Behavior based Routing Misbehavior Detection in Wireless Sensor Networks

Sebastian Terence[1, 2], Geethanjali Purushothaman[2*]
[1] Department of Computer Science and Engineering, Karunya Institute of Technology and Sciences, Coimbatore, Tamil Nadu - India
[e-mail: jsebinfo@gmail.com]
[2] School of Electrical Engineering, VIT, Vellore, Tamil Nadu - India
[e-mail:pgeethanjali@vit.ac.in]
*Corresponding author: Geethanjali Purushothaman

Received August 30, 2018; revised March 24, 2019; revised April 15, 2019; accepted May 16, 2019; published November 30, 2019

Abstract

Sensor networks are deployed in unheeded environment to monitor the situation. In view of the unheeded environment and by the nature of their communication channel sensor nodes are vulnerable to various attacks most commonly malicious packet dropping attacks namely blackhole, grayhole attack and sinkhole attack. In each of these attacks, the attackers capture the sensor nodes to inject fake details, to deceive other sensor nodes and to interrupt the network traffic by packet dropping. In all such attacks, the compromised node advertises itself with fake routing facts to draw its neighbor traffic and to plunge the data packets. False routing advertisement play vital role in deceiving genuine node in network. In this paper, behavior based routing misbehavior detection (BRMD) is designed in wireless sensor networks to detect false advertiser node in the network. Herein the sensor nodes are monitored by its neighbor. The node which attracts more neighbor traffic by fake routing advertisement and involves the malicious activities such as packet dropping, selective packet dropping and tampering data are detected by its various behaviors and isolated from the network. To estimate the effectiveness of the proposed technique, Network Simulator 2.34 is used. In addition packet delivery ratio, throughput and end-to-end delay of BRMD are compared with other existing routing protocols and as a consequence it is shown that BRMD performs better. The outcome also demonstrates that BRMD yields lesser false positive (less than 6%) and false negative (less than 4%) encountered in various attack detection.

Keywords: False route advertisement, Wireless Sensor Network, Blackhole attack, Grayhole attack, Sinkhole attack.

1. Introduction

In recent days, the applications of wireless sensor network (WSN) have been increasing rapidly. Sensor networks are generally deployed in unheeded environment such as battle field, temperature monitoring, animal monitoring, etc. Sensor node collects data from the physical phenomenon and sends it to the base station through multiple hop fashion. They are limited in energy, processing and memory. Since, sensor nodes are placed in open environment, its communication nature makes sensor nodes highly defenseless against various attacks such as selective forwarding, sinkhole, grayhole, blackhole, wormhole, sybil, selfish and pollution attacks [1]. Human interruption cannot be provided for sensor network to deal with adversary attacks. Instead autonomous cooperative, coordinated actions and pre-programmed policies, help WSN to protect it against adversary [2].

Packet dropping attacks such as blackhole attack, grayhole attack and sinkhole attack use the same strategy to launch the attack. In these attacks, the compromised node deceives the genuine node by attracting fake routing information. Even though these attacks use the same strategy, the consequence of the above mentioned attacks differs by its nature of attack. In blackhole attack, the compromised node drops all the received data packets. In grayhole attack, the compromised node drops selective data packets and in sinkhole attack, the compromised node may drop all the data packets or drop few data packets or tamper the received data [3, 4]. Methodologies such as cryptography based technique, network coding based technique, behavior based technique, sequence number based technique, etc are used to identify various malicious activities in the network [5, 6]. All these methodologies have their own advantages and drawbacks. Since these attackers use similar technique to launch these attacks, we attempt to develop a solution to avoid and detect these attacks in WSN.

From the literature, it is understood that malicious node attracts more packets & drops more packets, and that its network participation is very limited such as it initiates/forwards very less number of control packets [7, 8]. Based on this fact, we have proposed behavior based routing misbehavior detection (BRMD) against packet dropping attacks. The objective of BRMD is to detect and mitigate malicious node in the network. To detect the malicious nodes, behavior of each node is monitored by its neighbors and periodically collected in the center node called monitor node. Monitor node is a special node which periodically runs detection algorithm and is used to detect malicious nodes in the network. The detection algorithm analysis is based on the following behavior of sensor nodes i) packet (data/ack) forwarding nature ii) control packet forwarding nature iii) route reply parameter such as sequence number and hop count. If a nodes route reply is always attractive and found that the node drops more number of data packets then it will be assumed as malicious node. The advantages of the proposed BRMD are, high detection accuracy compared to the other existing method and that it yields less false positive and false negative. The result also shows that the performance of BRMD is higher than the other existing protocols. The paper is organized into six sections as follows: Section 2 discusses the major types of packet dropping attacks in detail; Section 3 presents the literature review of various existing methods in detection of packet dropping attacks. Section 4 exhibits the proposed BRMD method in detail; Section 5 asserts the implementation methodology of the proposition and the conclusion is made in section 6.

2. Packet Dropping Attacks in Wireless Sensor Network

In wireless network, routing protocols can be classified into proactive, reactive and hybrid protocols. The proactive routing protocols such as optimized link state routing (OLSR), destination sequence distance vector (DSDV), etc. maintains the routing information for all available routes, even if it is not required. Periodic update of the topological information is required always. But in reactive protocols such as ad hoc on-demand distance vector (AODV), dynamic source routing (DSR), etc. obtains a route only when it is required. In AODV protocol [9] the source node triggers route discovery process when it wants to transfer data to the destination node by broadcasting route request (RREQ) message to its neighbor. This reduces the control packets required for route establishment and route maintenance. The neighbor nodes send route reply (RREP), if it has a route to the destination node, otherwise the intermediate node broadcasts RREQ message to its neighbor. When RREQ reaches the destination node, RREP is sent to the source through inverse routes from the destination node. AODV also allows intermediate nodes to send RREP when it has valid route to the destination node.

