensor Networks

1.2 Parts of WSN

1.2.1 Sensor Node: This is a core component of Wireless Sensor network. This node plays a multiple roles in WSN such as simple sensing, data storage, routing and data processing.
1.2.2 Clusters: Clusters are the organizational unit for WSNs. The dense nature of these networks requires the need for them to be broken down into clusters to simplify tasks such a communication.
1.2.3 Cluster heads: Cluster heads are the managing the cluster head. They often are needed to managing task in the cluster. These tasks include but are not limited to data-aggregation and organizing the communication schedule of a cluster.
1.2.4 Base Station: The base station is at the upper level of the hierarchical WSN. It provides the communication link between the sensor network and the end-user.
1.2.5 End User: The data in a sensor network can be used for a wide-range of applications. Therefore, a particular application may make use of the network data over the internet using a PDA or even a desktop computer.

2. SINKHOLE ATTACK

In a sinkhole attack the adversary's aim is to lure nearly all the traffic from a particular area through a compromised node, creating a metaphorical sinkhole with the adversary at the centre. Sinkhole attacks typically work by making a compromised node look especially attractive to surrounding nodes with respect to the routing algorithm.

© 2016, IJCSE All Rights Reserved

Sinkhole attacks are difficult to counter because routing information supplied by a node is difficult to verify. As an example a laptop-class adversary has a strong power radio transmitter that allows it to provide a high-quality route by transmitting with enough power to reach a wide area of the network.

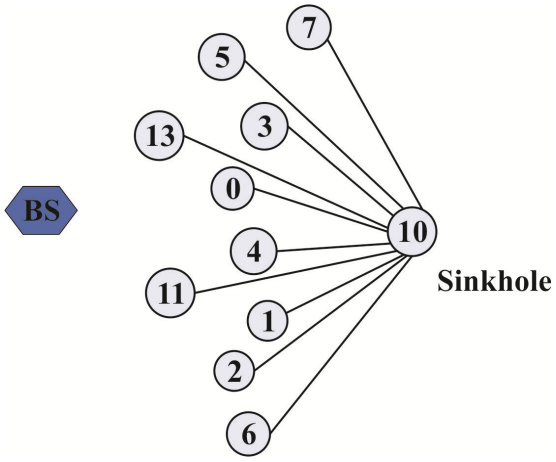

Figure 2: Demonstration of a sinkhole attack

As shown in Figure 2, a compromised node attracts all the traffic from its neighbours by telling its neighbour that it has shortest route to reach to the base station. This route is artificial high quality route.

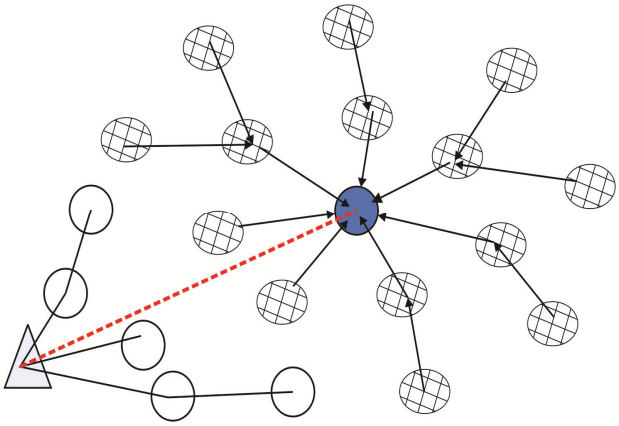

Figure 3: Sinkhole using an artificial high quality route

As shown in Figure 3, a sinkhole can also be performed using a wormhole [27], which creates a metaphorical sinkhole with the intruder being the centre; the intruder then relays the messages received in one part of the network toward the sink using a tunnel.

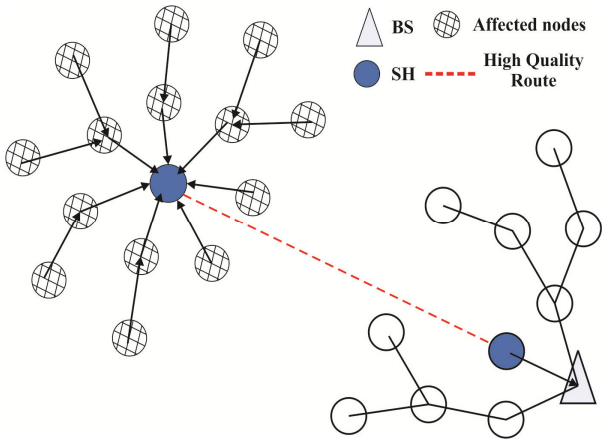

Figure 4: Sinkhole using a wormhole

3. METHODOLOGY

Different intrusion detecting mechanisms in WSN have been introduced and studied by the researchers in order to detect various attacks. The proposed methodology follows AODV based detection approach.

