J Inf Process Syst, Vol.15, No.1, pp. 203~216, February 2019
https://doi.org/10.3745/JIPS.03.0110

ISSN 1976-913X (Print)
ISSN 2092-805X (Electronic)

JOURNAL OF INFORMATION PROCESSING SYSTEMS JIPS

A Novel Technique to Detect Malicious Packet Dropping Attacks in Wireless Sensor Networks

J. Sebastian Terence* and Geethanjali Purushothaman**

Abstract

The nature of wireless transmission has made wireless sensor networks defenseless against various attacks. This paper presents warning message counter method (WMC) to detect blackhole attack, grayhole attack and sinkhole attack in wireless sensor networks. The objective of these attackers are, to draw the nearby network traffic by false routing information and disrupt the network operation through dropping all the received packets (blackhole attack), selectively dropping the received packets (grayhole and sinkhole attack) and modifying the content of the packet (sinkhole attack). We have also attempted light weighted symmetric key cryptography to find data modification by the sinkhole node. Simulation results shows that, WMC detects sinkhole attack, blackhole attack and grayhole attack with less false positive 8% and less false negative 6%.

Keywords

Blackhole Attack, Grayhole Attack, Packet Dropping Attacks, Sinkhole Attack, Wireless Sensor Network

1. Introduction

Sensor nodes are grouped into wireless sensor network (WSN), where each sensor comprises of a power supply (commonly batteries), communication device (radio transceivers), analog-to-digital converter (ADC), information storage and a microprocessor. WSN has two categories, namely mesh-based system and multipoint-to-point or peer-to-peer system. The mesh-based system supports highly distributed applications like environmental monitoring and national security systems, where the multi-point-to-point system supports small short-range spaces such as home, an industrial unit, a construction area or a human body. Applications of wireless sensors include air traffic control, battlefield management, earthquake detection, habitat monitoring, heartbeat sensor, health care, mobile robotics, tsunami alerting, etc. [1]. WSN uses the radio communication system as a transmission medium which makes them susceptible to various attacks such as sinkhole attack, blackhole attack, grayhole attack, wormhole attack, etc.

In this paper, the authors studied packet dropping attacks namely blackhole attack, grayhole attack and sinkhole attack in WSN and analyzed various solutions to detect packet dropping attacks. In these attacks, an adversary compromises a sensor node by including false routing information, where compromised

Manuscript received July 26, 2016; first revision April 3, 2017; accepted May 29, 2017.
Corresponding Author: Geethanjali Purushothaman (pgeethanjali@vit.ac.in)
* Dept. of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu, India (jsebinfo@gmail.com)
**School of Electrical Engineering, VIT, Vellore, Tamil Nadu, India (pgeethanjali@vit.ac.in)

node advertises itself to own an excellent link to the destination node or the base station which misleads its neighbor nodes to utilize the route repeatedly [2].

The main motivation of these attacks are to attract the traffic of the network henceforth disturb the network by dropping the data and tampering the data. These attacks differ with strategy adopted by the attacker [3]. Researchers have been proposing various techniques to detect these attacks. But each technique has its own advantage and disadvantage in detecting these attacks. We have proposed a WMC to detect packet dropping attacks which successfully detects sinkhole attack, blackhole attack and grayhole attack.

The paper is grouped into six sections. Major types of packet dropping attacks in WSN are discussed in Section 2. Section 3 discusses various existing methods in detection of packet dropping attacks. Section 4 exhibits the proposed WMC method in detail. The implementation methodology of the proposition is asserted in Section 5 and the conclusion is given in Section 6.

2. Problem Statement

WSN are majorly prone to the following packet dropping attacks: sinkhole attack, blackhole attack, and grayhole attack.

In sinkhole attack [4], the compromised node advertises itself to possess an excellent link to the base station which misleads the neighbors of the compromised node to choose and utilize the route to reach the destination node repeatedly. To attract the surrounding network traffic and to make it appear possessing an excellent link to the base station, the compromised node modifies routing packets to advertise fake routing information. Likewise, neighbors of the compromised node selects forged route for data communication. In Fig. 1, the compromised node broadcasts fake route information to possess an excellent link to the base station and mislead its neighbors to forward the packets through sinkhole node to the base station. Every neighbor of the sinkhole node chooses this node to forward the data packets to the base station. In this fashion sinkhole node attracts its neighbors node traffic. It can drop the data packets, selectively drop the data packets and tamper the data packets.

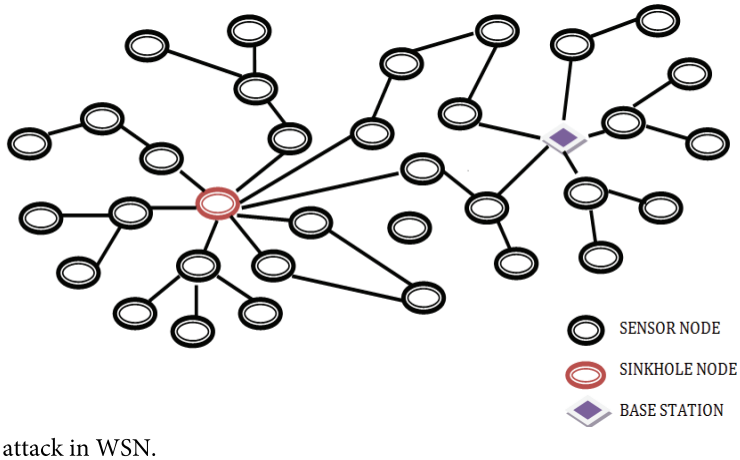


Fig. 1. Sinkhole attack in WSN.

