Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

MRWDP: MULTIPOINT RELAYS BASED WATCH DOG MONITORING AND PREVENTION FOR BLACKHOLE ATTACK IN MOBILE ADHOC NETWORKs

OPINDER SINGH[†], DR. JATINDER SINGH[‡], AND DR. RAVINDER SINGH[‡]

[†]Research Scholar, IKG PTU, Kapurthala, Punjab, India. E-Mail: opindermca2008@gmail.com
[‡]IKG PTU, Kapurthala, Punjab, India. E-Mail:bal_jatinder@rediffmail.com

ABSTRACT

Mobile Adhoc Networks (MANETs) do not include any fundamental power and also infrastructure less networks, so unprotected against black hole attacks. It decreases the network performance by dropping the number of messages. Black hole node always attracts the concentration of source nodes by guarantee them that it has the minimum cost path towards destination nodes. Many techniques have been proposed so far, in order to reduce the impact of the black hole attack by detecting and preventing it. Among the existing techniques, Watchdog (WD) technique has shown better performance in preventing the black hole attack. It utilizes the local knowledge of the next hop node and eavesdrops it. If it gets that spending time of the message is more than the given threshold, then it characterize that node as black hole attacker. But this method has several shortcomings that it does not track the link transmission errors, which may be because of congestion in MANETs and also it not offers high mobility for maximum number of nodes, which eventually decreases the performance. In order to handle this issue, a new multipoint relays (MPRs) based WD monitoring and prevention technique is proposed in this paper. The multipoint relays based WD monitoring and prevention technique utilizes the dynamic threshold value to detect the black hole attacker node by utilizing Clustering, WD and MRPs based optimistic path for communicating the messages. Experimental results clearly indicates the effectiveness of the proposed technique over others. Thus, it reduces the overall message dropping, which improves the performance of the MANETs.

Keywords: *Black hole, MANETs, WD, Multipoint relays.*

1. INTRODUCTION

MANETs can be defined as a network which is free from infrastructure for its operations. In MANETs number of mobile nodes are interconnected by using wireless links. [1]. Different nodes that lie within the range of other nodes can send or receive data from each other. If two nodes in MANETs are not within the range of each other and there is the need to send data messages from one node to another, then multi-hop communication is used with the help of intermediate nodes [2]. In MANETs nodes are free to move in the network. As nodes are free to move randomly in the MANETs so there exists no fixed topology for this type of network. This gives rise to the change in communication information [3]. Due to the dynamic nature of this network, there is no any central network administration.

MANETs are more prone to malicious attacks because of various vulnerabilities, i.e. Lack of centralized node, scalability, dynamic topology, limited power supply, no predefined boundary, limited resources, bandwidth constraint, etc. These issues may alter the battlefield conditions for Adhoc network against various security threats [4]. The necessity for more effective security mechanisms for MANETs is increasing due to its dynamic nature and continue growth in various fields. MANETs are organized in the unfavorable environments. Different nodes in the MANETs

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

have an unreliable communication medium which makes it tough to deploy security mechanism [5]. Therefore, security of different nodes in MANETs is a great challenge against various attacks. A variety of attacks are possible in MANETs including jamming, collision, black hole, flooding, wormhole, sinkhole, selective message drop, Sybil, cloning, denial-of-service, tampering etc. The Black hole attack is the most hazardous attack on MANETs [6].

In Black hole attack, a malicious node drops all of the data messages received from source node without transferring to the target node [7]. In this attack, malicious node introduces itself as a node having the smallest route to the destination node. Black hole attack in MANETs is performed by an internal malicious node which fits in the routes from the source node to destination node [8]. As soon as this malicious node gets route request from the source node, it introduces itself as a node having the shortest path to the destination by showing the minimum hop sum No. and maximum sequence No.. By performing this, the malicious node gets the chance to make it an active data route element [9]. After this malicious node capable of introducing black hole attack in MANETs by dropping all of the data messages received from the source node [10].

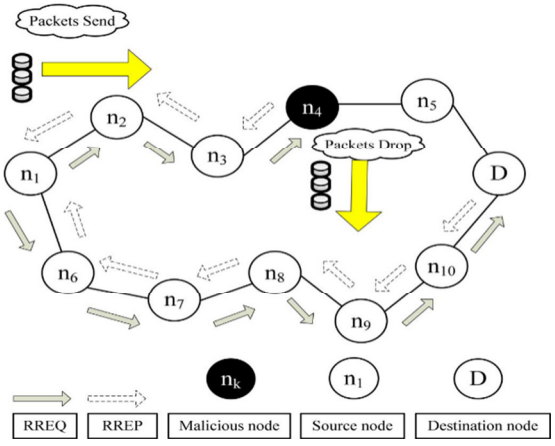

Figure 1: Black hole attack in MANETs

In the figure 1, Adhoc network is shown with malicious node n4 which is performing black hole attack. In this, n1 and D nodes are source and destination nodes respectively. When n1 send RREQ for sending data messages to the destination node D. A Malicious node n4 send immediate reply without looking into the communication table, claiming the shortest route to the destination node D. When source node n1 receive RREP from n4 node through n3, n2 nodes, it assumes this route as the best path to a destination and start transferring data messages through it. On the way to destination malicious node n4 starts dropping all of the data messages which are transferred by node n1.

2. RELATED WORKS

Subsequent section contains comprehensive study of various techniques especially designed to detect the black hole attack. The overall objective is to evaluate the shortcomings of these techniques.

Marchang and Datta [1] has proposed a light aggregation trust based secured communication technique. The black hole monitoring technique is used for evaluating the trust among nodes, demand minimum resources and also utilized local knowledge, therefore it is easily scalable. However, it has a poor attack monitoring rate because it does not consider the previous knowledge while evaluating the trust values. Orallo et al. [2] have utilized the WDs in order to monitor malicious nodes which have reduced the monitoring time and enhanced the performance of the MANETs. Dias et al. [3] have proved that the cooperative WD technique can trace and act against malicious nodes, in order to improve the network performance. The Cooperative WD technique depends upon the mutual exchange of nodes reputation in the network. However, it has not considered the local information of nodes, therefore, unable to detect those malicious nodes which have started dropping the messages in currently.

Orallo et al. [4] proved that the recognition procedure done by WD technique may produce false positives as well as false negatives which may bring to erroneous functions. Also, depending upon the local WDs alone may produce poor results when monitoring malicious nodes, in term of speed as well as precision. In order to improve the speed

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

of the malicious node monitoring, a new technique is proposed. The new technique utilized the collective communication based WD as a collaborative technique based upon diffusion of local malicious nodes, therefore information about malicious nodes can be computed rapidly. Kim et al. [5] have proposed a novel black hole monitoring technique, also known as the algebraic WD. It allows nodes to monitor selfish behaviors probabilistically and also utilized overheard messages to regulate their Neighbors (NBR) locally. In this technique senders play an active role in the inspection of the node downstream. Baadache and Belmehdi [6] demonstrated a novel approach to detect the black hole attack by using an authentic end-to-end acceptance based technique to evaluate the exact transmission of data messages by transit nodes. However, it has not considered the local information of nodes, therefore, unable to detect those malicious nodes which have started dropping the messages in currently.

Yang et al. [7] discussed an Anti-Blackhole Mechanism in order to detect the malicious behavior of nodes. This technique utilizes black hole monitoring nodes to detect the black hole attacker nodes. These nodes stay in sniff mode in order to monitor the mistrustful value of a node depends upon the anomalous disparity among the communication messages transferred from the node. When a mistrustful value goes beyond a threshold, black hole monitoring node(s) will transmit a block message, informing other nodes to cooperatively isolate the black hole node. Poongodi and Karthikeyan [8] have proposed a method called Localized Secure Architecture for MANETs. This method utilized security monitoring nodes which will be activated if threshold value exceeded from the predefined value. If black hole nodes are monitored, then security monitoring nodes inform other nodes about the selfish node.

