Detecting Black-Hole Attacks in WSNs using Multiple Base Stations and Check Agents

Reem Alattas
Department of Computer Science & Engineering
University of Bridgeport
Bridgeport, CT

***Abstract*—Wireless Sensor Networks (WSNs) consist of multiple sensors distributed in a certain geographic area. The goal of using WSNs is to monitor certain phenomena such as; environmental or physical. The nodes in WSNs transmit data through a wireless network that lacks infrastructure, which makes those networks exposed to security threats. One of those security threats is the black-hole attack which can be considered as a Denial of Service (DoS) attack that is very difficult to detect. In this attack, the intruder re-programs a set of nodes in the target network to prevent the received packets from being sent to the destination. Such changes to the sensors results in high delay and low throughput. Therefore, we propose in this paper a novel technique for detecting black-hole attacks in WSNs using multiple base stations and check agents.**

Keywords—Wireless Sensor Networks; WSN; Black-hole attacks; multiple base stations; check agents

I. INTRODUCTION

Wireless Sensor Networks (WSNs) consist of sensor nodes spread in an Ad Hoc manner that work together to collect data, process, and transmit. These sensors are used to monitor objects, areas, or both. However, WSNS are subject to various types of security attacks because of their wireless nature and infrastructure-less environment. One of the major attacks is the black-hole attack.

Black-hole attack is implemented using a malicious node that promotes bad routes to be used instead of good routes by source nodes during path finding process. We mean by good routes the shortest routes and the most stable.

When the source node specifies the path that includes the malicious node, this node starts dropping packets selectively or fully. These malicious nodes are called black-hole nodes and the region containing those nodes is called black-hole region. A typical black hole attack components are demonstrated in Fig. 1.

Problem Identification

In WSNs, black-holes are invisible and can only be detected by monitoring lost traffic. Therefore, delivering packets successfully to the destination is better than preventing data to be captured by an attacker. The data must be encrypted using an efficient encryption algorithm to make the packets captured by the attacker useless. Thus, packets can be delivered to the destination even in the presence of black-hole nodes.

In this paper, we propose a solution that uses multiple base stations to improve packets delivery from source nodes to destination through at least one base station to ensure successful packet delivery in the presence of black-hole attacks. Also, our proposed solution includes check agent which is a self-controlling software program that moves from one node to another checking for black-hole nodes.

II. RELATED WORK

After reviewing black-hole attacks in different types of networks, we found out that security solutions for addressing black-hole attacks in WSNs are different than the solutions proposed to solve the same threat in other networks types. The reasons are attributed to the low speed processing and the minimal storage requirements of WSNs [1].

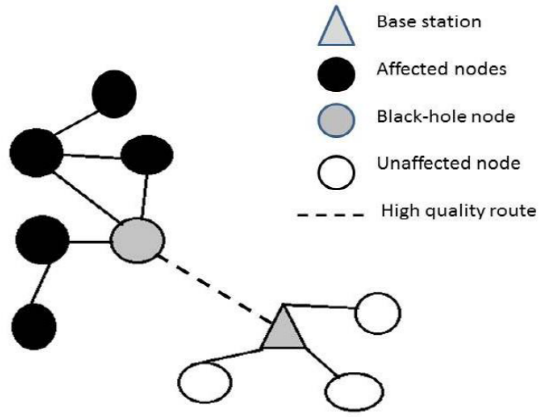

Fig. 1. Black Hole Attack

In [2], Karakehayov introduced REWARD, a new routing algorithm for black-hole attacks detection in WSNs. This technique saves information about black-hole nodes and regions in a distributed database. In order to avoid black-hole nodes, REWARD provides alternative paths for the geographic routing. This method uses two types of broadcast messages, MISS and SAMBA, to recruit security servers; which are nodes that keep records of the distributed database and modify the geographic forwarding of packets to avoid black-hole nodes and regions. This method is very costly because it requires O(n) for each original message; where n is the number of black-hole nodes.

978-1-5090-4171-8/16/$31.00 ©2016 IEEE

In paper [3], Lou and Kwon proposed H-SPREAD in 2006; a hybrid multipath scheme for secure and reliable data collection in WSNs. This scheme is based on SPREAD; a security protocol for reliable confidential data delivery in a mobile ad-hoc network (MANET); proposed by Lou et al in paper [4]. The new method is based on a distributed N-to-1 multi-path discovery protocol that can find multiple paths from every sensor node to the base station simultaneously in one process.