There are two phases in the research work. In the first phase, wireless sensor network is simulated using NS2 and sinkhole attacks are injected. In the second phase, detection approaches are applied to the wireless sensor network.

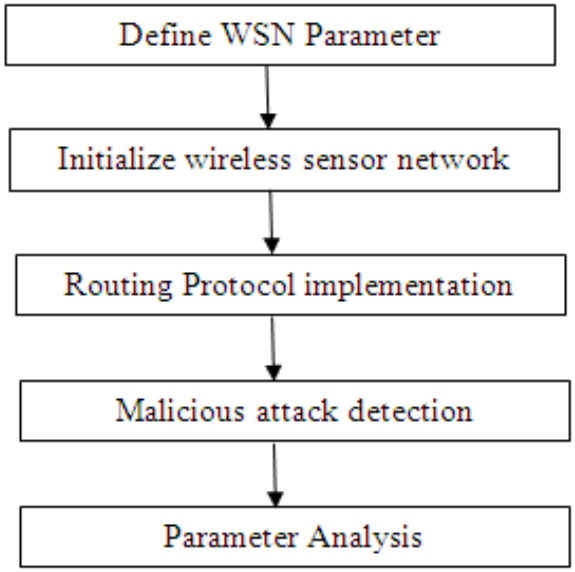

Figure 5: Flow of Work

4. RESULTS AND DISCUSSION

In the purposed work WSN has been initialized for sensing information from environment. The sensor nodes have been

© 2016, IJCSE All Rights Reserved

deployed in the environment for capturing information. These nodes capture information from particular environment and transmit this information to base station. Various parameters have been used in WSN for sensing information. These nodes consume energy while sensing, receiving and transmitting information.

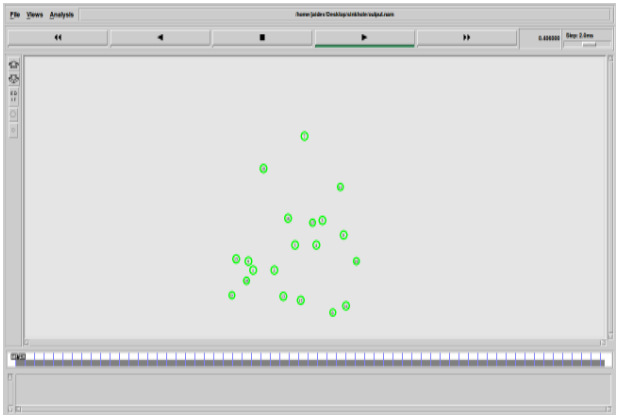

Figure 6: Initialization of Nodes

Figure 6 represents initialization of wireless sensor network for sensing information from environment. In this figure nodes have been initialized by defining various parameters about nodes location, nodes size and energy model. In WSN nodes sense information from a particular environment and transmit information to base station for decision making process.

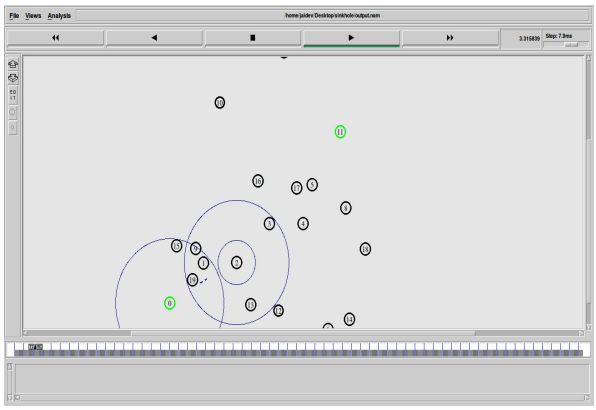

Figure 7: Routing between nodes

Figure 7 represent the Routing occurred between the nodes. Each & Every node communicates with one-another. One node sends the message to other nodes & that receiver node respond to the sender node according to that message.