Banerjee et al. [9] propose an AODV based black hole attack mitigation technique in MANETs without modifying the message format of AODV and without introducing any black hole monitoring messages. Dasgupta et al. [10] provide a colored petri net model for monitoring and prevention of black hole attack in Adhoc network. This model modifies a No. of properties and provides better results as simulated through a CPN tool. Kurosawa et al. [11] in their work provide a dynamic learning based technique for detecting black hole attack in MANETs. This technique is based on using dynamically updated training data for the isolating malicious node. Jain et al. [12] make use of AODV's sequence No. for mitigation of black hole attack in MANETs without modifying the message format of AODV. All the monitoring and prevention are performed by an originating node without relying on other nodes in the network. Yong et al. [13] makes use of neighbor set based along with the communication recovery technique for mitigating black hole attack in MANETs. Simulation results show that this technique reduced the overhead of the network. Li et al. [14] in their work present a trust based on demand multipath communication for isolating black hole attack. A node's trust is based upon its message forwarding ratio. In this method, a source node creates numerous reliable paths to a destination in solitary path discovery.

Namdeo et al. [15] provide an enhanced WD based solution for protecting MANETs against black hole attack. In this, malicious node is detected on the basis of message flooding and dropping parameters. Cai et al. [16] proposed a distributed black hole monitoring system for adversarial MANETs. This mechanism is used for preventing the networks from numerous forms of black hole attack. Message delivery ratio is enhanced by using this distributed approach. Imran et al. [17] provide monitoring and prevention technique for isolating black hole attack in MANETs. In this technique, DPS nodes are deployed in MANETs that uninterruptedly monitors the performance of their neighbor nodes. These DPS notice the RREQs broadcasted by its neighbor nodes. After checking the No. of parameters of its neighbor nodes, DPS node declares that suspicious node as the black hole node and then broadcast threat message on the network. Chatterjee et al. [18] in their work present a technique for isolating black hole attack in MANETs by using node stability system. This proposed mechanism can

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

successfully identify and isolate singular and co-operative black hole nodes from the network. Ghathwan et al. [19] introduce an artificial intelligence based technique for preventing from the cooperative black hole attack in MANETs. This is an integrated approach based on both A* and Floyd-Warshall's procedures. This mechanism works on the basis of finding a shortest secure path for AODV (SSP-AODV).

Babu et al. [20] discussed a novel honeypot based monitoring and isolation approach for preventing from black hole attack in MANETs. This proposed approach reduces the overhead, message drop ratio and the communication load of the network. Kamatchi et al. [21] introduce a new mechanism based on secret sharing and random multipath communication for preventing from black hole attack in MANETs. This message reduces the message delay and message drop ratio in the network. Mohammed et al. [22] proposed a leader election based black hole monitoring system for mitigating black hole attack in MANETs. For an optical leader election VCG model, Cluster dependent and cluster independent concepts are used. Ritchie et al. [23] have demonstrated a COB communication model by using complexity polynomial for preventing against black hole attack in MANETs. Performance of this technique is much better when compared with Dynamic Source Communication. Chang et al. [24] proposed a Cooperative bait monitoring scheme for protecting MANETs from collective attacks. This scheme works on the basis of reverse tracing approach for modifying the performance of the network. Djenouri et al. [25] have utilized Bayesian and social based techniques for mitigating malicious attacker nodes in MANETs. This approach works on the basis of judgement to isolate the guilty nodes from the network. Kaushik et al. [26] provide a solution for preventing the network from both Black hole and cooperative black hole attacks. The drawback of modified AODV is increased overhead.

Gong et al. [27] in their work presented a cooperative immune system for prevention of MANETs against collective attacks. The concept of probability is used for analyzing and detecting attacks. Ying et al. [28] discussed the threshold based black hole monitoring system for selective black hole attack in MANETs. In this mechanism IDS nodes are set to sniff mode for estimating the suspicious value of nodes. Arathy et al. [29] provide the Collaborative Black Hole procedure for detecting single and collective attacks in MANETs. The proposed D-MBH and D-CBH mechanisms are used for generating list of single, multiple and collective black hole attacker nodes. This approach reduces the computational overhead. Babu et al. [30] make use of an alleviation procedure for handling black hole attacker nodes in MANETs. The proposed approach is responsible for improved quality of service and cost effectiveness. Casado et al. [31] provide a light aggregation monitoring model for isolating malicious nodes in MANETs. In this model, firstly various message discard conditions of malicious attack are modelled then, for analyzing these conditions, an enhanced windowing procedure is used.

Jalil et al. [32] provide an enhanced route discovery AODV for mitigating black hole attack in MANETs without including any control messages. Shi et al. [33] proposed a cluster based approach for preventing MANETs from black hole attacker node. Cluster heads (CHs) are nominated by using analytic hierarchy methodology. Batham et al. [34] introduce a new trust based mechanism by using Dempster-Shafer Theory. In this approach communication is only limited between trusted nodes. Olmos et al. [35] provides a novel collective WD mechanism for detecting malicious nodes in the Adhoc networks. This approach reduces the false negative and improves speed of monitoring. Arunmozhi et al. [36] introduce a defense mechanism for detecting attacker node in the MANETs. This technique is based on time of route reply by different nodes in the network, which is then compared with the threshold value. Vasudevan et al. [37] in their work present a certification based authentication technique for mitigating black hole attack problem in MANETs. Multicast AODV technique is used for this authentication mechanism.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

But the review has shown that [1] - [37] have not focused on finding the link transmission errors. The link transmission errors may occur in the MANETs because of the packets flooding and due to maximum No. of nodes. Therefore existing techniques have certain shortcomings, which eventually decreases the MANETs performance. In order to handle this issue, a new multipoint relay based WD monitoring and prevention technique is proposed in this paper. The MRWDP utilizes the dynamic threshold value to detect the black hole attacker node, and then clustering and WD based optimistic path is selected for communicating the messages. Thus, it will reduce the overall message dropping, which will improve the performance of the MANETs. This paper is organized as: In section 3, the proposed black hole monitoring technique is discussed. In section 4, black hole attack detection for different NLs (Network Layers) is discussed. The Simulation results of MRWDP using the NS-2 simulator are discussed in section 5. The comparisons of the MRWDP with available state of the art techniques are provided in section 6. In the last section conclusion and future directions are also demonstrated.

3. PROBLEM STATEMENT

From the designed systems, the actual MANET AODV standard technique is adopted [5]. The clustering based process is utilized in accordance with the good service quality, in which every single node elect by itself along with the nodes in their transmission range. On deciding upon cluster head, it is responsible to monitor the number of multipoint relays (MPRs). It determines the actual value of Quality of Service (ÙÒŠ) for every ìth node by the following,

$$ÙÒŠ(ì) = sc(ì) \times o(ì) \times \frac{1}{\bar{v}(ì)} \quad \text{..... (1)}$$

Where $sc(ì)$ is actually the remainder of the mileage to get out of this path, $o(ì)$represnts the 1-hop neighbor nodes in the similar route as well as $\bar{v}(ì)$ is the typical quickness from the ìth node.

In comparison to [5] it is considered that the nodes in the network use the available path information for electing Cluster Heads (CHs). As soon as the attached CHs usually are determined, exactly same solution is utilized in [5] to find the MPRs. The black hole lowers the throughput of various well-known routing techniques. It basically utilize MPR nodes, creating a considerable effect on multi-level connectivity. For example, it is assumed that about 10% from the MPRs being malicious. Since we are utilizing clustering therefore every node can communicate with other by utilizing nearest CHs. Nevertheless, when black hole attacks are available; the maximum amount of CHs loses their connectivity with other CHs as well as nodes. Therefore increase in black hole attacker nodes degrades the connectivity of MANETs a lot [17]. Thus black hole attack detection and removal techniques are required to improve the performance of the MANETs. WD based black hole detection technique is found to be an efficient technique in the existing literature, but WD based attack detection suffers from some major issues. 1. A large number of false positive rates may occur in dense MANETs, 2. Due to very high interference and noise level in Adhoc networks, wrong threshold values are produced which results in false judgements. 3. If randomly wrong signature keys are assigned, it will result in the false evaluation. 4. The link transmission error and collision problems are big issues in MANETs.