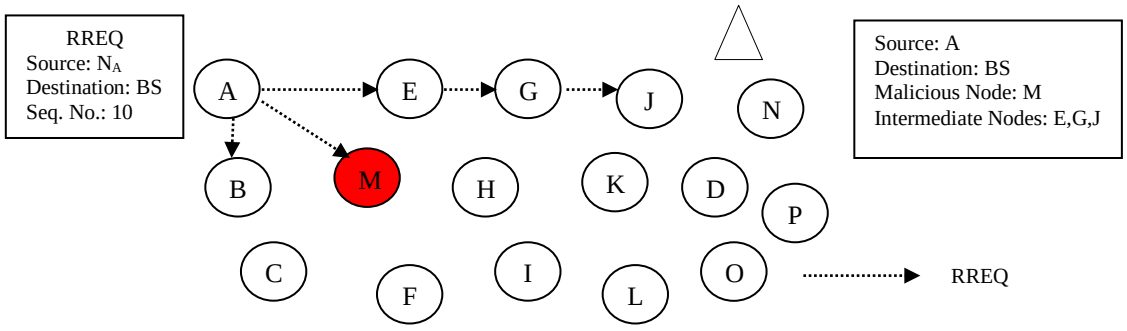

Fig. 1. Broadcast RREQ to its neighbors

Source node may receive more than one route to the destination node. It may use routing credentials such as sequence number and hop count for best route selection. Sequence number is updated by the intermediate node, when it receives new control packet related to the destination node. This sequence number helps a node to identify the freshness of the route. Hop count determines the number of intermediate nodes between the source and the destination node. The source selects route with minimum hop count. The RREP with maximum sequence number and minimum hop count is fresh route with less number of intermediate nodes between the source and the destination. The source node selects this route when multiple RREP is received. This fact can be misused by the malicious node in packet dropping attacks such as blackhole attack, grayhole attack and sinkhole attack where the malicious node advertises itself to have the best route to the destination node which attracts the surrounding network traffic and misleads its neighbor nodes to use this route repeatedly. Likewise, victim nodes selects forged route for data dissemination.

The network is modelled such that node A transfers packet to the base station. **Fig. 1** shows node A, broadcast RREQ to its neighbors. Let node M is malicious. It prepares fake RREP(M) with minimum hop and high sequence number (Hop Count=1, Sequence Number=35) for the base station and sends to it node A. Node J, which is one hop neighbor to the base station, prepares RREP(J) with legitimate values (Hop Count=3, Sequence Number =12) and sends to source node A. **Fig. 2** shows reception of RREP at node A. The source node compares all the received RREP and selects the shortest route. Here node M which contains less hop count and

high sequence number is selected for data dissemination. The surrounding node B also sends the data packet to the base station through node M, since it seems to be the most recent with an optimal hop count as shown in **Fig. 2**. In this way malicious node attracts its neighbor node traffic. After attracting the surrounding network, the malicious node can drop the entire data packet (in case of blackhole attack), selectively discard the data packet (in case of grayhole attack and sinkhole attack) [10].

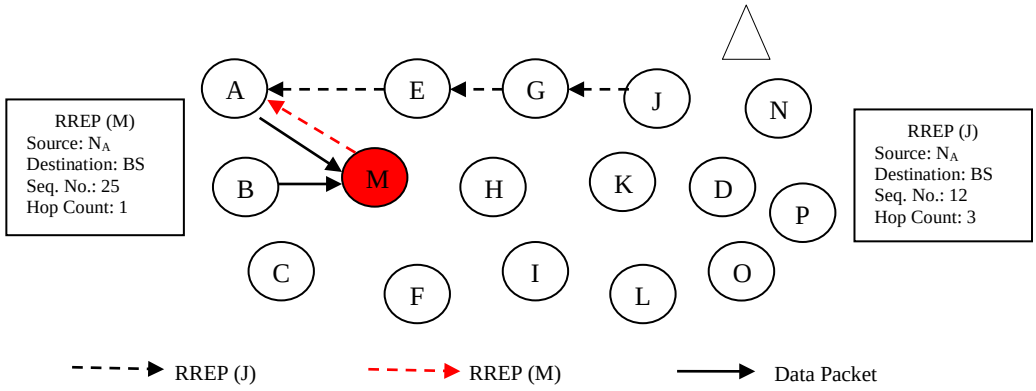

Fig. 2. Reception of RREP

3. Related Work

Researchers have initiated different techniques to detect malicious packet dropping attacks. These solutions can be classified as follows: Behavior based detection, sequence number based detection and acknowledgment based detection.

3.1 Behavior Based Detection

In behavior based detection, the behavior of a node such as number of packet received, number of packet forwarded by a node, packet loss rate are calculated by its neighbors (or) intrusion detection system (IDS) and the observed values are used for malicious node detection.

Ju Ren et al. [11] proposed a channel aware detection technique with adaptive detection threshold (CRS – A) to identify selective forwarding attacks in WSN. Here network lifetime is divided into an evaluation period, estimation stage and data transmission stage. Each node calculates its neighbors reputation value based on its behavior. Medium access control (MAC) layer collisions are also considered when it calculates reputation value. The limitation of this method is that the sensor nodes are static. Umer et al. proposed fuzzy based geographic forwarding protocol (FuGeF) [12] to avoid malicious node in packet transmission. This technique uses three parameters such as distance, connectivity cost and remaining energy to evaluate the sensor node. By using these three parameters, sensor nodes chooses the genuine node to forward data packets to the destination. Later this work was enhanced by the same author as trust based fuzzy implicit cross layer protocol (TruFix) [13]. In TruFix, node trust is calculated by different parameters such as traffic statistics, signal to noise ratio, remaining buffer capacity, relay packet rate, packet's waiting relay period and etc., to evaluate sensor nodes. If the sensor's reputation is greater than the maximum trust value, then the sensor would be classified as trusted node, if minimum then the sensor would classified as Distrusted node. If sensor's reputation is less than the maximum trust and greater than the minimum trust, then the sensor would be classified as uncertain node. The limitation of this technique is, it

does not detect malicious node. Marti et al. [14] introduced one of the reputation methodology called watchdog to mitigate misbehavior node in wireless network. Watchdog monitors each node by checking whether received packet is transferred or not. If the received packet is in a buffer for more than a certain time period, then the watchdog increases fault count. When the fault count is greater than the threshold value, watchdog concludes the node as misbehaving. Watchdog mechanism suffers due to high number of false detection. Different proposal are given by many researchers based on watchdog IDS to detect malicious node in wireless network. As we mentioned earlier, all these techniques suffer due to high false detection.