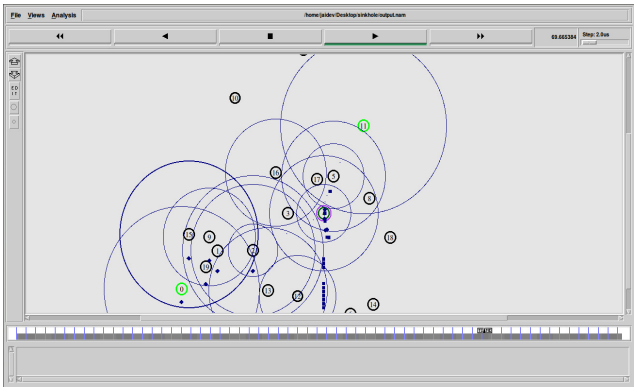

Figure 8: Attack occurred in the Network

Figure 8 represent the Sinkhole attack occurred in the network. Sink hole attack is performed on sink node attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data doesn't receive at base station that loss the information of the network.

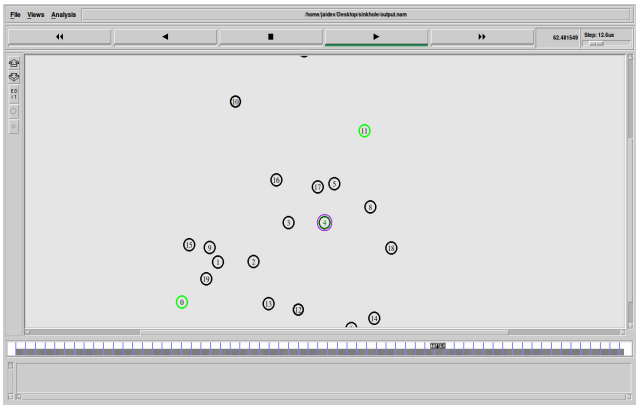

Figure 9: Detection of Sinkhole Attack

In wireless sensor network the packet are transmitted based on routing metric that used by different routing protocols. The compromised node used its routing metric that used by routing protocol to lie to his neighbours in order to launch sinkhole attack. Then all the data from his neighbours to base station will pass through compromised node. In this actual data doesn't receive at base station that loss the information of the network. Here, the sinkhole attack detection scheme has to be implement that detect attacking node and provide reliable information.

Comparison between Previous result and proposed results

Table 1 is based on the comparison of previous result and proposed results. After comparing various parameter, current result are noted as more accurate and reliable.

© 2016, IJCSE All Rights Reserved

Table 1: Comparison Table

Sr. No	Parameters	Proposed value	Previous value
1	PDR	80%	60%
2	Packet Throughput	50%	35%
3	Packet Delay	40%	60%
4	Packet Loss	50%	70%

- PDR (Packet Delivery Ratio) is defined as the number of packet deliver with respect to time.
- Packet Throughput is defined as the number of packet delivered successfully over the network
- Packet Delay is defined as the Delay between packets during transmission.
- Packet Loss is defines as the number of packets which fails for delivery over the network.

Figure 10 represents the comparing graph. Graph compares proposed result with previous result and show current results are more accurate form previous result. Graph is based on various parameters like Packet Delivery Ratio (PDR), Packet Throughput, Packet Delay and Packet Loss.

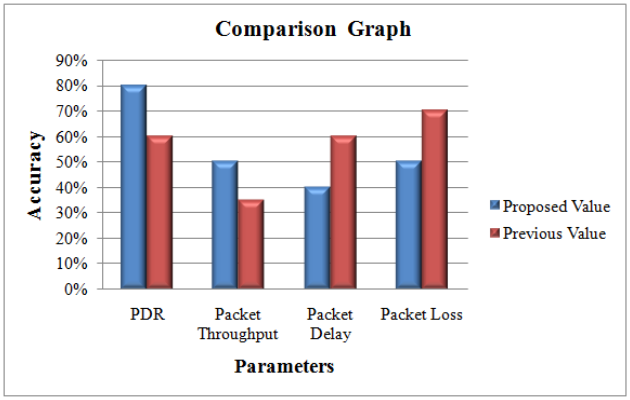

Figure 10: Comparison Graph

CONCLUSION

Wireless sensor network is a branch of networking that deals with sensing of information from deployed area. Sensor nodes collect the information by sensing the information and transmit using sink nodes. Sink nodes collects the information from sensor nodes and transmit this information to base station. In the transmission of data from source to destination various routing and off-demand routing are here in methodology. Various malicious nodes have been introduced to perform various types of attacks on the network to degrade or collect same information. The new attack that has been used for acquiring information by performing sinkhole attack. Sink hole attack is performed on sink node attacking node replaces the actual sink node by advertising its availability and resumes all the data from the sensor node. Actual data doesn't receive at base station that loss the information of the network. We eliminate the sinkhole attack from network by using various sinkhole detection algorithms. At last we got various types of parameters & On the basis of these parameters we conclude that our system gives us better results.