To handle these issues, an improved cooperative CL (Cross Layer) detection technique is designed, in which WD evaluators are associated with MAC and physical layers techniques. Several constraints used from numerous layers are assembled to decide whether black hole attack happened or not. Thus proposed technique has better detection rate than standard WD. Therefore, it reduces the overall message dropping, which improves the performance of the MANETs.

In order to detect the black hole attacks in MANETs, WD method is enhanced in such a way that it can handle the collision issue. The standard WD method has not ability to distinguish among black hole attacks and collisions. To handle this issue CL is utilized, in which several evaluator nodes from several layers are collaborated to improve the malicious nodes detection rate. In proposed approach, the WDs are chosen on the bases of normal distribution with mean 0 and variance 1.

4. COOPERATIVE CROSS LAYER DESIGN

In MANETs nodes are adhoc in nature, therefore it become difficult to detect the attackers available in the network. Many existing techniques do not outperforms in MANETs, because nodes keeps changing their positions. The primary focus of CL based technique is to control the knowledge among layers, therefore, improve attack detection rate. Subsequent section discusses various detection

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

algorithms for physical and NL (Network Layer). In particular, Figure 2 shows knowledge swap among (A) physical and NL, (B) MAC and NL, (C) three layers.

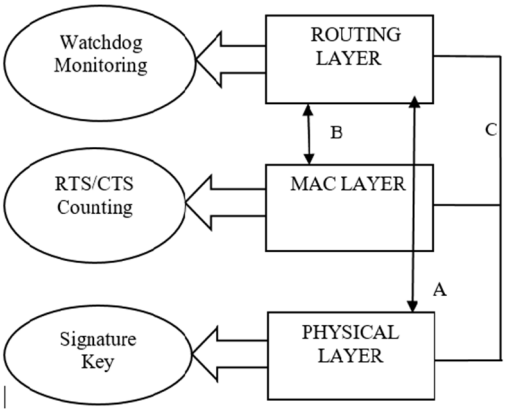

Figure 2: Various Levels of Monitoring

4.1. Physical Layer Black Hole Monitoring

This section describes the physical layer based black hole detection algorithm. This technique is the first defence layer of the proposed technique. In this strategy WD observes the receiver node to decide regarding to forward or discard the signal. Consider a mobile ad hoc network consists of m legitimate nodes. In this network, for each node we assign a unique signature key denoted by $\acute{S}_a$, where a=1, 2, 3… m represents the different nodes. If z_a represents the signal message sent by the a^{th} user in the MANET, then interrupted received signal k_a have two feasible hypotheses represented as

$$k_a = \begin{Bmatrix} z_a + o, Hp \\ \acute{S}_a z_a + o, H1 \end{Bmatrix}, \ldots\ldots\ldots\ldots\ldots (2)$$

In Eq. 2, $o \sim \acute{C}\acute{N}(0\beta^2)$ represents the complex additive white Gaussian noise vector (AWGN) having average = 0 and variance $=\frac{\beta^2}{2}$. The possibility of received signal that is sent from an intruder is represented by null hypothesis, Hp and the received signal is sent from genuine user which carry a signature key $\acute{S}_a$, is represented by alternative hypothesis, H1 . Considering these issues, probabilities (tu) of obtained signal conditioned on every hypothesis is rewritten by using following equations.

$$tu(k_a \mid Hp) = \frac{1}{\sqrt{2\pi\left(\frac{\beta^2}{2}\right)}} \exp\left(-\frac{(ka-za)^2}{2\left(\frac{\beta^2}{2}\right)}\right), \ldots\ldots\ldots\ldots$$

(3)

$$tu\left(k_a \mid H1\right) = \frac{1}{\sqrt{2\pi\left(\frac{\beta^2}{2}\right)}} \exp\left(-\frac{(ka-\acute{S}_a za)^2}{2\left(\frac{\beta^2}{2}\right)}\right), \ldots\ldots\ldots\ldots$$

(4)

Accordingly, by employing highest log likelihood experiment, detector recognizes a obtained data as genuine when $tu(k_a \mid, H1) > tu(k_a \mid Hp)$, i.e. when

$$\wedge(k_a) \triangleq \frac{tu(k_a \mid H1)}{tu(k_a \mid Hp)} \gtrless_{Hp}^{H1} 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (5)$$

By applying the log theorems and mathematical formulas, then get

$$2k_a z_a(1 - \acute{S}_a) + z_a^2(\acute{S}_a^2 - 1) \ldots\ldots\ldots (6)$$

Which results in the following decision threshold

$$k_a \gtrless \frac{z_a(\acute{S}_{a+1})}{2} \ldots\ldots\ldots\ldots\ldots\ldots (7)$$

Every WD supervising nodes eavesdrop and ensure signal communication happening in communication range, where the signature keys $\{\acute{S}_a\}_{a=1}^{m}$ are saved in respective buffers. If obtained data was supposed to be sent from an intruder, then, a message is dropped by WD. If the user is legitimate, then physical layer passed the obtained data to MAC and NLs for further detection. In real scenario, miss-detection actions can be tolerable than false alarm actions. The proposed detection scheme is worked in this direction as , if received signal sent by intruder is not identified by physical layer detector, then it will go through other checking procedures and if an intended user wrongly identified as an intrusion, then it is dropped. For that reason, it is needed to distinguish between the probabilities of miss detection and false alarm of proposed detector, so the system can make informed choices based on some predefined false-alarm or miss-detection probability including choices of $\acute{S}_a$.The probability to identify an intruder as genuine i.e. false alarm can be calculated as

$$t_{€Å}^{(a)} = tu\left\{H_1 \mid H_p\right\} = tu\{k_a > \frac{z_a(\acute{S}_{a+1})}{2} \mid H_p\}. (8)$$

$$t_{€Å} = \int_{\frac{z_a(\acute{S}_{a+1})}{2}}^{\infty} \frac{1}{\sqrt{2\pi\left(\frac{\beta^2}{2}\right)}} \exp\left(-\frac{(k-za)^2}{2\left(\frac{\beta^2}{2}\right)}\right) ck \ldots\ldots (9)$$

Where after some mathematical manipulations, it is arrive at

$$t_{€Å}^{(a)} = \acute{Q}(z_a \frac{\acute{S}_{a-1}}{\sqrt{2\frac{\beta^2}{2}}}) \ldots\ldots\ldots\ldots (10)$$

In Eq. 10 $\acute{Q}(.)$is the standard $\acute{Q}$-function, defined as $\acute{Q}(z) = \frac{1}{\sqrt{2\pi}} \int_0^{\infty} \exp\left(-\frac{z^2}{2}\right) cz$ thus, we

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

can make the design problem as choosing some $\acute{S}_a$ to satisfy a target false alarm threshold, such that

$$\acute{S}_a^{(opt)} = \frac{\sqrt{2\,\beta^2}\,Q^{-1}(t_{\text{€Å}}^{a})}{z_a} + 1 \quad \text{..... (11)}$$

As the selected threshold, it can compute the resultant possibility of monitoring, t_c, as shown

$$t_c = 1 - tu(\text{Ħ}p\text{Ħ}1) \quad \text{..... (12)}$$

$$t_c = \int_{\frac{z_a(\acute{S}_{a+1})}{2}}^{\infty} \frac{1}{\sqrt{2\alpha(\frac{\beta^2}{2})}} \exp\left(-\frac{(k-\acute{S}_a z_a)^2}{2\left(\frac{\beta^2}{2}\right)}\right) ck \quad \text{..... (13)}$$

Which results in

$$t_c^{(a)} = \acute{Q}(z_a \frac{1-\acute{S}_a^{(opt)}}{\sqrt{2\frac{\beta^2}{2}}}) \quad \text{..... (14)}$$

Note here that, an exponential deteriorating effect is created by the noise of broadcast channel on $t_c^{(a)}$. Procedure 1 describes the proposed design of physical layer detector, where we consider that those nodes which are at same broadcast range will be neighbours and all neighbours will be monitored.