Randomized dispersive routes were suggested by Shu, Liu, and Krunz in [5] to secure data collection in WSNs by changing the routes over time. So, if the routing algorithm becomes known to the enemy, she cannot identify the route taken by each packet. Moreover, this new mechanism is capable of overcoming black-holes while consuming low energy which makes it cost effective.

Vulnerability of the WSN to black hole attacks was discussed by Prathapani et al in paper [6]. Those attacks are detected using intelligent agents called Honeypots. The Honeypots send dummy Route Request (RREQ) packets to detect black hole attacks.

Medadian et al presented a new methodology to detect black hole attack by using negotiation with neighbors claiming to have a route to destination in [7]. Simulation results indicate that the proposed method offers better security and packet delivery performance than conventional AODV in the presence of black holes with minimal added delay and overhead. Then, an effective approach that utilizes multiple base stations deployed in WSNs to counter black holes influence on transmission of data was presented in [8] by Misra et al.

In paper [9], Nanda and Krishna developed a scheme for preventing DoS attacks in WSNs. The proposed system defends the network against DoS attacks and assures confidentiality, integrity, and authenticity of transmitted data between sensor nodes. Then, Schaffer et al defined taxonomy of security and reliability for clustering in WSNs [10]. Furthermore, they mentioned classical attacks and suggested appropriate countermeasures against them.

Guechari and Mokdad proposed a new method for detecting Denial of Service (DoS) attacks in cluster-based WSNs in [11]. This new technique depends on the election of controller nodes (cNodes) that spot and report DoS attack actions. cNode examines traffic and warns the cluster head by sending a message if any unusual traffic is detected. The proposed solution improves the network performance by minimizing the energy consumption and improves security by avoiding attacks.

In paper [12], Tiwari et al proposed a specification based Intrusion Detection System for WSNs. The proposed system optimizes local information collected by watch dogs into global information. The global information in turn is decision taken by cluster head. It pays off the communication pattern in the network.

Blilat et al proposed a model for comprehensive security approach that can be used to address the needs of WSNs in [13]. The paper emphasized security features and challenges to be addressed in the design process of secure WSNs.

In paper [14], Yu et al categorized the different kinds of attacks and solutions associated with trust schemes in WSNs. Furthermore, it developed a trust mechanism and summarized some trust approaches.

Mahmood et al proposed and evaluated Data Packet Separation Slot Size Randomization (DS-SSR) and Round Robin (RR) slot size assignment in [15]. Both are modifications to the Lightweight Medium Access Control (LMAC) protocol. The paper shows the impact of using those security methodologies on network features; such as throughput and energy consumption.

In paper [16], Gill and Yang reviewed the design and implementation of an original defense strategy used to detect DoS attacks. The existing approaches were generic and did not filter out all attack traffic. Actually, a small amount of attack traffic reached the victims, which was considered as a major threat to WSNs due to their limited resources.

ZiaTanveer documented all known security concerns in WSNs along with the research direction towards suitable solutions and countermeasures in [17]. Then, Raymond and Midkiff surveyed various DoS attacks on WSNs and the proposed countermeasures in [18]. In paper [19], Modares et al discussed security issues in WSNs as security being fundamental to the acceptance. Finally, Pathan et al investigated security challenges in WSNs and concluded that most attacks in WSNs are caused by the insertion of false information by the compromised nodes within the network in [20].

III. Proposed Solution

The proposed solution forces every node in the network to maintain a list of neighboring nodes. Moreover, it uses Dijkstra's algorithm to establish the routing path and a check agent to examine the nodes.

Dijkstra's algorithm results from applying greedy method to single source shortest path problem. This algorithm outputs the weight of the shortest path not the path itself. However, we can obtain the path with a slight modification.

The check agent is a self-controlling software program that moves from node to another in order to check for the presence of black-hole nodes in the WSN. The Checkup resulting values are compared as explained next.