REFRENCES

[1] S. Ahmad Salehi, M. A. Razzaque, Parisa Naraei, Ali Farrokhtala, "Detection of Sinkhole Attack in Wireless Sensor Networks", *IEEE International Conference on Space Science and Communication*, 2013, pp. 361 – 365.

[2] A. Vijayalakshmi, T. Shrimathy, T. G. Palanivelu, "Mobile Agent Middleware Security for Wireless Sensor Networks", *IEEE International Conference on Communication and Signal Processing*, 2014, pp. 1669 - 1673.

[3] Vandana B. Salve, Leena Ragha, Nilesh Marathe, "AODV Based Secure Routing Algorithm against Sinkhole Attack in Wirelesses Sensor Networks", *IEEE International Conference on Electrical, Computer and Communication Technologies*, 2015, pp. 1 – 7.

[4] Mohamed Guerroumi, Abdelouahid Derhab, Kashif Saleem, "Intrusion detection system against SinkHole attack in wireless sensor networks with mobile sink", *IEEE International Conference on Information Technology*, 2015, pp. 307- 313.

[5] D. Sheela, C. Naveen Kumar, G. Mahadevan, "A non cryptographic method of sink hole attack detection in wireless sensor networks", *IEEE International Conference on Information Technology*, 2011, pp. 527 – 532.

[6] Mohamed Guerroumi, Abdelouahid Derhab, Kashif Saleem, "Intrusion Detection System against Sink Hole Attack in Wireless Sensor Networks with Mobile Sink", *IEEE International Conference on Information Technology - New Generations*, 2015, pp. 307 – 313.

[7] Krishan Kant Varshney, P. Samundiswary, "Performance analysis of malicious nodes in IEEE 802.15.4 based wireless sensor network", *IEEE International Conference on Information Communication and Embedded Systems*, 2014, pp. 1–5.

[8] Ritwik Banerjee, Chandan Kr. Bhattacharyya, "Energy efficient routing and bypassing energy-hole through mobile sink in WSN", *IEEE Conf. on Computer Communication and Informatics (ICCCI)*, 2014, pp. 1 – 6.

[9] Babar Nazir, Halabi Hasbullah, "Mobile Sink based Routing Protocol (MSRP) for Prolonging Network Lifetime in Clustered Wireless Sensor Network", *IEEE Conf. on Computer Applications and Industrial Electronics (ICCAIE)*, 2010, pp. 624 – 629.

[10] Pushpendu Kar, Sudip Misra, "Reliable and Efficient Data Acquisition in Wireless Sensor Networks in the Presence of Tran faulty Nodes", *IEEE Conf. on IEEE Transactions on Network and Service Management*, 2016, pp. 99 – 112.

© 2016, IJCSE All Rights Reserved

[11] Siba Mitra, Ajanta De Sarkar, "Energy aware fault tolerant framework in Wireless Sensor Network", *IEEE Conf. on Applications and Innovations in Mobile Computing (AIMoC)*, 2014, pp. 139 – 145.

[12] Priyanka Deshpande, Mangala S. Madankar, "Techniques improving throughput of wireless sensor network: A survey", *IEEE Conf. on Circuit, Power and Computing Technologies (ICCPCT)*, 2015, pp. 1 – 5.

[13] Imran Makhdoom, Mehreen Afzal, Imran Rashid, "A novel code attestation scheme against Sybil Attack in Wireless Sensor Networks", *IEEE Conf. on Software Engineering Conference (NSEC)*, 2014, pp. 1 – 6.

[14] J. Krithiga, R. C. Porselvi, "Efficient Code Guard mechanism against pollution attacks in interflow Network coding", *IEEE Conf. on Communications and Signal Processing (ICCSP)*, 2014, pp. 1384 – 1388.

[15] R. Geetha, S. Raj Anand, E. Kannan, "Fuzzy logic based compromised node detection and revocation in clustered wireless sensor networks", *IEEE Conf. on Information Communication and Embedded Systems (ICICES)*, 2014, pp - 1 – 6.