Procedure 1: Physical layer monitoring procedure.
Input:
Consider k_no be the amount of destructive nodes, Ś be the threshold value resulting earlier, X be the NBR, k*X* be the amount of observing nodes, route be the route from the sender to the receiver and *P* be the established indicator and p is the received signal.
Output:
Consider PĦ be the physical layer monitoring No., monitoring_% be the monitoring rate of the physical layer level observing.
Procedure:
for a = 1 : k_no do
for I=1 : kX do
if X(k_no(a),kX(I)) = 1 then
for *l*=1 : size(path) do
if path(*l*) = k_no(I) then
if p ≤ Ś then
PĦ = PĦ + 1
}}}}}}
monitoring_% = PĦ × $\frac{1}{kX}$ ×$\frac{1}{k\_no}$.....(15)

4.2 Medium Access Layer (ML) Black Hole Monitoring

In ML, IEEE 802.11 protocol focuses on distributed coordination, which consider a collision avoidance technique, Request to Send (RTS) and Clear to Send (CTS) in order to avoid the channel interference [20]. The primary problem which decrease the throughput in MANETs, is transmission collision at MAC level. However, this problem can be handled by considering the clustering. Because the CHs are responsible for communicating the data from the nodes, to respective destinations [16].

4.3. Network layer (NL) Black Hole Monitoring

WD protocol [11] is proposed for NL, in which several nodes are elected as WDs based on normal distribution. In order to analyze the performance of MPRs and gives the guarantee that they can trace the black-hole attackers. These nodes eavesdrop the transmission among nodes placed within its respective radius by evaluating data frames sent from source node as compared to nodes that are acknowledged by respective destination. When any dissimilarity is found, then WD alarms that given path is not secured against black hole attack. In [21], mutual communication between WDs is taken place, and assessment is made based upon the mutual decisions of various WDs. In this mutual system, every WD has equal voting weight. Procedure 2 describes various steps which are used to detect black hole attack at NL.

Procedure 2 describes the procedure of cooperative watch dog monitoring strategy, wherever the quantity of real evaluation higher each time. This watch dog notices distinction between the very first packets kept included in the buffer along with the received through the source. Then outcomes are most summed up to supply this discovery fraction and this can be considered the quantity of evaluation to the complete amount of mischievous nodes.

Procedure 2: Cooperative NL monitoring procedure.
Input:
Consider k_no be the report of destructive nodes, wd be the WD observing nodes in the NL, X be the neighbours if 1 they would be NBR, real being the real monitoring for thief's to a legitimate report by utilizing Cooperative WD plan and k_no
Output:
Consider yes be aggregationed monitoring for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

every WD and monitoring_% be the monitoring rate of the network level monitoring
Procedure:
for a = 1 : size(k_no) do
for p = 1 : size (wd) do
if X(k_no(a),wd(p)) = 1 then
real =real + 1
}}
yes = yes + (true (p))
}
monitoring_% = $\frac{\text{yes}}{\text{size (k\_no)}}$..... (16)

4.4. Physical and Network Cross Layer Design

Several authenticated nodes are assigned as physical layer supervising nodes, thus will improve the attack detection rate cooperatively. Physical supervising nodes will authenticate the nodes by checking the signature key. If source node has key then it is assigned as authenticated node or otherwise as attacker node. Procedure 3 describes various steps which are utilised to detect the black hole attacker nodes.

Procedure 3: Physical and Network Cross layer monitoring procedure.
Input: consider leg_list to be the legitimate users report results from the physical layer monitoring, wd be the WD observing nodes in the NL, X be the NBR if 1 they are NBR and k_no be the report of destructive nodes.
Output: Consider real be the real monitoring for thief's to legitimate report, By utilizing CL layering plan
Consider monitoring_% be the monitoring rate of the physical and network level observing.
Procedure:
for a = 1 : size(leg_list) do
for p = 1 : size (wd) do
if (X(leg_list(a),wd(p)) = 1) && (leg_list(a) is member of k_no list) then
real = real + 1
}}}
aggregation = sum(wd)
monitoring_% =true × $\frac{1}{\text{aggregation}}$ × $\frac{1}{\text{size(k\_no)}}$

.....(17)

4.5. MAC and Network Cl-Layer Design

In ML, it becomes difficult to distinguish attacks and collisions. ML based attack detection utilise RTS/CTS requests in order to improve the black hole detection rate. Procedure 4 represents various steps required to detect the black hole detection rate. Initially MAC track collisions, when outcomes from NL are assigned to MAC, it become easy to distinguish among collisions and attacks, thus will improve the detection rate further.

Procedure 4: Network and MAC CL monitoring procedure.
Input: consider WR represents the watch dog diagnosed destructive nodes
Consider MAC_report be the MAC monitors reports, no_d be the new No. of monitoring after filtering, WD be the WD nodes, no_d be the No. of destructive nodes, MAC be the MAC monitor nodes, MAC_s be the MAC status of possibly 1 or 0.
Output: Consider updated_aggregation_a the aggregation with two decisions, updated_aggregation raising the amount of WD's right after eradicating methods having troubles and updated_d_% be the monitoring percentage after CL among MAC with NLs.
Procedure:
1:
for a = 1 : size(WR) do
for I = 1 : size (MAC_report) do
if MAC(I) = WR(a) then
WR(a) = 0
}}}
no_d = WR
2:
for a = 1 : size(WD) do
for q = 1 :size (MAC) do
if WD(a) and MAC(I) are NBR then
updated_aggregation_a(a) = WD(a)*MAC_s(I);
}}}
updated_aggregation= sum(updated_aggregation_a)
updated_d% = $\frac{1}{\text{updated\_aggregation}}$ × $\frac{1}{\text{no\_destructive}}$ × no_d …… (18)

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

4.6. Physical, Mac, and Multi-Level Cross Layer Detectors

In end, considering both CL techniques, it is assumed that MAC supervising technique at physical level, can improve the performance further. For example, collisions which are detected throughout the WD detection and physical detection and may lead to false alarms by considering the MAC supervising. If collisions are found at supervised nodes then false detection rate can be improved by using MAC supervising. Procedure 5 describes how physical, MAC, and network monitoring procedure works.

Procedure 5: Physical, MAC, and network monitoring procedure.
Input: Consider k_no be functioning as a report on destructive nodes, updated_aggregation be the physical monitoring nodes lead coming from spanning by utilizing ML, X be the function neighbour (NBR) if 1 they are NBR, real_cl be the real monitoring for intruders from legitimate list using Cooperative WD scheme and k_no be the report of destructive nodes.
Output: Consider yes_cl be biased monitoring for every WD and monitoring_% be the monitoring rate after CL layering the three levels.
Procedure:
for a = 1 : size(k_no) do
for l = 1 : size (updated_aggregation) do
if N(k_no(a),updated_aggregation(l)) = 1 then
real_cl = real_cl + 1
}}
yes_cl = yes_cl + (real_cl(l))
}

$$\text{monitoring\_\%} = \frac{\text{yes\_cl}}{\text{size (k\_no)}} \quad \ldots\ldots\ldots\ldots\ldots (19)$$

5. EXPERIMENTAL SETUP AND RESULTS

In order to assess the efficiency and competence of proposed technique, MRWDP and other some well-known black hole monitoring techniques for MANETs are simulated by using NS-2.3. The existing and proposed black hole monitoring techniques are implemented on a Linux workstation (2.4 GHz Intel i7 processor with 4 GB RAM and 1 TB memory). The simulation is done several times, by considering 15 nodes every time. The parameters used for simulation are shown in Table 1.

Table 1: Simulation parameters

Parameter	Value
Tool used	Network simulator 2.3 and MATLAB 2013a
Simulation time	600 seconds
Dimensions in meters	800X800
Adhoc nodes	15
Protocol	AODV
Communication type	Wireless
Packet size	1024 KB
Mobility model	Two ray ground propagation model

We start the simulation by deploying the simulation of MANETs. In this Adhoc network, node 0 is the source node which is flooding route request for getting path towards destination node 7 in the network as shown in figure 2. The no. of nodes in the network will reply back with best the paths to the destination. A Source node will detect and isolate the attacker node, depending upon the various parameters as discussed in MRWDP. In this way, a secured path from source to destination will be discovered.

Figure 3, represents node 5 and node 11 are detected as malicious nodes (i.e. Black hole nodes). These nodes are detected after checking route replies from various nodes in the mobile Adhoc network against predefined parameters under MRWDP technique.

