



DETECTING BLACKHOLE ATTACK IN WSN BY CHECK AGENT USING MULTIPLE BASE STATIONS

Nitesh Gondwal¹, Chander Diwaker²

CSE Department

University Institute of Engineering & Technology

Kurukshetra University, Kurukshetra

INDIA

Abstract: Due to the wireless nature and infrastructure-less environment of WSN, they are more vulnerable to many types of security attacks. This paper proposes a technique to detect the black-hole attack using multiple base-stations and a check agent based technology. This technique is Energy efficient, Fast, Lightweight and Reduces message complexity. An effective solution is proposed that uses multiple base stations to improve the delivery of the packets from the sensor nodes reaching at least one base station in the network, thus ensuring high packet delivery success. The proposed technique is more efficient than the previous techniques and gives better results. Check agent is a software program which is self-controlling and it moves from node to node and checks the presence of black-hole nodes in the network. Routing through multiple base stations algorithm is only activated when there is a chance of black-hole attack on the network.

Keywords: WSN, Black-hole attacks, multiple base stations & Check agent.

I. Introduction

A WSN is composed of large number of sensor nodes which are distributed in the wireless environment. This feature allows a random distribution of the nodes in the disaster relief operations or inaccessible terrains and several other applications. The other applications [9] of WSN includes environmental control such as fire-fighting or marine ground floor erosion, also installing sensors on bridges or buildings to understand earthquake vibration patterns, surveillance tasks of many kinds like intruder surveillance in premises, etc. Due to the wireless nature and infrastructure-less environment of WSN, they are more vulnerable to many types of security attacks. Generally, the attacks are of two types in WSN- active attacks and the passive attacks. Black-hole attack is one of the harmful active attacks.

II. Black Hole Attack

Black-hole attack- In the black-hole attack, a malicious node advertises the wrong paths as good paths to the source node during the path finding process as in reactive routing protocols or in the route updating messages as in proactive routing protocols. Good path means the shortest path from source node to the destination node or the most stable path through the sensor network.

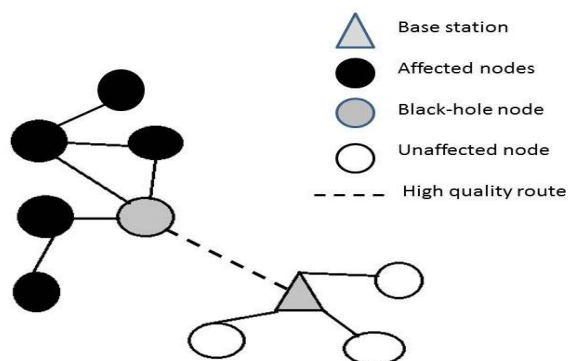


Fig. 1 Black hole Attack [15]

When the source select the path including the attacker node, the traffic starts passing through the adversary node and this nodes starts dropping the packets selectively or in whole. Here, these re-programmed nodes are termed as black hole nodes and the region containing the black-hole nodes are black hole region. Black hole region is the entry point to a large number of harmful attacks [14].

III. Checking Agents & multiple Base stations

In a WSN, successful packet delivery to the BS is more essentially required than the prevention of data to be captured by an attacker. By using efficient data encryption algorithms such as AES and data anonymity techniques, the information captured by an attacker can be made inconsequential. So, focus should be on the objective of delivering the packets to the BS in the presence of black hole nodes. Here, a good solution is proposed that uses multiple BSs placed in the network to improve the delivery of packets from the SNs reaching at least one BS in the network, thus ensuring high packet delivery success. In a WSN, a BS is a laptop class device so the idea of deploying multiple BSs is inexpensive. Here, multiple BSs are used to improve data delivery in the presence of black hole attacks.

Check agent is a software program which is self-controlling and it moves from node to node and checks the presence of black-hole nodes in the network. The technique is implemented using java language and the results are compared with and without the check agents.

IV. Related Work

An Algorithm has been proposed in which the list of neighboring nodes is maintained by each node in the network. Routing path is established here using Dijkstra algorithm. Initially, routing is done through the nearest base station i.e., without using multiple base stations technique. Routing through multiple base stations is only activated when there is a chance of black hole attack in the network. It is needed in the sensor networks to save the energy. Steps involved in algorithm are:

STEP 1- Routing through nearest base station is activated to send the packets.

STEP 2- when there is a chance of black-hole attack then to check the presence of black hole nodes in the network, Check agent randomly visits every node in the network

STEP 3- When check agent visits a node 'i',

- Checks the frequency of receiving packets for every neighboring node in the list of node 'i'.
- If it finds 0 (No packet from node 'j' to 'i') for neighboring node 'j',
- It doubts node 'j' is a black hole node and it triggers routing process algorithm through multiple base stations for time t.

STEP 4- Within time 't', it confirms whether node 'j' is a black-hole node or not.

STEP 5- If node 'j' is a black hole node, it revokes node 'j'.

STEP 6- After time 't', it triggers routing process algorithm through nearest base station.(without using multiple base stations).