3.2 Sequence Number Based Detection

The sequence number is one of the parameters to deceive the victim nodes. Since false sequence number is used to deceive victim nodes, many researchers used sequence number based detection technique against packet dropping attacks.

Babu Karuppiah et al. [15] used status bit and sequence number based detection technique against malicious packet dropping attacks to improve the watchdog monitoring system in WSN. The status bit reduces false identification of malicious node. The negative and positive value of status bit helps to identify the suspicious node with downstream and upstream nodes with malicious sequence. Multiple attackers cannot be handled with this technique. Dhaka et al. [8] used two control packets namely 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. The algorithm concludes a node to be malicious, if the receiver sequence ID is much higher than the senders sequence ID from the received route reply packets. As this technique depends only on sequence number to detect malicious node, false detection rate is high. Vimal et al. [16] used coming route reply table (CRRT) to store all the incoming route replies for route request. CRRT contains various fields like source address, destination address, hop count, next hop, lifetime and destination sequence number. It compares the destination sequence number of each route reply with the threshold value. If the destination sequence number of route reply is greater than the threshold value, then the algorithm concludes that the route reply packet is generated by blackhole attack. The limitation of this method is, selective packet drops and multiple attackers are not identified in this technique.

3.3 Acknowledgment Based Detection

In acknowledgment based detection technique, network layer acknowledgment [17, 18, 19, 20] is used. In these techniques, each node expects acknowledgment from its neighbor's neighbor.

Balakrishnan et al. [18] projected TWOACK technique to perceive malicious nodes in a network. In this method, a network layer acknowledgment detects the malicious node. Here, while forwarding a packet, two-hop acknowledgment is sent by each node in reverse direction to confirm the nodes cooperation. Liu et al. [19] also adopted similar procedure and called as 2ACK method. The TWOACK method does not use any authentication method to avoid tampering of data packets and suffers with message overhead due to two-acknowledgment message for every data packet from intermediate node. In 2ACK method, an authentication mechanism is given to prevent tampering of its acknowledgment packets and message overhead is reduced by sending one acknowledgment instead of two. Shakshuki et al. [20] also used network layer acknowledgment called end-to-end-acknowledgment (EAACK), against blackhole attack detection. The EAACK utilizes TWOACK to detect the misbehavior node in

the route. EAACK uses alternative (second) route to communicate the destination and confirm the malicious node. If the alternative route suffers with misbehaving activity and if it drops the packets selectively, then EAACK fails to detect the malicious node. Altisen et al. [17], proposed a technique where the network layer acknowledgment is used to assess the neighbors. Whenever the source node forwards data to the sink node, it waits for an acknowledgment form the sink node. If the source node receives an acknowledgment, then it increases the reputation of its neighbor. In route discovery process nodes choose neighbor whose reputation value is high. This technique is only optimal for static network. Above mentioned acknowledgment based detection techniques suffers due to message overhead [18, 19] and high computation [17]. Each node has to send an acknowledgment to its neighbors neighbor for every data packet and each node has to run the detection algorithm to detect the malicious node [17, 19, 20].

Most of the above discussed methodologies relay only on one parameter namely sequence number [8, 15, 16], packet acknowledgment [17, 18, 19, 20], buffer memory [14] to detect malicious node. This increases false positive and false negative. To overcome this issue, we have used multiple parameters such as packet delivery rate, number of control packet sent, sequence number, hop count to detect malicious node. It helps to decrease false detection rate and increases detection technique performance in terms of packet delivery rate and throughput. In the next section a detailed description is provided about the proposed technique.

4. Behavior based Routing Misbehavior Detection

4.1 Network Model and System Assumption

The network contains two kind of nodes namely i) Sensor Node ii) Monitor Node. Sensor node does sense the environment and also involves in routing operations such as forwarding/receiving data, control and acknowledgment packets. Monitor node monitors the sensor nodes under its region and identifies the compromised node in the network. Monitor nodes are high end nodes [10], which run the algorithm and assess the sensor nodes. These nodes have high energy and computation power when compared with sensor nodes. They are aware about their real distance to the base station and other monitor node. Monitor nodes communicate with each other when it is required. Sensor nodes have a key K_x, random function F and a unique identifier. Sensor uses pair-wise shared key to create data packet and acknowledgment packet. The complete authentication procedure used in WSN can be found in secure route discovery against wormhole attacks in sensor networks (SeRWA) [21], so this part is excluded here. Therefore the compromised node can't create acknowledgment for the data packet. Destination node prepares and sends (in reverse direction) acknowledgment packet to the source node for the received data packet. Sensor node maintains listener_table (LT) in which the sensor node stores the no_of_packet_sent (nps), no_of_packet_received (npr) and occurence_value (ov), sequence number (sn), hop count (hc). Sensor node forwards its LT to the monitor node with regular time interval. LT construction is given in algorithm I in section 4.3. We assume that the network is free from bad mouthing attack [22], so the compromised node cannot manipulate LT values and compromised nodes do not work in cooperative fashion [23].