The MRWDP technique works as first of all source node 0 will send the request for the route in the network for the path to the destination node 7. Other nodes in the network will reply back to the source node with route to the destination node. After getting route reply from the various nodes, the source node will maintain a route reply table with various parameters. This technique will first check the malicious node with the help of different parameters. After getting multipoint_relay from the various nodes, the source node will prepare a multipoint_relay table in which various values for different parameters are stored. These parameters

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

are multipoint_relay time, hop_count, sequence No., the distance for the destination node. From these values stored in multipoint_relay table, dynamic threshold value against these parameters will be obtained.

Based on these dynamic threshold values first of all multipoint_relay time of all of the nodes will be checked. If it varies in large extent from average threshold value for the multipoint_relay time in the multipoint_relay table, then this node may be a malicious node. Mostly, malicious node reply immediately without checking any route to the destination node and give multipoint_relay in very short interval of time. After this Hop_sum and Sequence no. values of all of the multipoint_relay nodes will be checked. It is the property of the black hole attacker node that it always gives minimum Hop_sum value without checking any route to the destination node. It always gives minimum Hop_Sum which totally different from the Hop_Sum values replied from other nodes in the MANET. If Hop_Sum value replied by an node is very low as compare to other nodes, then this node may be a black hole attacker node.

Sequence number replied by the no. of nodes in the MANET in response to the request made by the source node represents the fresh route to the destination node. The Black hole attacker node will always try to show highest sequence number without checking other route replying nodes in the network. In a MANET, highest sequence No. of a route replying node is preferred for establishing the path from source to destination, but it should not be exceptionally high. After comparing Hop_Sum values of various nodes, next step is to check the Sequence_No. , If Sequence_No. of any node is not in the sequence of other route replying nodes, and then this node will be Black hole attacker node. Figure 4 represents that MRWDP isolates the attacker node from the network.

After this whole network is divided into different clusters (two clusters are shown in figure 6 by red and green color nodes). Clusters are used to reduce the overhead in the MANET.

Figure 5 shows the safe communication path from the source node to the destination node which is established by isolating black hole nodes. This path is established by using different CHs for the various clusters. CHs are selected based on the rating values of the nodes which are shown in figure 6. In next part of the paper, performance evaluation of MRWDP against various parameters is provided.

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

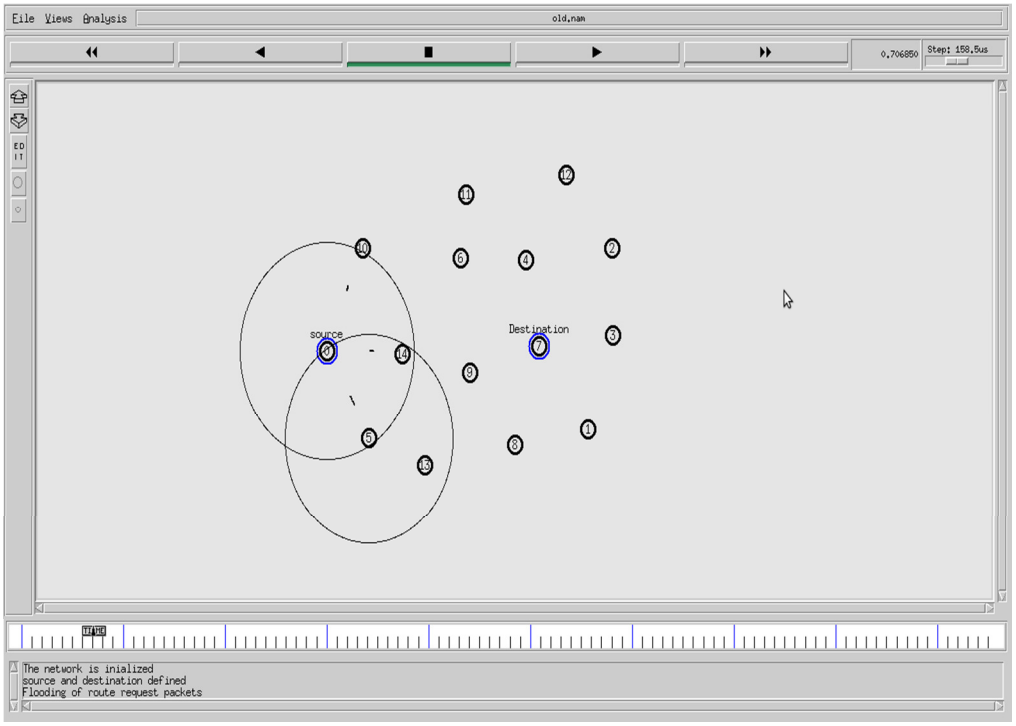

Figure 2: Route Discovery In Mobile Adhoc Network

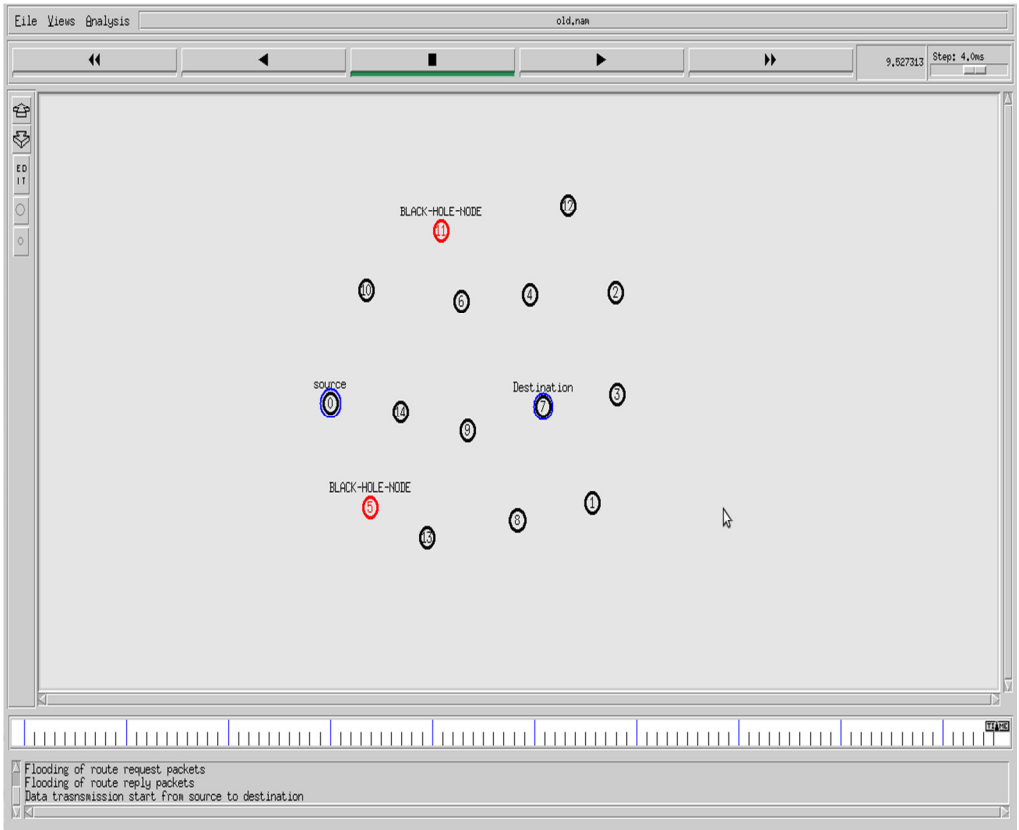

Figure 3: Monitoring Of Malicious Node (I.E. Black Hole Node)

Journal of Theoretical and Applied Information Technology
31st March 2017. Vol.95. No 6