[16] Yong-Sik Choi, Young-Jun Jeon, Sang-Hyun Park, "A study on sensor nodes attestation protocol in a Wireless Sensor Network", *The 12th IEEE International Conf. on Advanced Communication Technology (ICACT)*, 2010, pp. 574 - 579.

[17] Yuling Lei, Yan Zhang, Yanjuan Zhao, "The Research of Coverage Problems in Wireless Sensor Network", *IEEE Conf. on Wireless Networks and Information Systems*, 2009, pp. 31 – 34. DOI: 10.1109/WNIS.2009.38

[18] Ruchi Mittal, M. P. S Bhatia, "Wireless sensor networks for monitoring the environmental activities", IEEE Conf on Computational Intelligence and Computing Research (ICCIC), 2010, pp. 1 – 5.

[19] Nikhil Marriwala, Priyanka Rathee, "An approach to increase the wireless sensor network lifetime", *IEEE Conf. on Information and Communication Technologies (WICT)*, 2012, pp. 495 – 499.

[20] Guanglai Chen, Shoujun Wang, Lifei Li, "Notice of Retraction the design of wireless wave height sensor network node based on Zigbee technology", *IEEE Conf. on Electric Information and Control Engineering (ICEICE)*, 2011, pp. 3683 – 3686. DOI: 10.1109/ICEICE.2011.5777656

[21] NS-2, The ns Manual (formally known as NS Documentation) available at following link: http: //www. isi.edu/nsnam/ ns/do

[22] Gisung Kim, Younggoo Han, Sehun Kim, "A cooperativesinkhole detection method for mobile ad hoc networks*", International Journal of Electronics and Communication 64* (2010) 390–397

[23] J.M.L.P. Caldeira, J.J.P.C. Rodrigues, P. Lorenz, L. Shu, "Intramobility handover enhancement in healthcare wireless sensor networks", *14th International Conference one-Health Networking, Applications and Services (Healthcom)*, 2012, pp. 261 – 266.

[24] Charanpreet Kaur and Amit Chhabra, "An Energy Efficient Multihop Routing Protocol for Wireless Sensor Networks", *International Journal of Computer Sciences and Engineering*, Volume-03, Issue-07, pp. 86 - 91, Jul - 2015.

[25] R. Silva, J. Sa Silva, M. Simek, F. Boavida, "A new approach for multi-sink environments in WSNs", *International Symposium on Integrated Network Management*, 2009. IM '09. IFIP/IEEE, pp. 109 – 112.

[26] Qingtian Sun, Shunfu Jin, Chen Chen, "Energy analysis of sensor nodes in WSN based on discrete-time queueing model with a setup", *Chinese Control & Decision Conference (CCDC)*, 2010, pp. 4114 – 4118, DOI: 10.1109/CCDC.2010.5498425.

[27] L. Lazos, R. Poovendran, C. Meadows, P. Syverson, L.W. Chang, "Preventing wormhole attacks on wireless ad hoc networks: a graph theoretic approach", *in: Proceedings of WCNC '05,* March 2005, pp.1193–1199.

[28] J. Petajajarvi, H. Karvonen, "Soft handover method for mobile wireless sensor networks based on 6LoWPAN", *International Conference on Distributed Computing in Sensor Systems and Workshops (DCOSS)*, 2011, pp. 1 – 6, DOI: 10.1109/DCOSS.2011. 5982208.

[29] Rohit Aggarwal, Er. Khushboo Bansal, "An Efficient Intruder Detection System against Sinkhole Attack in Wireless Sensor Networks: A Review", *International Journal of Computer Sciences and Engineering (IJCSE),* pp. 64 – 68, Volume-4, Issue-4, April 2016,

AUTHORS PROFILE

Rohit Aggarwal, Student of M.Tech, Computer Science and Engineering Department at Desh Bhagat University, Mandi Gobindgarh – 147301, Punjab, India. The research interest lies in Result Based approach on Intrusion Detection System against Sinkhole Attack in Wireless Sensor Networks.

Er. Khushboo Bansal, Assistant Professor of Computer Science and Engineering Department at Desh Bhagat University, Mandi Gobindgarh – 147301, Punjab, India. The research interest lies in Result Based approach on Intrusion Detection System against Sinkhole Attack in Wireless Sensor Networks.

© 2016, IJCSE All Rights Reserved