Monitor node uses its resources in monitoring the sensor nodes. Monitor node collects LT from the sensor nodes and stores the received LT details such as such as nps, npr, ov, sn, hc into monitor_table (MT). Then the monitor node calculates the following: global_no_of_packet_sent (gnps), global_no_of_packet_received (gnpr),

global_occurance_value (gov), global_sequence_number (gsn), global_hop_count (ghc) by finding cumulative of the received LT values which is explained in algorithm II in section 4.3. Before discussing the steps in BRMD, some basics definitions are given below for better understanding.
a) Source: Node which sends data to destination node (or) base station.
b) Sender: Node which forwards data to its neighbor.
c) Receiver: Node which receives data from its neighbor.
d) Destination: Node which collects data from source node.

4.2 Listener Table Parameters

In BRMD, each node is rated with five factors no_of_packet_sent (nps), no_of_packet_received (npr), occurence_value (ov), sequence number (sn) and hop count (hc). The assessment procedure of nps, npr, ov, sn and hc are given below.
a) No_of_packet_sent (nps): Whenever a node (sender) sends data packet to its neighbor (receiver), the sender node increases the nps of its neighbor (receiver) in its LT. In the same vein, when a node sends acknowledgment packet to its neighbor, the sender node increases the nps of its neighbor (receiver) in the listener table.
b) No_of_packet_received (npr): BRMD is designed in such a way that, when a node (receiver) receives the data packet or ACK from its neighbor (sender), the receiver increases the npr of sender. For example, if node A forwards data packet to node B, then node B would increases the npr of node A.
c) Occurrence value (ov): Occurrence value is used to exemplify the active participation of the sensor nodes in the network. Whenever a node hears the control message from its neighbor, the receiver node increases the occurrence value of its neighbor (sender) in the listener table. In general, the part of malicious node is very less compared to the genuine node as a consequence the occurrence value used to identify the malicious nodes in route discovery process.
d) Sequence number (sn): After choosing optimal route for data dissemination, the source node stores sequence number of (optimal) route reply in its LT with respect to the route initiator (advertiser).
e) Hop count (hc): Similarly hop count of optimal route reply is stored in LT with respect to the route initiator (advertiser).

Periodically sensor node shares the LT values with the monitor node. Monitor node detects malicious node based on the received values. The detection technique of malicious node is discussed in the next section.

4.3 Malicious Node Detection

In this technique, when node needs to transfer data to base station (or) destination, it triggers route request. Node which is having route to destination sends route reply. The source node chooses optimal route for data dissemination. After choosing optimal route, routing credentials such as sequence number and hop count of route reply is stored in LT (Line 8-10). Whenever a node shifts the data packet (or) the acknowledgment packet to its neighbor the nps of the neighbor (receiver node) is increased (Line 1-2), together the receiver increases the npr of the sender node (Line 3-4). Furthermore the sender ov is increased by the receiver node when it receives control packet from its neighbor (Line 5-6). In all cases, the values are accrued by one. This listener table maintained by the sensor node is shared periodically to the monitor node.

Algorithm I: Listener Table Construction

```
// The sensor node executes the following code
//Initially nps(x) = 0, npr(x) = 0, OV(x) = 0
//  i is sender and x is receiver
1. if node i sends data packet ||ACK packet to node x then
2.     node i increases the nps of receiver node in its listener table by 1 // nps(x) = nps(x) +1
//  i: receiver and x is sender
3. else if node i receives data packet or ACK packet from node x then
4.    node i increases the npr of sender node in its listener table by 1 // npr(x) = nprx) + 1
5. else if node i receives control packet from node x then
6.    node i increases the OV of sender node in its listener table by 1 // OV(x) = OV(x) +1
7. end if
8. if node i chooses route for data dissemination then
9.    node i records sequence number and hop count of route reply
       // sn(x) = sn(x) + sn && hc(x) = hc (x) + hc
       //here x is a node, which initialize route reply
10. end if
```

By this means the monitor node constructs a monitor table. Algorithm II (Line 11-23) is designed in such a way that the monitor table calculation is based on the cumulative nps (Line 15), npr (Line 16), ov (Line 17), sn (Line 18), hc (Line 19) of each node from its neighbor observation**.** These cumulative values are called as global values namely gnps, gnpr, gov, gsn, ghc. Monitor node calculates the packet delivery ratio (PDR) of each node in Line 20 and is defined as ratio between numbers of packet received from a node to the number of packet sent to a node from a node. These cumulative values are values used in malicious node detection, which is explained in algorithm III.

Algorithm II: Construction of Monitor Table

```
// The monitor node executes the following code
// Initially gnps(x) = 0; gnpr(x) = 0; gov(x) = 0; gsn(x)=0; ghc(x)=0;
//  x is any node in MT (Monitor Table)
// i= 1 to n; where n is number of entries in LT (Listener Table)
// j=1 to m; where m is number of sensor nodes under monitor node
11. sensor node[i] sends LT to the monitor node
12. for each i in MT(M)
13.     for each j in LT(N)
14.         if LT[nodeid] == MT[nodeid] then
15.               gnps(j) = gnps(j) + nps(i)
16.               gnpr(j) = gnpr(j) + npr(i)
17.               gov(j) = gov(j) + ov(i)
18.               gsn(j) = gsn(j) + sn(i)
19.               ghc(j) = ghc(j) + hc(i)
20.               PDR(j) = gnps(j) / gnpr(j)
21.           end if
22.     end for
23. end for
```

Algorithm III: Malicious node detection

```
// Monitor node executes the following code
// i= 1 to m; where m is number of sensor nodes under monitor node
24. for each i in m
25.       if PDR[i] < λPDR
26.             suspicious[i] = suspicious[i] + 1
27.       end if
28.       if gov(i) <  λO
29.             suspicious[i]  = suspicious[i] + 1
30.        end if
31.        if gsn[i] > λSq
32.              suspicious[i] = suspicious[i] + 1
33.        end if
34.        if ghc[i] > λHC
35.              suspicious[i] = suspicious[i] + 1
36.        end if
37.        if suspicious[i] >= 3
38.             add node i to malicious node
39.        else if suspicious[i] =2
40.            add node i to suspicious node
41.         end if
42.  end for
```

In the process of malicious detection, the choice of threshold is considered to be significant since malicious node discovery depends on the threshold value.