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

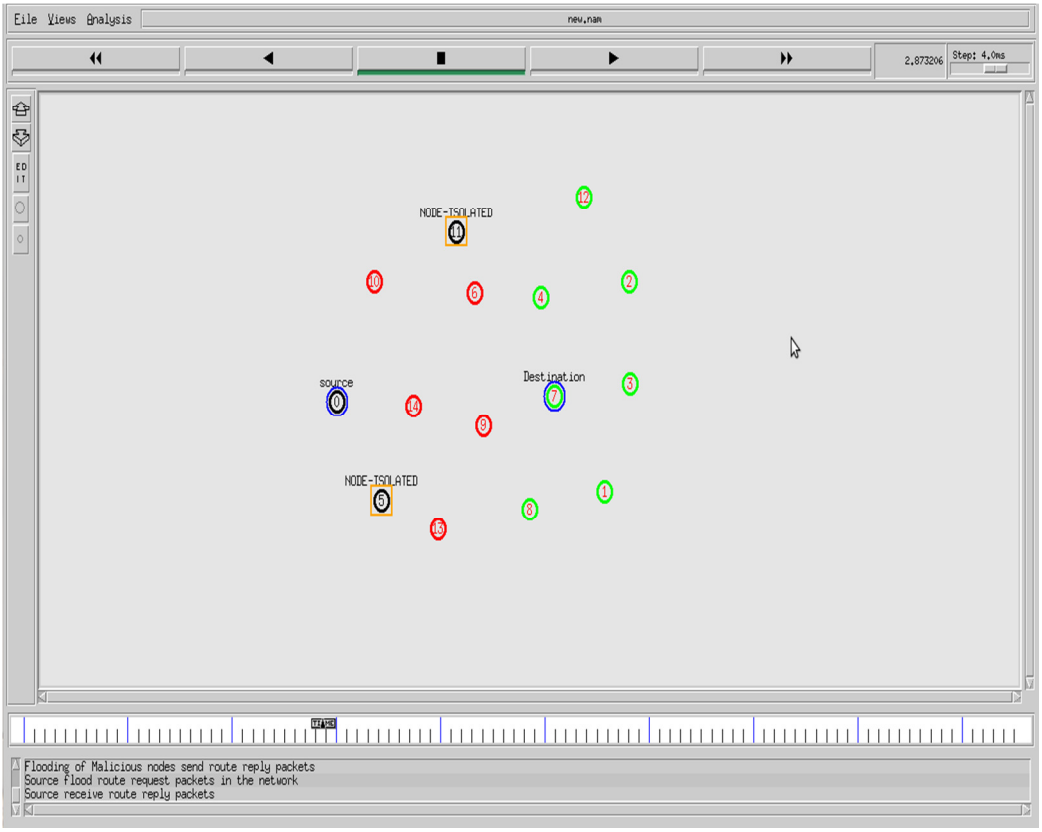

Figure 4: Isolation Of Malicious Nodes

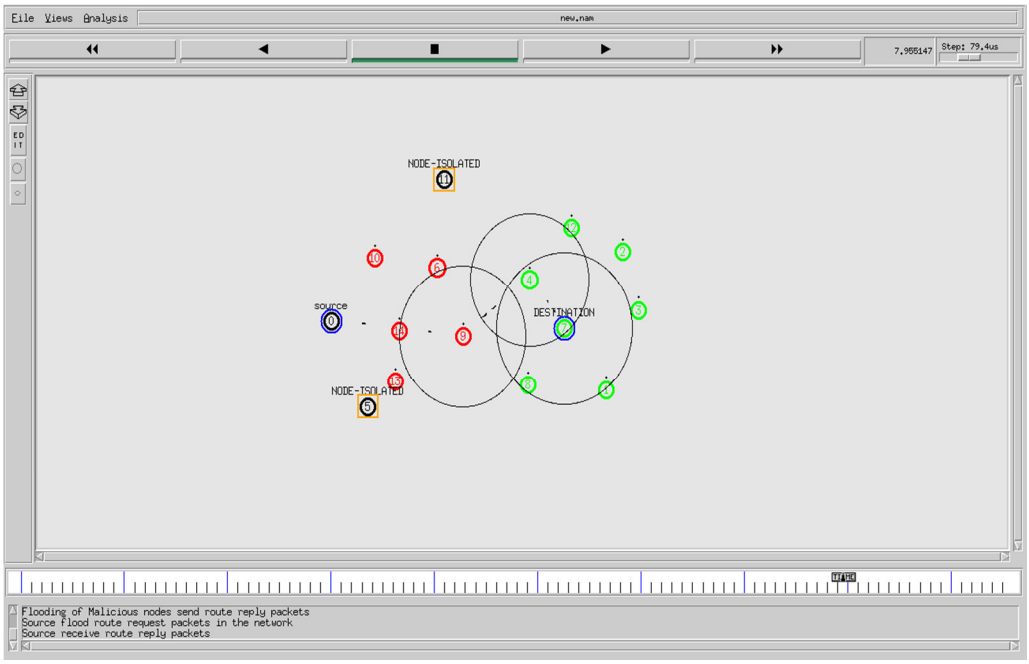

Figure 5: Secure Communication Path After Isolating Malicious Nodes

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Source	Neighbor	SX-Pos	SY-Pos	Distance	Rating
0	1	-19	383	575	7
0	2	-19	383	628	7
0	3	-19	383	608	1
0	4	-19	383	453	8
0	5	-19	383	175	2
0	6	-19	383	315	5
0	7	-19	383	451	7
0	8	-19	383	434	2
0	9	-19	383	295	2
0	10	-19	383	185	3
0	11	-19	383	382	7
0	12	-19	383	584	5
0	13	-19	383	287	10
0	14	-19	383	149	9
1	0	537	236	575	3
1	2	537	236	315	7
1	3	537	236	168	1
1	4	537	236	336	5
1	5	537	236	471	3
1	6	537	236	408	10
1	7	537	236	176	7
1	8	537	236	160	7
1	9	537	236	284	10
1	10	537	236	574	7
1	11	537	236	498	6
1	12	537	236	444	1
1	13	537	236	353	1
1	14	537	236	428	1
2	0	587	548	628	5
2	1	587	548	315	9

Figure 6: Sample Rating Of Nodes

6. PERFORMANCE ANALYSIS

This section represents the comparison between some well-known black hole attack detection techniques with the proposed technique. The throughput is taken as primary quality metric for comparison. It represents that how many packets are successfully delivered within a given time. The throughput may be increased if the attacker node is detected as early as possible. Throughput is defined as

$$\text{Throughput} = \frac{\Sigma\rho}{\Upsilon} \quad \ldots\ldots\ldots\ldots\ldots\ldots (20)$$

Where ρ=No. of messages received at the destination,

ϒ=Simulation time

Figure 7 shows the throughput analysis of MRWDP with some existing techniques. The figure clearly depicts that the MRWDP after isolation of malicious node results in the increase of throughput.

End-to-end delay is the mean time taken by a data message to travel from source node to the destination node. This average time includes any type of delay due to route discovery process along with a queue in data message transmission. In this, only those messages are included which are successfully transferred to the destination node. This is calculated as:

$$\text{Delay} = \frac{\Sigma(\lambda-\mu)}{\Sigma(\eta)} \quad \ldots\ldots\ldots\ldots\ldots\ldots (21)$$

Where

λ =Arrive Time,

μ = Send Time,

η = No. of Connections

The lesser value of the end to end delay is an indicator of the better performance of the technique. Figure 8 shows the end-to-end delay comparisons of MRWDP technique with some existing approaches for preventing MANETs from black hole attack. The figure demonstrate that the MRWDP results in the decrease in end-to-end delay.

Overhead is defined as the additional time taken to deliver messages at the destination. Overhead in the mobile Adhoc network is increased due to malicious node. The proposed approach results in decreasing the overhead of MANET as compare to existing procedures used for isolating the black hole attack as illustrated in figure 9.

Message loss is the failure of transferred messages to reach the destination. It happens due to network congestion or some attacker node in the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

network. Message loss is responsible for reducing the message delivery ratio. It is calculated as:

Message Loss= δ-ρ……. (22)

δ= No. of messages send from source

ρ= No. of messages received at the destination

Figure 10 shows the message loss comparisons of MRWDP approach with existing procedures used for preventing MANETs. The figure clearly shows that the MRWDP results in the decrease in message loss. Previously a number of watchdog based intrusion detection techniques were available, but no technique solves the link transmission error and collision problem in MANETs. For handling these issues, clustering and multipoint relay based watchdog technique is proposed. The results clearly depict the success of the proposed technique and all research objectives are met.