In blackhole and grayhole attack, the source node broadcast a route request to find the path to the destination node. The compromised node sends fake route information with highest sequence number and lowest hop count for the destination node [5,6] when it receives route request from the source node. After receiving all the route replies, the source node approves forged malicious route since its hop count is minimum compared to the other available route. After route selection, the victim node uses the forged route to send the data. During data dissemination, the compromised node may drop all the data packets in case of blackhole attack where as in grayhole attack compromised node drops the data packet statistically following a predetermined probability distribution [7].

The primary objectives of these attacks are to attract the network traffic with fake routing information and to disturb the normal network flow. Various techniques to detect these packet dropping attacks have been discussed in the next section.

3. Related Work

Sanchez-Casado et al. [7] proposed an anamaly-based intruder detection system (IDS) to identify adversary packet dropping behaviors in wireless network. Here IDS gathers various network related information from each node. Using this information, the packet dropping probability (P_D) is calculated. The calculated dropping probability (P_D) is compared with a predefined threshold value and the system concludes the reviewed node as a genuine node if P_D is lesser than the threshold value, otherwise it concludes as a compromised node. The dropping probability (P_D) depends on the probability of the control packet to be lost due to collisions (P_{CLOST}), the probability of the packet loss due to broken links (P_{PLOST}) and the probability of data packet forwarded ($P_{FORWARD}$). The disadvantage is that the initial computation cost for finding the dropping probability of each node is high.

Kumar and Kumar [6] used a specific table to store all the incoming route replies for route request. The source node stores all the received routing details like source ID, destination ID, destination sequence number (DSN), etc. in a table until route selection. Before route selection, DSN of the route replies are compared with the threshold value. If the DSN of route reply is greater than the threshold value, then the algorithm concludes that the route information is generated by blackhole attack otherwise source node selects a route for data dissemination. The limitation is every node should run the detection algorithm to identify the fake route.

Dhaka et al. [8] used code sequence packet and response sequence packet to detect grayhole and blackhole attack. Code sequence packet contains the sender details with sender sequence ID and the response sequence packet contains receiver details with destination sequence ID. Route request is broadcasted within the communication range, when a node needs to transfer a data packet to the destination node. The algorithm concludes a node to be malicious, if the receiver sequence ID is much higher than the sender sequence ID.

Su [5] proposed intrusion detection systems to prevent blackhole attacks in wireless networks. IDS nodes are introduced. It records route request packets in one table and records unreliable route replies in another table. IDS node stores each node's number of broadcasted route request and the number of forwarded route request. In this technique, if the intermediate node is not the target node, then it has to forward route request packet to its neighbor, but instead of forwarding route request packet to its neighbor, if it forwards route reply packet, the neighboring IDS node increases its deceitful value by 1. If

the deceitful value is greater than the threshold value, IDS blocks the respective node by broadcasting a block message.

Mohanapriya and Krishnamurthi [9] proposed modified dynamic source routing (DSR) for the recognition and elimination of selective blackhole attack. In modified DSR, the data packet is sent to the destination through the shortest path and intimates the quantity of data package to be sent in a block to the target using different routes (2nd shortest path to arrive at the destination). The destination node calculates the probability of the packet acknowledged, if the probability of packet acknowledged at the destination is greater than threshold value of packet loss, the target node propels an ALARM packet to the neighbor IDS node. The IDS node detects the malicious node by checking the number of data packets promoted by all the nodes from the source node to two-hop distance.

Balakrishnan et al. [10] projected TWOACK technique to perceive malicious nodes in a network. In this method a network layer acknowledgement is used to detect the malicious node. In this technique, while forwarding a packet, two-hop acknowledgement is sent to other nodes to confirm the nodes cooperation. Liu et al. [11] also used 2ACK method. The major difference is that the TWOACK method does not use any authentication method to avoid tampering of data packets, it suffers with message overhead due to two acknowledgement message for every data packet. In 2ACK method, an authentication mechanism is given to prevent tampering of its acknowledgement packets and also message overhead is reduced with one acknowledgement.

Heydari and Yoo [12] used medium access control (MAC) layer acknowledgement called PIGACK instead of network layer acknowledgement to detect misbehavior nodes in wireless network. In PIGACK method, every node has to maintain a table to store malicious flag and reporter node details. Each node when sends a data packet and receives PIGACK packet it must save next node's confirmation and sends back with its confirmation for the next packet transformation. If a node fails to send PIGACK two times, it will be marked as a misbehaving node and will be abandoned from other nodes. The above-mentioned ACK methods (i.e., TWOACK, 2ACK and PIGACK) suffers due to computation overhead where every nodes should run the algorithms to detect the malicious node. But in WMC method, the monitor node collects response from other nodes and detects the compromised node.