The threshold values are calculated based on the mean of the PDR, the occurrence value, sequence number and the hop count in a region. The threshold value of the PDR is calculated as follows,

Let Sum_PDR = 0

n: Number of Nodes in the region, λ_{PDR} : packet_delivery_ratio_threshold

$$Sum\_PDR = Sum\_PDR + \sum_{i=1}^{n} PDR(i) \quad (1)$$

$$Mean = (Sum\_PDR)/n \quad (2)$$

$$\lambda_{PDR} = c * Mean \ where 1.5 \le c \le 2 \quad (3)$$

In the same way remaining threshold values [(i-e) occurrence_threshold (λ_O), sequence_number_threshold (λ_{sq}), hop_count_threshold (λ_{hc})] have calculated. The selection of threshold plays vital role in malicious detection as the malicious detection depends on the threshold value. Detailed discussion on threshold selection is given in section 5.

4.4. Penalty for Malicious Node

The monitor node checks various parameters (PDR, gov, gsn and ghc) of sensor node with the threshold value. If sensor node obtains greater value compared to the threshold value, then the monitor node increases the suspicious value of the node (Line 24-36). If the suspicious value of sensor node is greater than or equal to 3 (out of 4), then it would considered as malicious node, and if suspicious value is 2 (out 4), then it would be considered as suspicious node. Thereafter the monitor node shares the malicious node list and suspicious node list with all the

nodes in its region. Using this data the sensor nodes removes malicious nodes from its neighbor list and renovates its neighbor list. Suspicious nodes are not removed from neighbor list, but suspicious node's route replies are not considered by its neighbor node which helps to prevent fake route replies from suspicious nodes.

The sinkhole nodes can tamper the data packet. As mention earlier, we applied authentication technique which is used in SeRWA [21], each sensor node validates the collected data packet integrity by using Message Authentication Code (MAC). If authentication fails, sinkhole node tampered data packet and the collected data packet should be dropped. Then the receiver node forwards a red alert message to the monitor node about its sender node. Let the sender node be M and receiver node be N. If the node N receives tampered packet from node M, then node N sends red alert message to the monitor node about node M. The monitor node forwards red alert message about node M to the all nodes in its region. The node which receives red alert message will remove the red alert node [(i-e) node M] from its neighbor list and rebuild its neighbor list by triggering neighbor discovery process.

4.5 Cost Analysis

Sensor node runs the listener table construction algorithm (Algorithm I). Execution of algorithm I happen in the following two scenarios: a) when sensor node forwards data/ACK/control packet to its neighbor b) when sensor receives data/ACK/control packet from its neighbor. For example when a sensor node detects an event in the environment, it needs to send the data to the base station, so it triggers route request by sending RREQ packet. Once the optimal route to the base station is found the sensor node starts forwarding the data packet, in-turn the base station sends back ACK to the sensor node (in reverse direction) for the received data packets. Since the number of data/ACK/control packets sent/received are based on number of occurrence of the event that are uncertain in the environment, time complexity of algorithm I is O(1).

Monitor node runs the monitor table construction algorithm (Algorithm II). Algorithm II contains two looping statements (Line 12-13), first loop (Line 12) depends on the number of sensor node under its region [(i-e) M] and the second loop (Line 13) depends on the average number of entries in the listener table (listener table size) of the sensor nodes [(i-e) N]. So algorithm II depends on two factors namely number of sensor node under its region and average number of entries (listener table size) in listener table. Suppose there are M number of sensor nodes under monitor node and N is the average number of entries in listener table then the algorithm II will be executed M*N number of time. Hence the time complexity of monitor table construction is O(M*N). For example, let us consider that each sensor node has details of 5 senor node (on an average) in its listener table [(i-e) listener table size is 5] and monitor node has 10 sensor node under its region, then monitor node updates its monitor table [5*10=50] by 50 times. The monitor node runs the malicious node detection algorithm (Algorithm III) to check the malicious node under its region. Algorithm III contains one looping statement (Line 24) and the loop depends on the number of sensor nodes under monitor node. Based on the number of sensor nodes (M number of sensors), the monitor node runs Algorithm III accordingly. Let monitor node has 10 sensor nodes under its region, monitor node runs algorithm III for 10 times to detect malicious node. Since algorithm III execution depends on number of sensors under monitor table, time complexity of malicious node detection is O(M) and the time complexity of all the three algorithms is given in **Table 1**.

Table 1. Time complexity of different algorithms

S.No	Algorithm	Time Complexity
1.	Listener Table Construction	O(1)
2.	Monitor Table Construction	O(M*N)
3.	Malicious node detection	O(M)

5. Performance Evaluation

We have used NS2.34 [24] for performance analysis. MannaSim Framework patch [25] is used with NS2 to create a sensor network environment. The simulation area covers 1000 m * 1000 m. The transmission range is 250m. The simulation parameters are given in **Table 2**. To evaluate the performance of the proposed method BRMD, simulation is carried out in network simulator 2.34 and simulation results are compared with FuGeF [12], TruFix [13] and well known routing protocol called AODV. Following are the various metrics is used for network performance analysis and from this it is shown that the network contains up to 25% of malicious node.