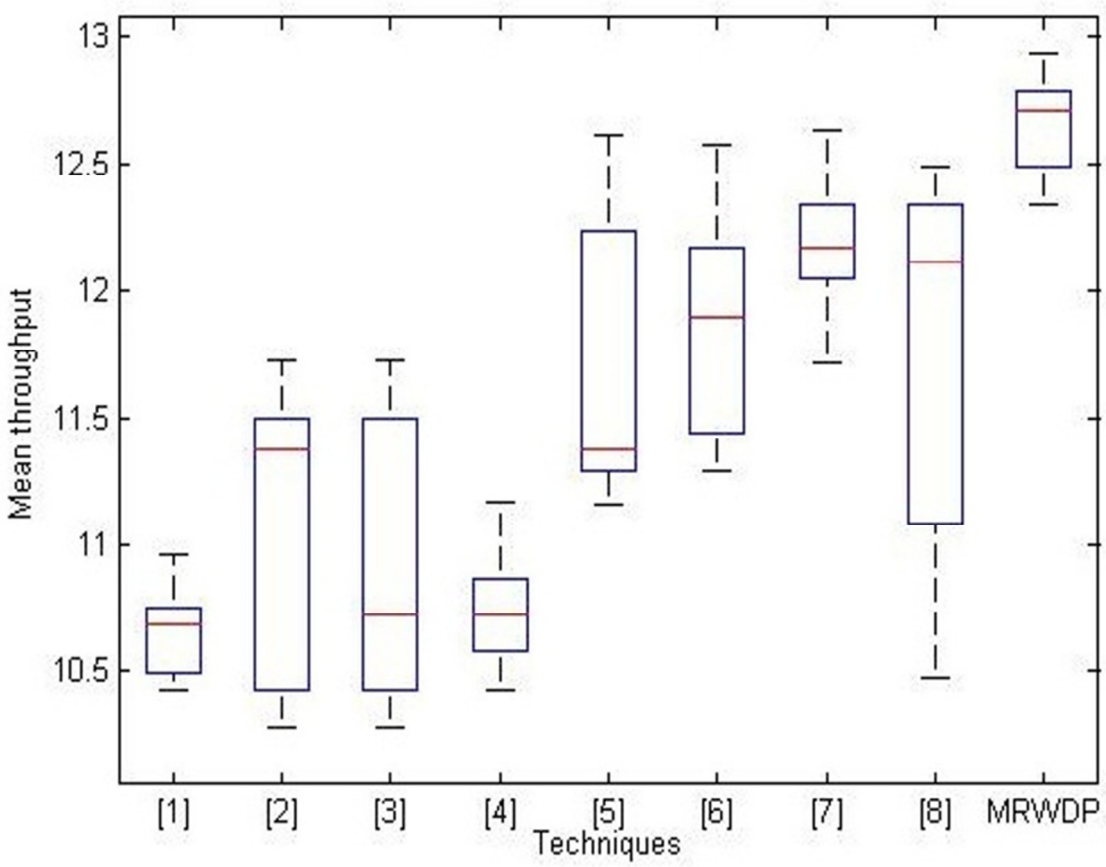

Figure 7: Throughput Comparison

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

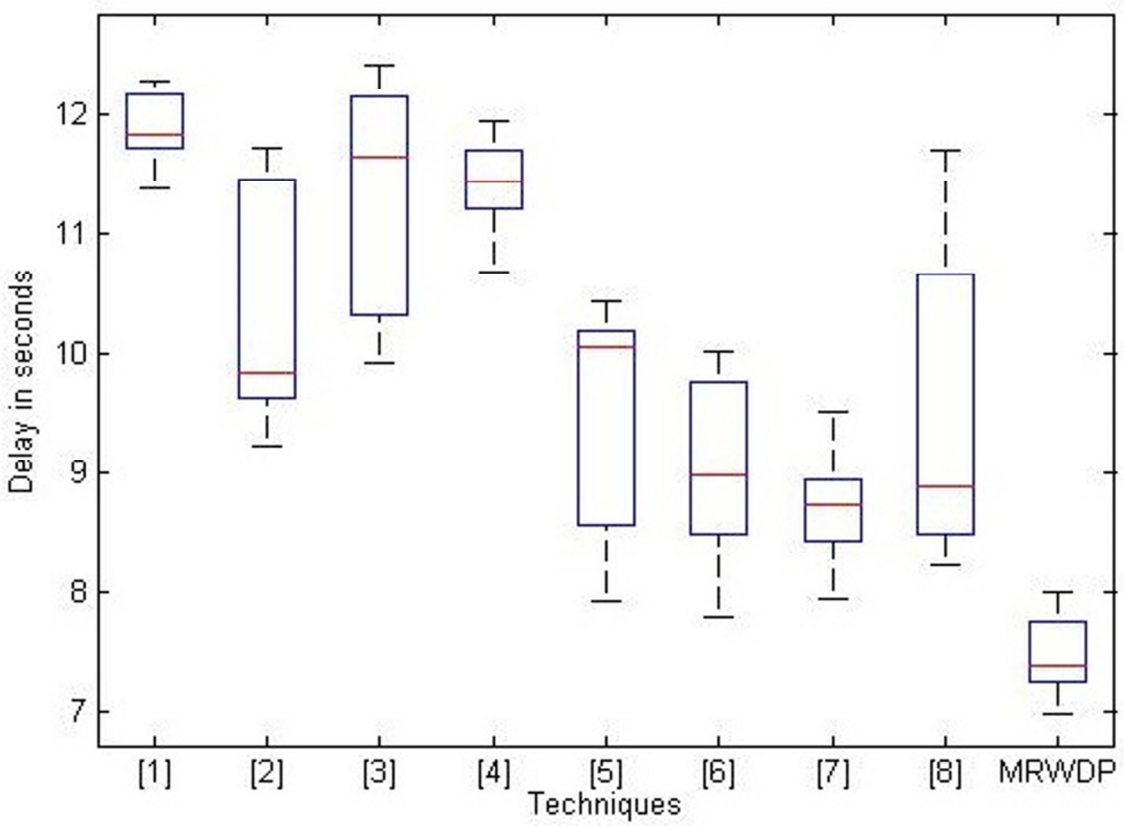

Figure 8: Delay of MRWDP

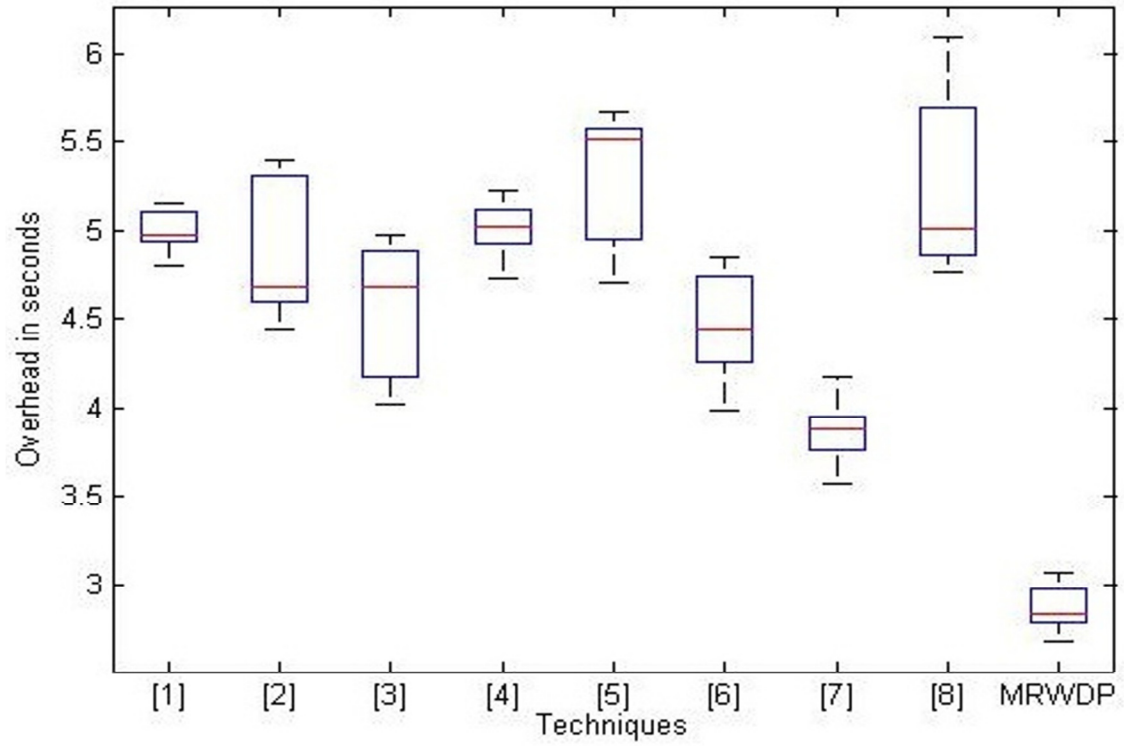

Figure 9: Overhead of MRWDP

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

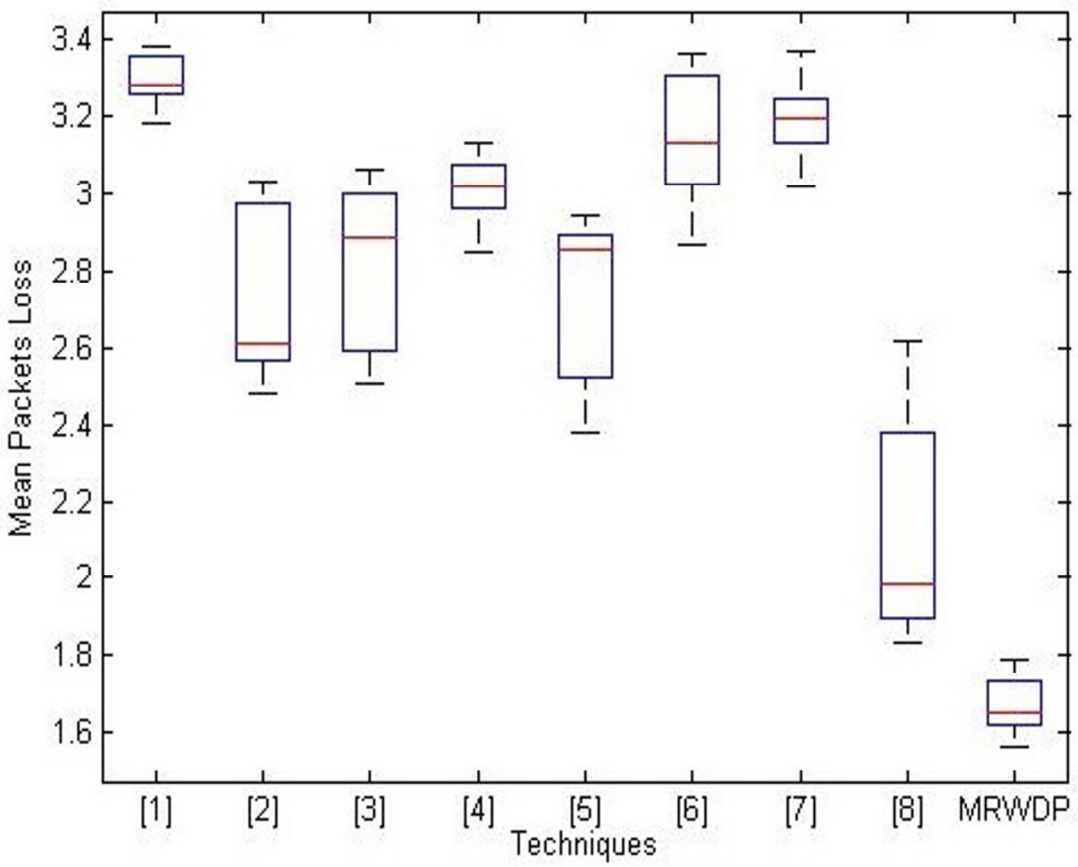

Figure 10: Message Loss of MRWDP

7. CONCLUSION AND FUTURE WORK

The black hole is an attack in MANETs, which suddenly decrease network performance by dropping the No. of messages. The black hole node always promotes itself by means of maximum sequence value and smallest hop sum. Black hole node all the time attempt to attract and monitor the concentration of the source node by guarantee them that it has the minimum cost path around destination node. The black hole reduces the performance of the network a lot. Among the existing techniques, WD technique has better performance in preventing the black hole attack. It utilizes the local knowledge of the next hop node and eavesdrops it. In WD technique, if the message exchange time exceeds the threshold then node is marked as malicious. But it has several shortcomings, one of them is that it is unable to monitor link transmission error.

In order to handle this issue, a new multipoint relay based WD monitoring and prevention technique is proposed in this paper. The MRWDP utilizes the dynamic threshold value to detect the black hole attacker node, and then clustering and WD based optimistic path is selected for communicating the messages. The MRWDP is designed and implemented in the NS-2.3 tool. Comparisons have been drawn with recently MRWDPs for monitoring and preventing against black hole attack. The performance analysis has clearly indicated that the MRWDP outperforms over the available techniques. Thus MRWDP has reduced the overall message dropping, which improves the performance of the MANETs.

We have proved that detection of malicious nodes is not only sufficient for performance improvement of MANETs. The performance of MANETs can be modified by leverages boundaries between network layers and various nodes. We have simulated the technique for

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