V. Implementation Results

The technique is implemented using java language and the results are compared with and without the check agents. The parameters taken as shown below:

Parameters	Value
Network scale	200*200
No. of nodes	Random
No. of base stations	4
No. black-hole nodes	4
No. of check agent	1

Parameters used

This technique proves 99% better results than the previous techniques. The detection of the black-hole by the check agent is done in a better way with 99% assured. The results are shown below.

- Fig 2 shows the graph between the average energy of the nodes and time. This shows that the energy of nodes decreases with the increase in time.

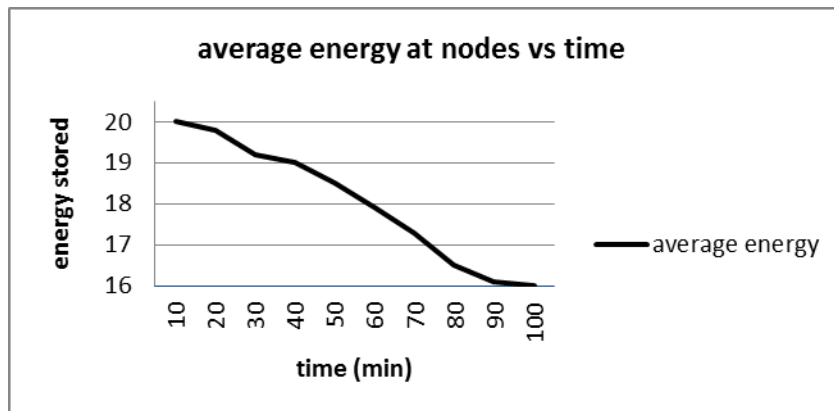


Fig. 2 Average Energy at nodes vs. Time

Fig. 3 shows that the no. of nodes increases as the radius of the black-hole region increases. As large is the black-hole region, more it covers the black-hole nodes.

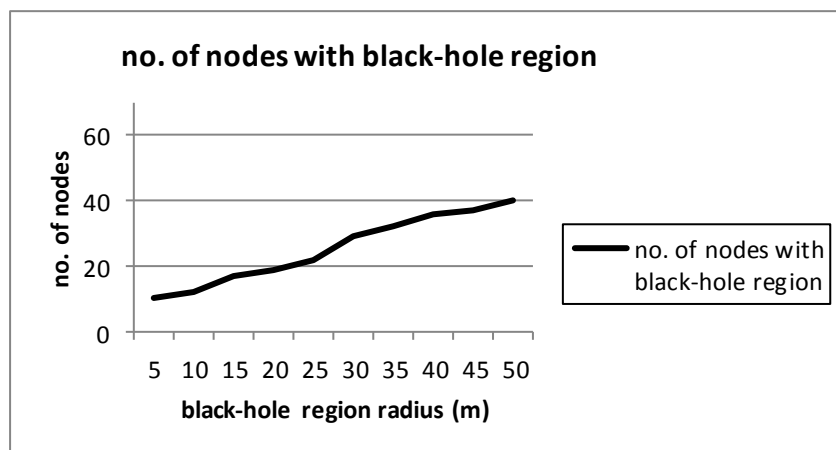


Fig. 3 No. of nodes vs. Black Hole Region Radius

Fig. 4 shows the %age of successful packet delivery with no. of base stations. It can be seen that the packet delivery is maximum in case of four base stations and least in case of one BS.

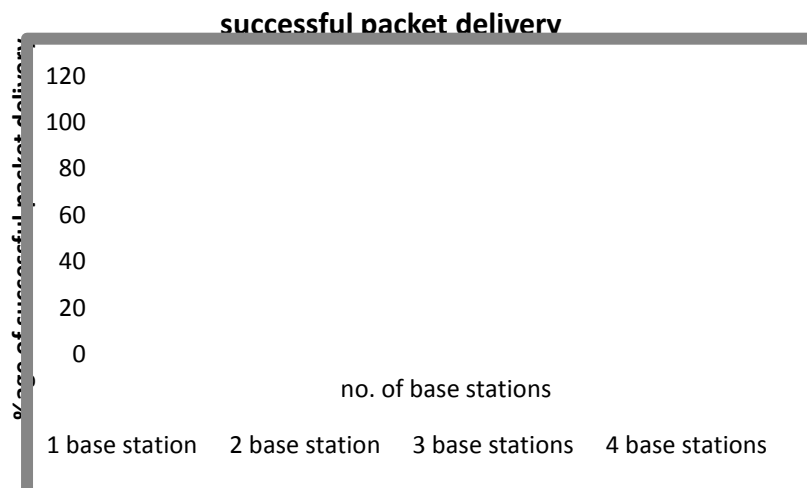


Fig. 4 Successful Packet Delivery vs. No. of Base Stations

Fig. 5 shows the message complexity with no. of nodes with and without check agent. It is shown that message complexity is more without check agent and less with the check agent.