The proposed solution activates routing through the nearest base station to send the packets. Then, in order to detect black-hole attacks, the check agent randomly visits every node in the WSN to check the receiving packets frequency for every neighboring node. If the frequency equals to zero, the checked neighboring node is suspected to be a black-hole node and the routing process algorithm through multiple base stations is triggered to confirm whether the checked neighboring node is a black-hole node or not. If the node is happened to be a black-hole node, it will be isolated from the network. Otherwise, the routing process algorithm through the nearest base stations is triggered.

Routing through the nearest base station is done without using multiple base stations technique. The reason for

978-1-5090-4171-8/16/$31.00 ©2016 IEEE

switching between those two routing algorithms in the WSNs is to save energy by keeping the consumed energy at a minimal level.

IV. Mathematical Model

Our new method is designed to detect black hole attacks using multiple base stations deployed in the WSN using mobile agents. Routing through multiple base stations algorithm is activated only if a chance of black hole attack is detected. The probability of black hole nodes presence is found using mobile agents.

In order to check the probability of black-hole nodes presence, we follow the following methodology shown in Fig. 2:

- The mobile agent randomly visits nodes in the WSN.
- When mobile agent visits node *i*,
  - it checks the receiving packets frequency for every neighboring node in the list.
  - if it finds that the frequency is "0" (i.e. No packets from node *j* to node *i*) for neighboring node *j*,
- it suspects that node *j* is a black hole node
- it triggers the routing process algorithm through multiple base stations for time *t*
- Within time *t*,
- the mobile agent confirms whether node *j* is a black hole node or not
- if node *j* is a black hole node , it will be isolated from the network
- After time *t*, it triggers routing process algorithm through nearest base station

The primary goal of using check agent is to detect the black hole nodes. This is done by exchanging information between a node and its neighboring nodes in the network.

V. Simulation Results

Our proposed method was implemented using C++ programming language and tested on Castalia; a simulator for WSNs that is based on OMNet++ platform. The results were obtained twice for comparison; once while using check agents and once without using check agents. The parameters used for experimenting are shown in Table I.

Comparing the two results yielded that using check agents maximizes the chances of detecting black hole attacks by 99%. The results are discussed next.

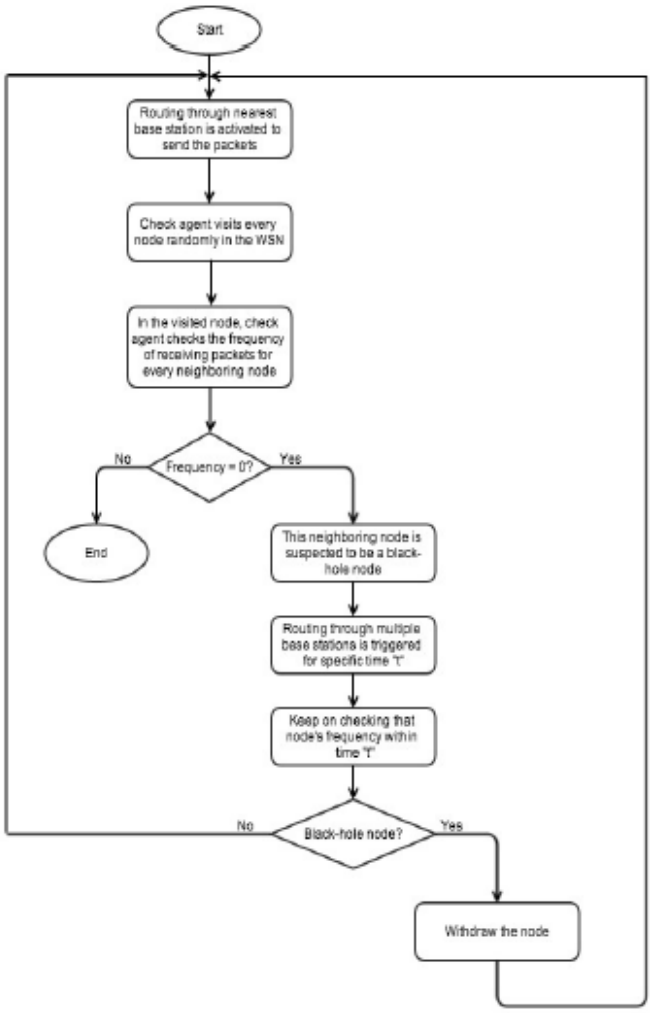

Fig. 2. Detection Process Steps

TABLE I. Used Parameters

Parameters	**Value**
Network Scale	200x200
No. of Nodes	Random
No. of Base Stations	4
No. of Black Hole Nodes	4
No. of Check Agents	1

Fig. 3 shows the relationship between the average energy consumed at sensor nodes and time. As time increases, the energy of nodes decreases because of neighboring nodes information storage at each node.