In [4], the authors proposed geo-statistical method and distribution method to detect and mitigate sinkhole attacks in WSN. The sinkhole node can attract other nodes to use its route to the base station. The neighboring nodes of the sinkhole node loses its energy faster than other nodes. Therefore, nodes around the sinkhole will experience the energy hole problem. In this technique, the base station samples the deployment area and obtains residual energy of the sensor nodes. If residual energy of the target node is less than the system wide energy threshold, it will be marked as suspicious region. The geo-statistical approach is centralized approach on the other hand network is distributed. The main limitation of these schemes is high computation cost.

Sreelaja and Vijayalakshmi Pai [13] proposed an intrusion detection system based on swarm intelligence to detect sinkhole attack in wireless sensor network. All the sensors have own intrusion detection system. Sensor node finds the sinkhole node using a rule matching method. The received route replies link qualities are compared with rule set to detect the malicious node. Voting method is used to confirm the malicious node. To minimize the number of keys required for authentication, an ant colony optimization method has been used. This method suffers due to more number of comparisons at each node to detect sinkhole attack.

Sundararajan and Arumugam [14] proposed instruction detection technique for low energy adaptive

clustering hierarchy (LEACH). Base station runs detection algorithms to identify sinkhole attack and selectively packet dropping attacks. Base station gets the number of packet transmitted value (ptv) and number of packet received value (prv) from cluster head and cluster members. Using received value, packet dropping ratio (pdr) is calculated and if pdr tends to ∞, then the respective cluster head is assumed as sinkhole node. This method detects sinkhole node if and only if sinkhole node plays as a cluster node. The prevention and identification method for data modification by sinkhole node is not addressed in this paper.

4. Detection Method

4.1 Network Model and System Assumption

The network is modeled with sensor node and monitor node. Sensor node does sense the data and forward to the destination node. Monitor node monitors the sensor nodes under its region and identifies the compromised node in the network. Each sensor node has a unique identifier, random function F, key K_x. The key (K_x) is saved in the sensor memory and it can be deleted completely [15]. Pair-wise shared key can be used to create data packet and its acknowledgement. Detailed authentication mechanism in WSN can be found in secure route discovery against wormhole attacks in sensor networks (SeRWA) [15], thus this part is not covered here. Hence the compromised node can't create acknowledgement for the data packet. We have assumed that no attackers work in cooperative manner. In cooperative attacks, multiple malicious nodes would work jointly to deceive the victim nodes [16,17]. The proposed WMC method intends to detect the malicious attacks, where a malicious node does not work in collaborative fashion.

4.2 One Hop Neighbor Discovery

Each sensor node discovers one hop neighbors by broadcasting hello messages. Reply is got from every node that accepts the hello message. Each node only accepts the first hello message from its neighbor. Based on the received hello messages, every node's neighbor list is constructed.

4.3 Preliminary Route Discovery

In preliminary route discovery process, the source node triggers route discovery by broadcasting routing beacons to discover shortest path to the base station. Each node admits with the first routing beacon from its neighbor. The updated routing beacon will be rebroadcast by each node. After receiving route reply from its neighbors, the source node selects shortest path for data transformation.

4.4 Data Dissemination

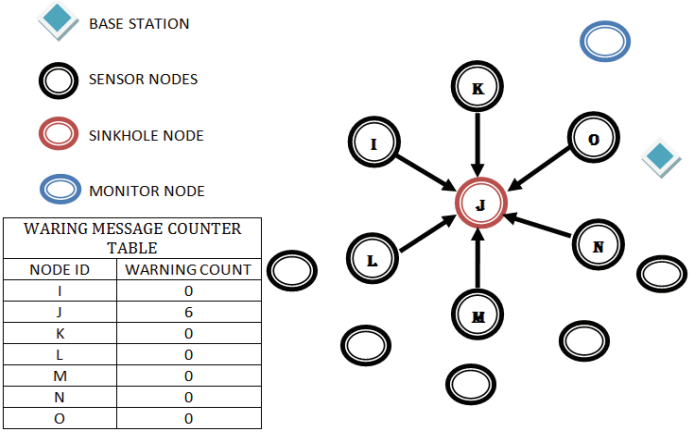
After route discovery, the source node directs the data packet to the destination node or to the base station by the chosen shortest path. In data dissemination, packet dropping attacks can be detected by warning message counter (WMC) method.

4.5 Warning Message Counter

In WMC method, each monitor node maintains the monitor table. The monitor table contains two fields, node ID and the warning count (WC). In this method, the source node selects the shortest path and directs the data packet to the destination through the chosen route. Acknowledgement will be send by the destination node for the received data packet. If no acknowledgement is received from the destination after sending the data packet through the selected path, the source node propels a warning message to the monitor node about the advertiser node. Whenever the monitor node receives this warning message, it updates warning count of the particular node in the monitor table. WMC can be explained in two cases: case I (sinkhole attack) and case II (blackhole attack and grayhole attack).