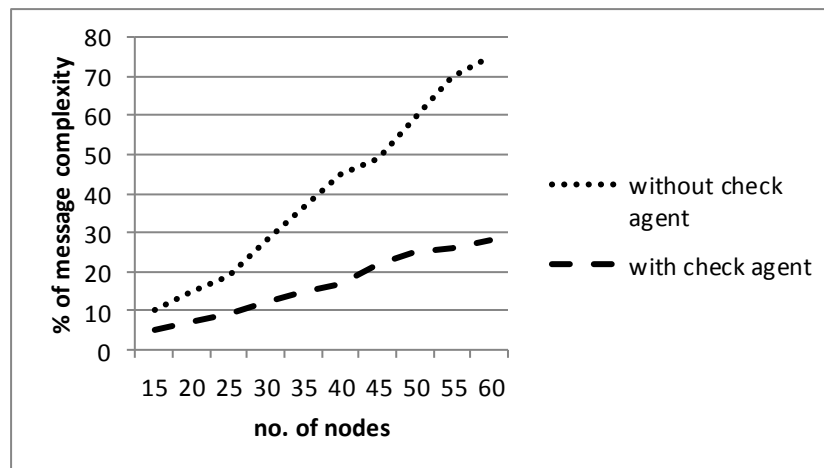


Fig. 5 Message Complexity vs. No. of Nodes

VI. Conclusion

The proposed work proves a 100% detection technique to prevent the occurrence of black-hole attack in WSN. This technique uses routing through multiple base stations only when there is a chance of occurrence of black-holes in the network. Otherwise routing through nearest base station is done to reduce extra use of messages in the network. Hence, it reduces the consumption of energy in the network by the node which is a major factor which is limited and is to be considered carefully in the sensor networks. Check agent plays a major role in the detection of black-holes in the network and also reduces extra overhead from the network. The data delivery is ensured as there is a provision of using multiple base stations in the network. But the work can be done further to handle the message complexity and to use less number of base stations in the network for better delivery results in the wireless sensor networks.

REFERENCES

- [1] Zhu Miaoliang, Qiuyu. "Mobile Agent System" Journal of Computer Research and Development, vol. 38(1), 2001, pp. 16-25.
- [2] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: A survey," Computer Networks, vol. 38, 2002.
- [3] L. Tong, Q. Zhao, S. Adireddy. "Sensor Networks with Mobile Agents", IEEE Military Communications Conference, Boston, MA, USA, 2003, pp.688-693;
- [4] Zhang Yuyong, Jingde. "Mobile Agent Technology" Beijing, Tsinghua University Press, 2003;
- [5] W. Lou, W. Liu, Y. Zhang, and Y. Fang. "SPREAD: Enhancing data confidentiality in mobile ad hoc networks"; In IEEE INFOCOM, volume 4, 2004. pp. 2404-2413;
- [6] Z. Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks"; In ACM Workshop on Real-World Wireless Sensor Networks, 2005;
- [7] M. Bailey, E. Cooke, F. Jahanian, J. Nazario, and D. Watson. "The Internet Motion Sensor: A distributed black-hole monitoring system", In Proceedings of the 12th ISOC Symposium on Network and Distributed Systems Security (SNDSS), 2005; pp. 167-179;
- [8] W. Lou and Y. Kwon. "H-SPREAD: A hybrid multipath scheme for secure and reliable data collection in wireless sensor networks"; IEEE Transactions on Vehicular Technology, 55(4):1320-1330, 2006.
- [9] R. Kompella, J. Yates, A. Greenberg, A. Snoeren, "Detection and Localization of network black holes"; In Proceedings of IEEE INFOCOM, 2007, pp. 2180-2188.
- [10] S. Roy, S. Singh, S. Choudhary, and N. Debnath. "Countering sinkhole and black hole attacks on sensor networks using dynamic trust management"; In IEEE Symposium on Computers and Communications, 2008; pp. 537-542.
- [11] Tao Shu, Marwan Krunz, and Sisi Liu, "Secure Data Collection in Wireless Sensor Networks Using Randomized Dispersive Routes" In IEEE INFOCOM, 2009. pp. 2846-2850.
- [12] G. Sladic , M. Vidakovic and Z. Konjovic "Agent based system for network availability and vulnerability monitoring" 2011 IEEE 9th International Symposium on Intelligent Systems and Informatics, September 8-10, 2011, Subotica, Serbia.
- [13] Satyajayant Misra, Kabi Bhattarai, and Guoliang Xue "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks" IEEE Communications Society subject matter experts for publication in the IEEE ICC 2011 proceedings
- [14] Atul Yadav et al., "Study of Network Layer Attacks and Countermeasures in Wireless Sensor Network" International Journal of Computer Science and Network (IJCSN) Volume 1, Issue 4, August 2012.
- [15] Gulshan Kumar, Mritunjay Rai and Gang-soo Lee "Implementation of Cipher Block Chaining in Wireless Sensor Networks for Security Enhancement" International Journal of Security and Its Applications Vol. 6, No. 1, January, 2012
- [16] M. Ketel, N. Dogan, A. Homaifar. "Distributed Sensor Networks Based on Mobile Agents Paradigm" International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012) Singapore, 2012;
- [17] Ping YI, Ting ZHU, Ning LIU, Yue WU, Jianhua LI "Cross-layer Detection for Black Hole Attack in Wireless Network" Journal of Computational Information Systems 8: 10 (2012) 4101-4109, 2012.