978-1-5090-4171-8/16/$31.00 ©2016 IEEE

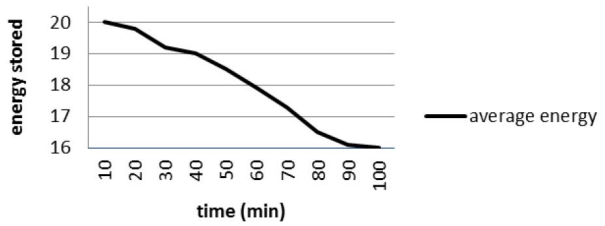

Fig. 3. Average Energy Stored at nodes vs. Time

As the radius of the black hole region increases, the number of affected nodes increases. Those nodes become black nodes accordingly as Fig. 4 shows.

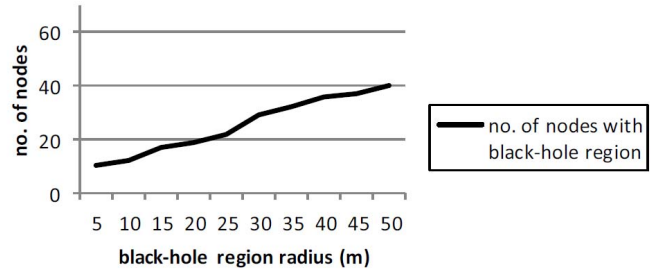

Fig. 4. No. of nodes vs. Black Hole Region Radius

Fig. 5 shows the effect of using check agents on the message complexity. It shows clearly that the complexity of the message increases without using check agents and decreases when using check agents.

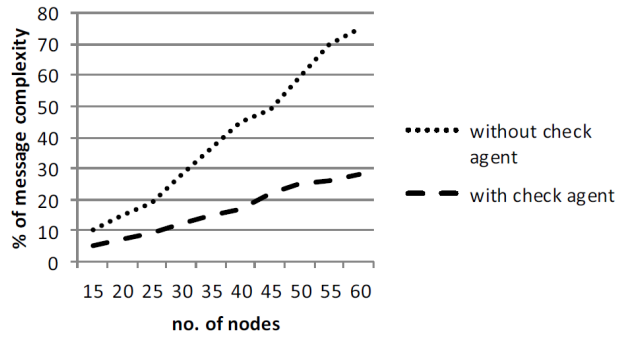

Fig. 5. Message Complexity vs. No. of Nodes

Finally, we concluded that as the number of nodes increases, the probability of detecting black hole attacks decreases; as Fig. 6 shows.

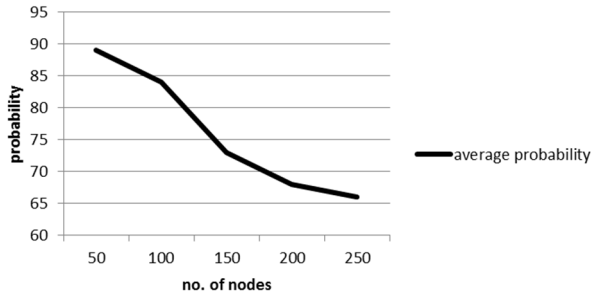

Fig. 6. Probability of Black Hole Attack Detection vs. No. of Nodes

VI. CONCLUSION

The proposed method effectively detects and prevents black hole attacks in WSNs. If there is a chance of black hole attack in the network, our method uses routing through multiple base stations. Otherwise, routing is done through the nearest base station only, in order to reduce energy consumption in WSNs. Also, we demonstrated that check agents have an important factor in black hole attacks detection in WSNs by decreasing the complexity of the messages and reducing network overhead. Data delivery is ensured due to the use of multiple base stations; which gives our method significant improvement compared to the current used methods.

REFERENCES

[1] Sheela.D, Srividhya.V.R, Asma Begam, Anjali and Chidanand G.M," Detecting Black Hole Attacks in Wireless Sensor Networks using Mobile Agent", International Conference on Artificial Intelligence and Embedded Systems (ICAIES'2012) July 15-16, Singapore, 2012.