Case I

In Fig. 2, consider node J as the sinkhole node, and node J advertises that it possess a good quality link. By receiving this fake advertisement the nodes I, K, L, M, N, O which is around J sends data packets to the node J. If the nodes I, K, L, M, N, O doesn't receive an acknowledgement from the base station, then the nodes I, K, L, M, N, O sends a warning message to the monitor node about the advertiser node J, otherwise they continue data dissemination through node J. By receiving this warning message, the monitor node increases the warning count of node J as shown in Algorithm 1.



WARING MESSAGE COUNTER TABLE

NODE ID	WARNING COUNT
I	0
J	6
K	0
L	0
M	0
N	0
O	0

Fig. 2. Example for warning message counter method.

Algorithm 1. Warning message counter

// The sensor node executes the following code

1. sensor node[i] sends Route Request for base_station to its neighbors [j,k,l,m]
2. ***if*** *node i receives Route Reply from the neighbor node* ***then***
3. select shortest route (Ex:j);
3. node i sends data packet to the base_station through shortest route (Ex:j)
4. ***if*** *node i fails to receive Acknowledgement from the base_station* ***then***
5. i sends a warning message to the monitor node about route advertiser node j
6. ***else***
7. node i continues data dissemination through the chosen path

// The monitor node executes the following code

1. ***if*** *the monitor node receives warning message about node j* ***then***
2. Monitor node increases warning count (WC)of j
3. ***if*** *WC(j) > λ* ***then***
4. j is malicious node;
5. Monitor node warns all the senor nodes in its region by sending alert message
6. ***else***
7. wait for warning message;

// The sensor node executes following code

1. ***if*** *sensor node[i] receives alert message from Monitor Node about node j* ***then***
2. node i removes node j from it's neighbor list
3. node i triggers route discovery
4. ***else***
5. node i continues data dissemination through node j

Case II

Case A: Let the source node I broadcast route request packet to discover a route to the destination node Z. The black hole node X sends route reply with large sequence number and fewer hop count to the source node. By receiving this fake route reply, the source node I chooses this path for data dissemination and sends data packet to node Z through node X. If the source node I fails to obtain acknowledgement then the source node sends a warning message to the monitor node, otherwise it continues data dissemination through X. By receiving this warning message, the monitor node increases the warning count of the adviser node X.

Case B: Grayhole attack is a special type of blackhole attack. The compromised node X drops all the received data packet in case of blackhole attack, where as in grayhole attack node X drops the data packets selectively [7].

In WMC, monitor node periodically checks the warning count status of each node in the monitor table.Comparing the threshold value with the warning count of a particular node the monitor node senses it as a compromised node otherwise the monitor node waits for warning count messages.

The threshold value of warning count is calculated based on the mean value of warning counts in a region. The threshold value of warning count is calculated as follows:

Calculation for threshold value of Warning Count:

Initialize Sum_Warning_Count = 0

n: Number of nodes in the region

$$Sum\_Warning\_Count = Sum\_Warning\_Count + \sum_{i=1}^{n} Warning\_Count(i) \quad (1)$$

$$Mean = (Sum\_Warning\_Count)/n \quad (2)$$

$$\lambda = c * Mean \quad where \quad 1.5 \leq c \leq 2 \quad (3)$$

The malicious node detection depends on the threshold value. The selection of threshold plays a vital role in malicious node detection. Detailed discussion of threshold selection is given in Section 5.

4.6 Secure Route Discovery against Malicious Node

The monitor node sends a compromised node list to all the sensor nodes in its region. Each node checks its neighbors list with the received malicious node list. If the node contains malicious node as its neighbor, it will remove the malicious node from the neighbor list and reconstructs its neighbor list by triggering neighbor discovery process.

In sinkhole attack, the malicious node can modify the data packet. As we are using authentication mechanism which is used in SeRWA [15], each node verifies the received data packet integrity through message authentication code. If verification fails, the data packet has been modified by sinkhole node and the received packet ought to be dropped. Otherwise data packet will be broadcast to the next node. If the data packet is tampered between two nodes, then the receiver node sends a red alert message to the monitor node about its sender node. Let the receiver node be Y and sender node be X. When the monitor node receives a red alert message about X, it sends red alert message to the all nodes in its region. If a node has red alert node (i.e., node X) as its neighbor, then it will remove the red alert node and rebuild its neighbor list by triggering neighbor discovery process.

4.7 Cost Analysis

Let N be number of sensor nodes in the network and N_{Avg} average neighbors for sensor node, where $N_{Avg} < N$.

The total time complexity of proposed WMC is linear to the number of sensors in the network (Table 1).