Table 2. Parameters used in NS2

S.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	0.036mW
7	Receive Power	0.024mW
8	Frequency	914MHz
9	Initial Energy	12 J
10	Traffic Type	CBR (Constant Bit Rate)
11	Packet Size	128 bytes
12	Number of nodes	250
13	Number of monitor nodes	10

5.1 False Positive and False Negative

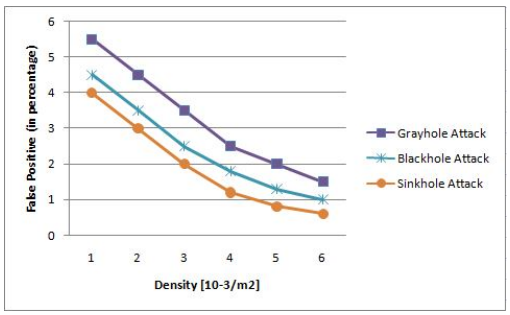

Fig. 3. False Positive Vs Density (c=1.5)

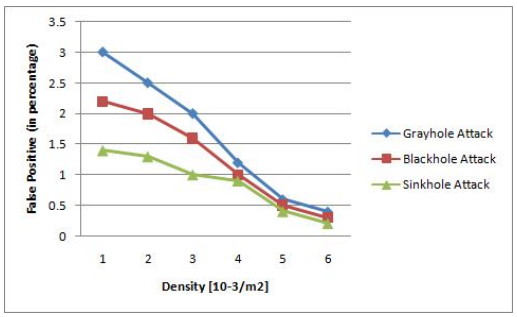

Fig. 4. False Positive Vs Density (c=2)

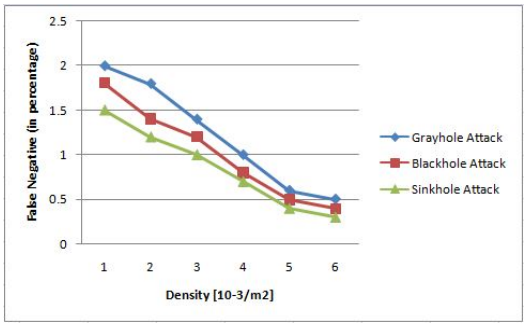

Fig. 5. False Negative Vs Density (c=1.5)

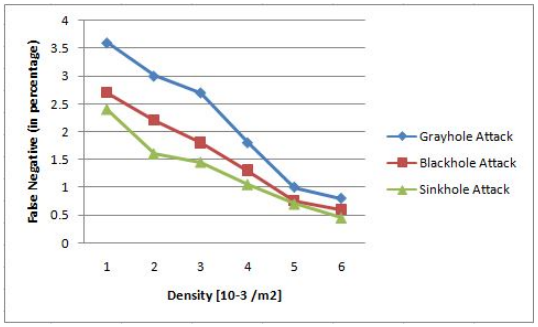

Fig. 6. False Negative Vs Density (c=2)

As we discussed in equations 1 - 3, choosing the constant plays a vital role in malicious node detection. To grasp the affinity between the threshold value and the attack detection, we have tested the proposed algorithm BRMD with fluctuating threshold in the presence of different attacks. From **Fig. 3-6**, it is understood that when the constant is high, it boots threshold value similarly when the constant is low it decreases threshold value. **Fig. 4** shows that high threshold decreases false positive. Since the packet drops by genuine node are believed as legitimate packet drops. Most of the legitimate packet drops are not considered as malicious packet drops. Also whenever threshold increases, our protocol indifferently does not sense the malicious packet drops which is utilized by malicious node since high threshold increases false negative. It helps malicious nodes to hide from detection methodology, and **Fig. 6** shows them as genuine node. It causes high false negative due to high threshold value.

On the other hand, low constant decreases the threshold value. Low threshold value increases false positive. In general, when threshold is decreased, the packet drops by genuine nodes are considered as malicious nodes. Due to this reason, the legitimate packet drops by genuine node are treated as malicious packet drops. So that the minimum threshold increases false positive shown in **Fig. 3**. Similarly the detection of packet drops increases in the minimum threshold. It produces low false negative shown in **Fig. 5** but on the other hand false positive increases. From this analysis, it's clear that threshold in one critical parameter in malicious node detection. Therefore we should select proper constant value which helps to set proper threshold value. To achieve better performance, we have assigned c=1.75, which yields better result in terms of false positive and false negative.

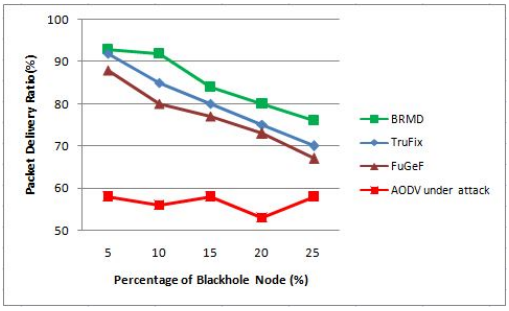

Fig. 7. PDR Vs Blackhole Attack

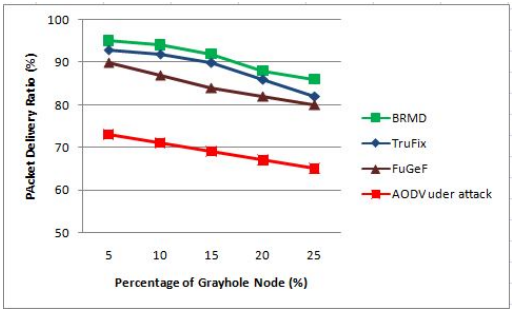

Fig. 8. PDR Vs Grayhole Attack

5.2 Packet Delivery Rate (PDR)

Packet delivery ratio is defined as the ratio of number of data packets successfully received by the destination node to the number of packets sent by the source node. The simulation results of packet delivery ratio for BRMD, FuGeF, TruFix and AODV (under attack) protocol are

shown in **Fig. 7 - 8**. From **Fig. 7 - 8** it's clear that the packet delivery ratio of BRMD is higher than other techniques. Suspicious nodes are identified by its behaviors and these kind of nodes are removed from neighbor node (if it malicious) otherwise these nodes are not allowed to trigger route replies. Hence malicious node cannot observe the network traffic by fake route reply, it helps BRMD achieve more than 75% and 85% packet delivery ratio even in 25% of blackhole node and grayhole node respectively. But TruFix obtains only 70% & 82% packet delivery rate, FuGeF obtains 68% & 80% packet delivery rate and AODV obtains below 60% & 70% packet delivery rate in midst of blackhole and grayhole attack.