[2] Z. Karakehayov. Using REWARD to detect team black-hole attacks in wireless sensor networks. In ACM Workshop on Real-World Wireless Sensor Networks, 2005.

[3] 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.

[4] W. Lou, W. Liu, Y. Zhang, and Y. Fang. SPREAD: Enhancing data confidentiality in mobile ad hoc networks. In IEEE INFOCOM, volume 4, pages 2404–2413, 2004.

[5] Shu, Tao, Marwan Krunz, and Sisi Liu. "Secure data collection in wireless sensor networks using randomized dispersive routes." Mobile Computing, IEEE Transactions on 9.7 (2010): 941-954.

[6] Anoosha Prathapani , Lakshmi Santhananr , Dharma P. Agrawal, "Intelligent Honeypot Agent for Blackhole Attack Detection in Wireless Mesh Networks", IEEE 6th International Conference on Mobile Adhoc and Sensor System (MASS) 2009.

[7] Mehdi Medadian, Ahmad Mebadi, Elham Shahri, "Combat with Black Hole Attack in AODV Routing Protocol", IEEE 9th Malaysia International Conference on Communications, 15 -17 December 2009.

[8] Satyajayant Misra, Kabi Bhattarai, Guoliang Xue, "BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks", IEEE International Conference on Communications (ICC) 2011.

[9] R. Nanda, P. Venkata Krishna, "A self enforcing and flexible security protocol for preventing Denial of Service attacks in wireless sensor networks", IEEE Recent Advances in Intelligent Computational Systems (RAICS) 2011.

[10] Peter Schaffer, Karoly Farkas, Adam Horvath, Tamas Holczer, Levente Buttyan, "Survey Secure and reliable clustering in wireless sensor networks: A critical survey", ACM, Computer Networks: The International Journal of Computer and Telecommunications Networking, July, 2012.

[11] M . Guechari, L. Mokdad, S. Tan, "Dynamic solution for detecting Denial of Service attacks in wireless sensor networks", IEEE International Conference on Communications (ICC) 2012.

[12] Mukesh Tiwari, Karm Veer Arya, Rahul Choudhari, Kumar Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", IEEE 4th International Conference on Computer Sciences and Convergence Information Technology (ICCIT) 2009.

[13] Asmae Blilat, Anas Bouayad, Nour el houda Chaoui, Mohammed El Ghazi, "Wireless Sensor Network: Security challenges", IEEE National Days of Network Security and Systems (JNS2) 2012.

[14] Yan Li Yu, Keqiu Li, Wanl Zhou, Ping Li, "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", Elsevier, Journal Of Network Computer and Applications, Special Issue on Trusted Computing and Communications, May 2012 Volume 35, Issue 3, Pages 867–880.

978-1-5090-4171-8/16/$31.00 ©2016 IEEE

[15] Ahmed R. Mahmood , Hussein H. Aly , Mohamed N. El-Derini, "Defending Against Energy Efficient Link Layer Jamming Denial of Service Attack in Wireless Sensor Networks", IEEE 9th IEEE/ACS International Conference on Computer Systems and Applications (AICCSA) 2011.

[16] K.Gill, Shuang-Hua Yang, " A scheme for preventing denial of service attacks on wireless sensornetworks", IEEE 35th Annual Conference of Industrial Electronics, (IECON '09) 2009.

[17] ZiaTanveer , Zomaya, "Security Issues in Wireless Sensor Networks", IEEE International Conference on Systems and Networks Communications (ICSNC) 2006.

[18] D.R.Raymond, S.F. Midkiff "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses", IEEE Pervasive Computing Jan-March 2008.

[19] Hero Modares, Rosli Salleh, Amirhossein Moravejosharieh," Overview of Security Issues in Wireless Sensor Networks", ACM 3rd International Conference on Computational Intelligence, Modelling & Simulation (CIMSIM '11), 2011.

[20] Al-Sakib Khan Pathan, Hyung-Woo Lee, Choong Seon Hong, "Security in Wireless Sensor Networks: Issues and Challenges", IEEE 8th International Conference on Advanced Communication Technology (ICACT) 2006.

978-1-5090-4171-8/16/$31.00 ©2016 IEEE