Table 1. Time complexity computation

No	Function	Time complexity
1	Neighbor discovery	$O(N * N_{Avg}) = O(N)$
2	Route discovery	$O(N)$
3	Warning message counter	$O(1)$
4	Total time complexity	$O(N)$

5. Performance Evaluation

We have used NS2 [18] for performance analysis. MannaSim Framework patch [19] is used with NS2 to create a sensor network environment. The simulation area covers 1000×1000 m^2. The communication range of each node is 60 m. The simulation parameters are given in Table 2. WMC is implemented to discover the packet dropped by the compromised node. The source node chooses the shortest path after the preliminary route discovery for data broadcast. Once the route is selected the source node directs the data packets to the destination in the chosen path. Data broadcast is done if an acknowledgement is received from the destination node, otherwise a warning message is sent to the monitor node about the chosen path. A comparison is made in the monitor node with the responses and the threshold value, in order to detect possible compromised activities. Some good nodes (false positive) are erroneously detected as compromised node. There may be various reasons for false positive. Packet drop may occur

due to collision in packets, errors in accessing shared medium, inference or signal loses, packet errors, etc. The compromised node detection depends on the threshold value. Small threshold value increases false positive, but large threshold increases false negative where false negative is nothing but the malicious node determined as a good node. Following three scenarios are simulated and Figs. 3–6 show the impact of threshold value in false positive and false negative rate.

Table 2. Software and hardware parameters

No.	Parameter	Value
1	Simulator	NS-2.34
2	Framework	MannaSim
3	Network size	1000×1000
4	MAC type	Mac / 802_11
5	Queue type	PriQueue
6	Transmit power (mW)	0.036
7	Receive power (mW)	0.024
8	Frequency (MHz)	914
9	Initial energy (J)	12
10	Processor	Intel Core i5 4570 @3.2–3.6 GHz
11	RAM	16 GB DDR3
12	Operating system	Fedora 16

1) Sinkhole Attack scenario: The compromised node creates attention towards the traffic by publicizing itself to have high quality link to the base station. The compromised node can drop all or selectively drop or modify the data packets.
2) Blackhole Attack scenario: The compromised node prepares fake route reply for route request and attracts the data packet and then the compromised node drops all the received packets.
3) Grayhole Attack scenario: The compromised node drops the packet selectively.

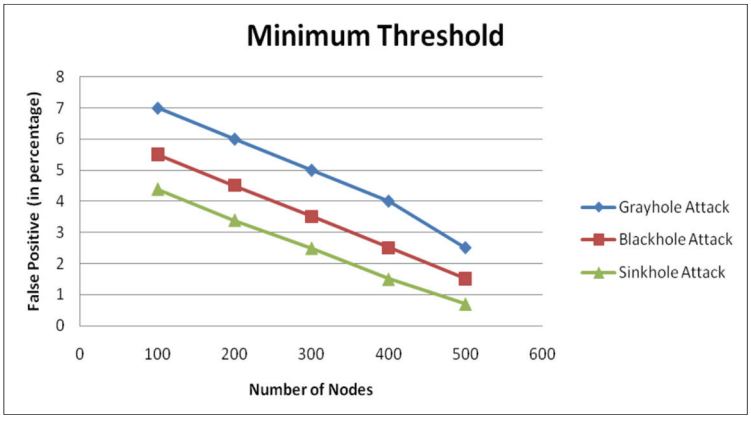


Fig. 3. Nodes versus false positive (c=1.5).

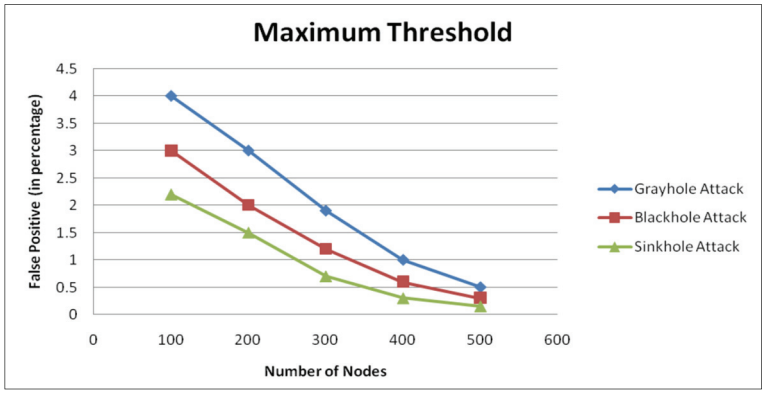


Fig. 4. Nodes versus false positive (c=2).

Figs. 3 and 4 describe a link between the false positive and the sensor nodes with different types of attacks under minimum threshold (c=1.5) and maximum threshold (c=2). Likewise Figs. 5 and 6 describes the bond between the false negative and the number of sensor nodes with different types of attacks under minimum threshold (c=1.5) and maximum threshold (c=2).

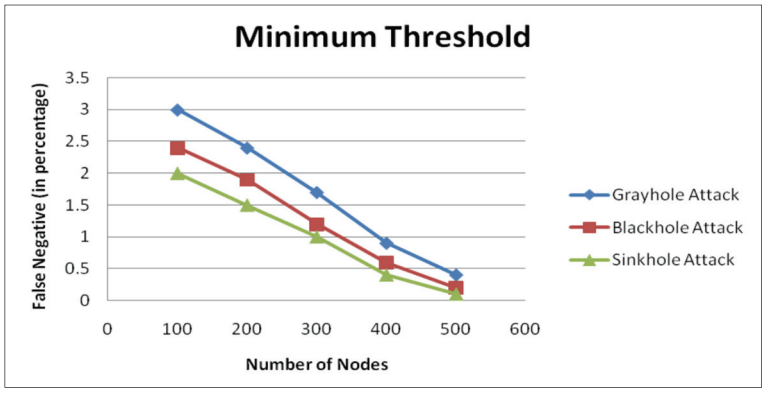


Fig. 5. Nodes versus false negative (c=1.5).