5.3 Throughput

Throughput is the relationship between number of packets successfully received and simulation time. The channel bandwidth is assigned 2 Mbps (approximately) between source node and destination. **Fig. 9 - 10** shows that the throughput of BRMD is greater than the other protocols such as TruFix, FuGeF and AODV (under attack). Since BRMD stops fake route replies, malicious nodes cannot observe more number of data packets henceforth its drop ratio is decreased. It helps to increase throughput of the network even in the presence on blackhole and grayhole attack. BRMD yields high throughput such as 14kbps and 18kbps even in the presence of blackhole and grahole attack whereas Trufix, FuGeF and AODV protocols obtain only 12kbps, 10kbps, 1kbps and 17kbps, 15kbps, 2.5kbps throughput in the presence of blackhole and grayhole attacks.

5.4 End-to-End Delay

End-to-End delay is defined as the average time taken to deliver data packets from source to the destination. **Fig. 11 - 12** shows that BRMD yields less delay than the other protocols. Because in BRMD, whenever malicious nodes starts dropping the control packets, data packets (or) ACK packets, it will be removed from routing table. This helps BRMD to produce less end-to-end delay such as 15ms and 21ms in delivering data packet in existence of blackhole and grayhole attack respectively. But other protocols such as FuGeF, TruFix and AODV gives 30ms, 31ms and 48ms end-to-end delay in existence of blackhole attack. In the presence of grayhole attack FuGeF, TruFix and AODV gives 22ms, 22ms and 38 end-to-end delay in the presence of grayhole attack.

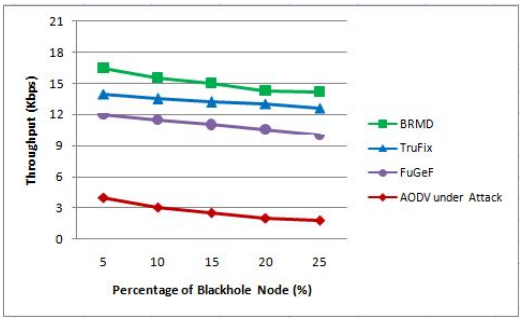

Fig. 9. Throughput Vs Blackhole Attack

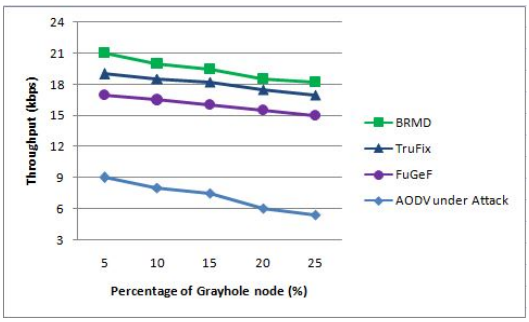

Fig. 10. Throughput Vs Grayhole Attack

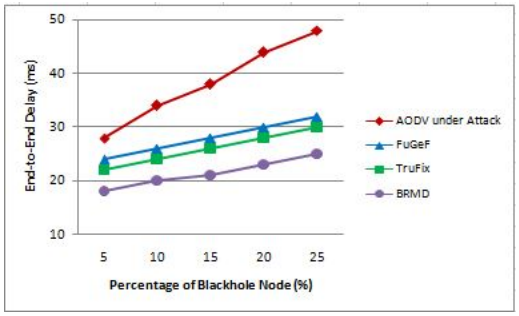

Fig. 11. End-to-End Delay Vs Blackhole Attack

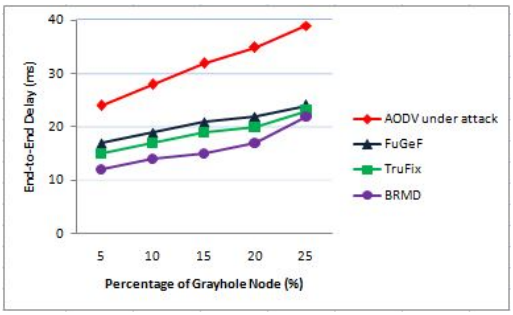

Fig. 12. End-to-End Delay Vs Grayhole Attack

6. Conclusion

In this paper, the authors studied malicious packet dropping attacks and have inspected various methodologies against packet dropping attacks. Many existing techniques suffer due to various limitations such as high computation overhead, high data overhead, false positive and false negative. The authors have proposed a behavior based routing misbehavior detection to select the secure route for data dissemination against malicious packet dropping attacks. The malicious nodes are detected by its behavior. The BRMD is compared with FuGeF, TruFix, AODV protocols and simulation results exhibit the efficiency of the proposed technique. BRMD increases the packet delivery ratio, throughput and decreases end–to-end delay in the presence of malicious node. BRMD also yields less than 6% of false positive and less than 4% of false negative in malicious node detection.

References

[1] Minho Jo, Longzhe Han, Dohoon Kim, and Hoh Peter In, "Selfish attacks and detection in cognitive radio ad-hoc networks," *IEEE network*, vol. 27, no. 3, pp. 46-50, May/June 2013. Article (CrossRefLink).

[2] Krontiris, Ioannis, Tassos Dimitriou, Thanassis Giannetsos, and Marios Mpasoukos, "Intrusion detection of sinkhole attacks in wireless sensor networks," in *Proc. of the 3rd International Workshop on Algorithmic Aspects of Wireless Sensor Networks (AlgoSensors 2007)*, pp. 150-161, July 2007. Article (CrossRefLink).

[3] Sundararajan, Ranjeeth Kumar, and Umamakeswari Arumugam, "Intrusion detection algorithm for mitigating sinkhole attack on LEACH protocol in wireless sensor network," *Journal of Sensors*, vol. 2015, pp. 1-12, Feb.2015. Article (CrossRefLink).