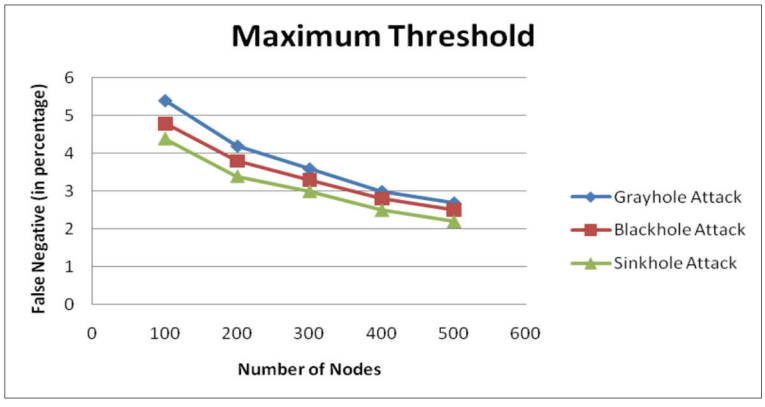


Fig. 6. Nodes versus false negative (c=2).

From Figs. 3–6, we find the minimum threshold amplifies false positive and reduces false negative. On the other hand maximum threshold reduces false positive and amplifies false negative. Another notable things is when number of nodes in the sensor network is amplified false positive and false negative are reduced. This is because increase in nodes reduces legitimate packet drop by normal nodes.

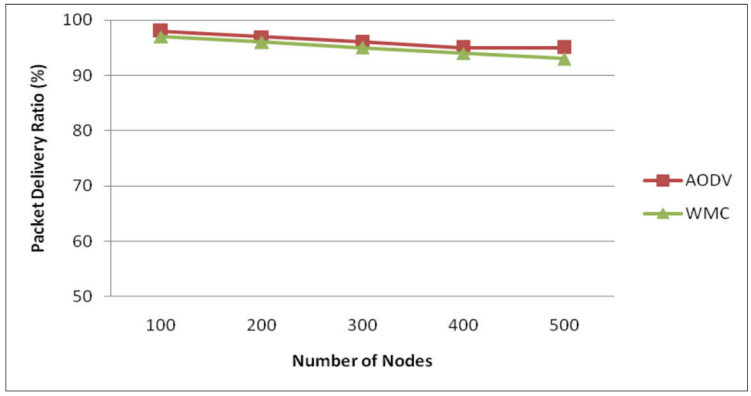


Fig. 7. Number of nodes versus packet delivery ratio.

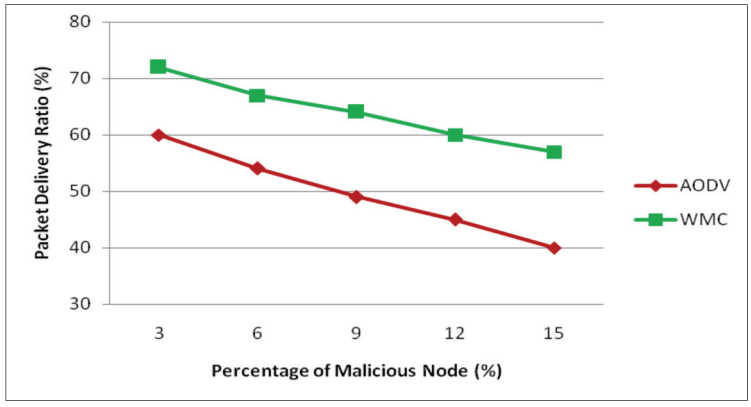


Fig. 8. Percentage of malicious node versus packet delivery ratio.

The performance of the proposed technique is compared with the AODV protocol in terms of throughput, packet delivery ratio (PDR) and routing overhead for evaluation. PDR is defined as the ratio of the number of data packets successfully received by the destination node to the number of packets sent by the source node. From Figs. 7 and 8, it is observed that the PDR of the proposed technique is higher than the AODV when there is an existence of malicious nodes in the network. This is due to safe route selection technique against malicious node in the route discovery.

Routing overhead (RO) is defined as the ratio of the number of routing packet transmitted with respect to the number of data packet transmitted in the network. Figs. 9 and 10 show that the routing overhead of AODV is high when there is an existence of malicious nodes in the network. The routing overhead of AODV is increased because it needs to send more number of control packets due to malicious activities of the compromised node. On the other hand in the proposed technique routing overhead is decreased, in the presence of malicious nodes.

Throughput is the ratio of the packets successfully received with respect to the simulation time. The channel bandwidth is assigned as 2 Mbps (approximately) between source node and destination node. Figs. 11 and 12 show that throughput of AODV is decreased in the presence of malicious node. But the proposed technique throughput is 1.7 Mbps, even in existence of the malicious node.

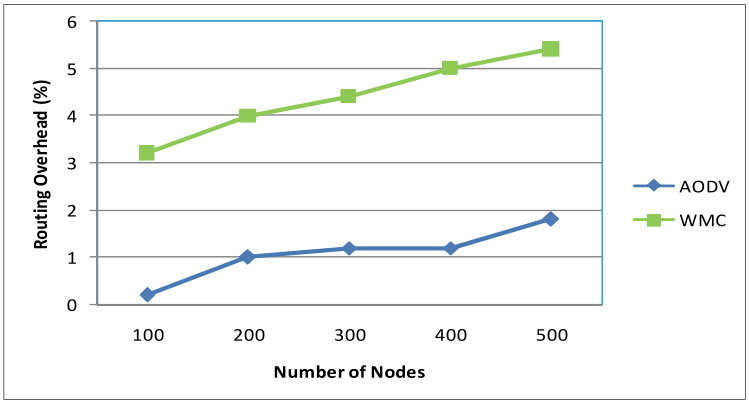


Fig. 9. Number of nodes versus routing overhead.

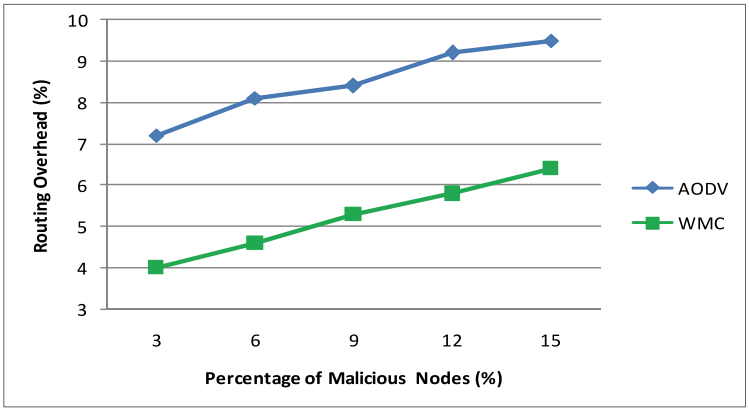


Fig. 10. Percentage of malicious node versus routing overhead.

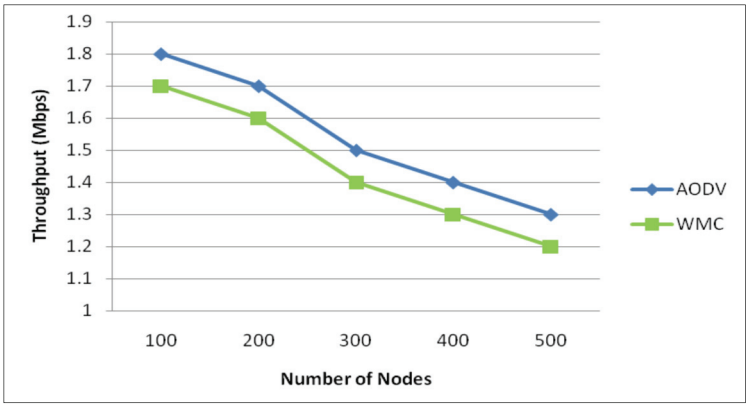


Fig. 11. Number of nodes versus throughput.

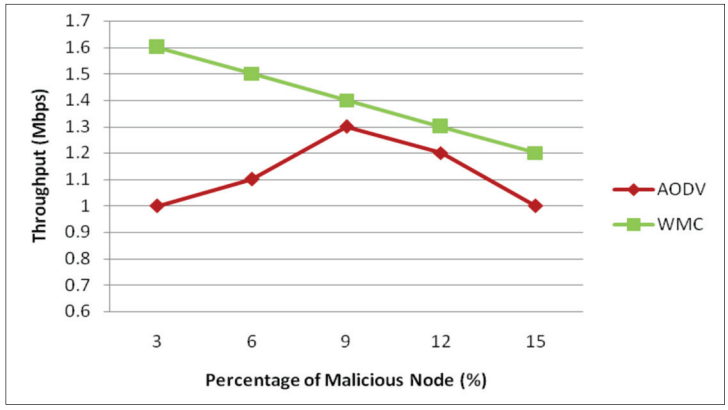


Fig. 12. Percentage of malicious node versus throughput.

6. Conclusion

A novel acknowledgement-based WMC is developed that uses network layer acknowledgement to identify packet dropping attacks in wireless sensor network. Most of the presented acknowledgement based approaches suffers due to computation overhead, where every nodes should run the algorithms to detect the malicious node. But in WMC method, the monitor node collects response from each node and detects the malicious node. The WMC technique is tested against three attacks namely sinkhole attack, blackhole attack and grayhole attack and the end result shows the correctness and efficiency of WMC in malicious node detection. The experimental result also shows that WMC technique has very small false positive and false negative in packet dropping detection. In future, the proposed algorithm can be extended for the detection of cooperative attacks, where numerous nodes work in collusion to avoid the detection process.