[4] Wazid, Mohammad, and Ashok Kumar Das, "A Secure Group-Based Blackhole Node Detection Scheme for Hierarchical Wireless Sensor Network," *Wireless Personal Communications*, vol. 94, issue 3, pp. 1165-1191, Sep. 2017. Article (CrossRefLink).

[5] Dong Xie, HaiPeng Peng, Lixiang Li, and Yixian Yang, "Efficient post-quantum secure network coding signatures in the standard model," *KSII Transactions on Internet and Information Systems (TIIS)* vol. 10, no. 5, pp. 2427-2445, May 2016. Article (CrossRefLink).

[6] Dong Xie, Haipeng Peng, Lixiang Li, and Yixian Yang, "An efficient privacy-preserving scheme for secure network coding based on compressed sensing," *AEU-International Journal of Electronics and Communications*, vol. 79, pp. 33-42, Sep. 2017. Article (CrossRefLink).

[7] Anwar, Raja Waseem, Majid Bakhtiari, Anazida Zainal, and Kashif Naseer 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. Article (CrossRefLink).

[8] Dhaka, Arvind, Amita Nandal, and Raghuveer S. Dhaka, "Gray and Blackhole Attack Identification using Control Packets in MANETs," *Procedia Computer Science* 54 pp. 83-91, August, 2015. Article (CrossRefLink).
[9] Perkins, Charles, Elizabeth Belding-Royer, and Samir Das, "Ad hoc on-demand distance vector (AODV) routing," *No.RFC* 3561, 2003. Article (CrossRefLink).
[10] Shafiei, Hosein, Ahmad 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. Article (CrossRefLink).
[11] Ju Ren, Yaoxue Zhang, Kuan Zhang, Xuemin Shen., "Adaptive and Channel-Aware Detection of Selective Forwarding Attacks in Wireless Sensor networks," *IEEE Transactions on Wireless Communications*, vol. 15, no. 5, pp. 3718-3731, May 2016. Article (CrossRefLink).
[12] Umar, Idris Abubakar, Zurina Mohd Hanapi, Aduwati Sali, and Zuriati A. Zulkarnain, "FuGeF: a resource bound secure forwarding protocol for wireless sensor networks," *Sensors*, no. 16(6), pp. 943, 2016. Article (CrossRefLink).
[13] Umar, Idris Abubakar, Zurina Mohd Hanapi, Aduwati Sali, and Zuriati A. Zulkarnain, "Trufix: A configurable trust-based cross-layer protocol for wireless sensor networks," *IEEE Access*, vol. 5, pp. 2550-2562, 2017. Article (CrossRefLink).
[14] Marti, Sergio, Thomas J. Giuli, Kevin Lai, and Mary Baker, "Mitigating routing misbehavior in mobile ad hoc networks" in *Proc. of the 6th annual international conference on Mobile computing and networking*, pp. 255-265. ACM, 2000. Article (CrossRefLink).
[15] Karuppiah, A. Babu, and S. Rajaram, "False Misbehavior Elimination of Packet Dropping Attackers during Military Surveillance using WSN," *Advances in Military Technology*, vol. 9, no.1, pp. 19-30 June 2014.
[16] Kumar, Vimal, and Rakesh Kumar, "An Adaptive Approach for Detection of Blackhole Attack in Mobile Ad hoc Network " *Procedia Computer Science*, vol. 48, pp.472-479, 2015. Article (CrossRefLink).
[17] Altisen, Karine, Stéphane Devismes, Raphaël Jamet, and Pascal Lafourcade, "SR3: secure resilient reputation-based routing," *Wireless Networks*, vol. 23, no. 7, pp. 2111-2133, 2017. Article (CrossRefLink).
[18] Balakrishnan, Kashyap, Jing Deng, and V. K. Varshne., "TWOACK: Preventing Selfishness in Mobile Ad Hoc Networks," in *Proc. of Wireless communications and networking conference*, pp. 2137-2142, April, 2005. Article (CrossRefLink).
[19] Liu, Kejun, Jing Deng, Pramod K. Varshney, and Kashyap Balakrishnan, "An acknowledgment-based approach for the detection of routing misbehaviour in MANETs," *IEEE transactions on mobile computing*, vol. 6, no. 5, pp. 536–550, May, 2007. Article (CrossRefLink).
[20] Shakshuki, Elhadi M., Nan Kang, and Tarek R. Sheltami, "EAACK – A secure Intrusion Detection System for MANETs," *IEEE Transactions on Industrial Electronics*, Vol. 60, Issue 3, pp. 1089-1098 March 2013. Article (CrossRefLink).
[21] Madria, Sanjay, and Jian Yin, "SeRWA: A secure routing protocol against wormhole attacks in sensor networks," *Ad Hoc Networks*, vol. 7, no. 6, pp. 1051-1063, 2009. Article (CrossRefLink).
[22] Banković, Z., Juan Carlos Vallejo, David Fraga, and José Manuel Moya, "Detecting bad-mouthing attacks on reputation systems using self-organizing maps," *Computational Intelligence in Security for Information Systems*, pp. 9-16. Springer, Berlin, Heidelberg, 2011. Article (CrossRefLink).
[23] Chang, Jian-Ming, Po-Chun Tsou, Isaac Woungang, Han-Chieh Chao, and Chin-Feng Lai, "Defending Against Collaborative Attacks by Malicious Nodes in MANETs: A Cooperative Bait Detection Approach" *IEEE Systems Journal*, vol. 9, no. 1, pp. 65-75, 2015. Article (CrossRefLink).
[24] NS2 web site, http://www.isi.edu/nsnam/ns/
[25] http://www.mannasim.dcc.ufmg.br/index.htm

J. Sebastian Terence 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 interest includes Internet of Things (IoT), sensor networks, MANET, networks and algorithms.

Geethanjali Purushothaman 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 2014-15. Her research interests include bio-signal and image processing, sensor network, pattern recognition, development of assistive devices, biomechanics and applications of renewable energy in assistive device.