References

[1] K. Sohraby, D. Minoli, and T. Znati, *Wireless Sensor Networks: Technology, Protocols, and Applications*. Hoboken, NJ: John Wiley & Sons, 2007.

[2] R. W. Anwar, M. Bakhtiari, A. Zainal, and K. N. Qureshi, "Wireless sensor network performance analysis and effect of blackhole and sinkhole attacks," *Jurnal Teknologi (Science & Engineering)*, vol. 78, no. 4-3, pp. 75-81, 2016.

[3] C. John and C. Wahi, "Security analysis of routing protocols for wireless sensor networks," *International Journal of Applied Engineering Research*, vol. 11, no. 6, pp. 4235-4242, 2016.

[4] H. Shafiei, A. Khonsari, H. Derakhshi, and P. Mousavi, "Detection and mitigation of sinkhole attacks in wireless sensor networks," *Journal of Computer and System Sciences*, vol. 80, no. 3, pp. 644-653, 2014.

[5] M. Y. Su, "Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems," *Computer Communications*, vol. 34, no. 1, pp. 107-117, 2011.

[6] V. Kumar and R. Kumar, "An adaptive approach for detection of blackhole attack in mobile Ad hoc network," *Procedia Computer Science*, vol. 48, pp. 472-479, 2015.

[7] L. Sanchez-Casado, G. Macia-Fernandez, P. Garcia-Teodoro, and R. Magan-Carrion, "A model of data forwarding in MANETs for lightweight detection of malicious packet dropping," *Computer Networks*, vol. 87, pp. 44-58, 2015.

[8] A. Dhaka, A. Nandal, and R. S. Dhaka, "Gray and black hole attack identification using control packets in MANETs," *Procedia Computer Science*, vol. 54, pp. 83-91, 2015.
[9] M. Mohanapriya and I. Krishnamurthi, "Modified DSR protocol for detection and removal of selective black hole attack in MANET," *Computers & Electrical Engineering*, vol. 40, no. 2, pp. 530-538, 2004.
[10] K. Balakrishnan, J. Deng, and V. K. Varshney, "TWOACK: preventing selfishness in mobile ad hoc networks," in *Proceedings of 2005 IEEE Wireless Communications and Networking Conference*, New Orleans, LA, 2005, pp. 2137-2142.
[11] K. Liu, J. Deng, P. K. Varshney, and K. Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehavior in MANETs," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 536-550, 2007.
[12] V. Heydari and S. M. Yoo, "Lightweight acknowledgement-based method to detect misbehavior in MANETs," *KSII Transactions on Internet And Information Systems*, vol. 9, no. 12, pp. 5150-5169, 2015.
[13] N. K. Sreelaja and G. A. Vijayalakshmi Pai, "Swarm intelligence based approach for sinkhole attack detection in wireless sensor networks," *Applied Soft Computing,* vol. 19, pp. 68-79, 2014.
[14] R. K. Sundararajan and U. Arumugam, "Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor network," *Journal of Sensors,* vol. 2015, Article ID. 203814, 2015.
[15] S. Madria and J. Yin, "SeRWA: a secure routing protocol against wormhole attacks in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051-1063, 2009.
[16] Q. Liu, J. Yin, V. C. Leung, and Z. Cai, "FADE: forwarding assessment based detection of collaborative grey hole attacks in WMNs," *IEEE Transactions on Wireless Communications*, vol. 12, no. 10, pp. 5124-5137, 2013.
[17] M. Sathish, K. Arumugam, S. N. Pari, and V. S. Harikrishnan, "Detection of single and collaborative black hole attack in MANET," in *Proceedings of International Conference on Wireless Communications, Signal Processing and Networking*, Chennai, India, 2016, pp. 2040-2044.
[18] The Network Simulator (NS2) [Online]. Available: http://www.isi.edu/nsnam/ns/.
[19] MannaSim [Online]. Available http://www.mannasim.dcc.ufmg.br/index.htm.

J. Sebastian Terence https://orcid.org/0000-0002-1965-3402

He received his M.Tech. degree in Computer Science and Engineering from Karunya University, Coimbatore, India in 2010. He is doing Ph.D. in VIT Univesity, Vellore, India. Currently he is working as Assistant Professor in Karunya University, Coimbatore. His research interests include sensor networks, MANET, networks and algorithms.

Geethanjali Purushothaman https://orcid.org/0000-0002-6659-7052

She received her B.E. degree in Electrical and Electronics Engineering from University of Madras, India in 2001. She obtained M.Tech in Electrical Drives and Control from Pondicherry Engineering College, India, in 2004. She received her Ph.D. degree from VIT University, Vellore, India, in 2012. Her Ph.D. thesis has been nominated for "Best Thesis" by Indian National Academy of Engineering (INAE). She received grants from the Department of Science and Technology (DST), Government of India. She also received Fulbright-Nehru Academic and Professional Excellence Fellowship for 2014-2015. Currently she is working as Associate Professor in VIT-Vellore. Her research interests include bio-signal and image processing, pattern recognition, development of assistive devices, biomechanics and applications of renewable energy in assistive device.