showing its importance. In future this technique can be used for some other routing protocols and can be improved further by using the fuzzy membership functions for better decision-making process. This work is limited to Black hole attack only, in the near future can be considered for multiple attacks at a time. Also, data mining technique can be introduced to detect the type of attacks, when multiple attacks are considered. The performance of MRWDP is checked by taking a fixed number of nodes. In future, the number of nodes can be varied to check the performance under various parameters.

ACKNOWLEDGEMENT

Authors are highly thankful to the Department of RIC, IKG Punjab Technical University, Kapurthala, Punjab, India for providing the opportunity to conduct this research work.

CONFLICTS OF INTEREST

The authors declare no conflict of interest.

REFERENCES

[1] N. Marchang and R. Datta, "Light-aggregation trust-based communicate on technique for mobile Adhoc networks," in IET Information Security, vol. 6, no. 2, pp. 77-83, 2012.

[2] E. Hernandez-Orallo, M. D. Serrat, J. C. Cano, C. T. Calafate and P. Manzoni, "Improving Selfish node Monitoring in MANETs Using a Collective WD," in IEEE Communications Letters, vol. 16, no. 5, pp. 642-645, 2012.

[3] J. A. F. F. Dias, J. J. P. C. Rodrigues, F. Xia and C. X. Mavromoustakis, "A Cooperative WD System to Detect Misbehavior nodes in Vehicular Delay-Tolerant Networks," in IEEE Transactions on Industrial Electronics, vol. 62, no. 12, pp. 7929-7937, 2015.

[4] E. Hernandez-Orallo, M. D. S. Olmos, J. C. Cano, C. T. Calafate and P. Manzoni, "CoCoWa: A Collective Contact-Based WD for Detecting Selfish nodes," in IEEE Transactions on Mobile Computing, vol. 14, no. 6, pp. 1162-1175, 2015.

[5] M. Kim, M. Medard and J. Barros, "Algebraic WD: Mitigating Misbehavior in Wireless Network Coding," in IEEE Journal on Selected Areas in Communications, vol. 29, no. 10, pp. 1916-1925, 2011.

[6] Baadache, A. and Belmehdi, A. "Struggling against simple and cooperative black hole attacks in multi-hop wireless Adhoc networks", in Computer Networks, vol. 73, pp. 173-184, 2014.

[7] Ming-Yang Su, "Prevention of selective black hole attacks on mobile Adhoc networks through black hole monitoring systems", in Computer Communications, vol. 34, Issue 1, pp. 107-117, 2011.

[8] Poongodi, T., and M. Karthikeyan. "Localized Secure Communication Architecture against Cooperative Black Hole Attack in Mobile Adhoc Networks", in Wireless Personal Communications: pp. 1-12, 2016.

[9] Banerjee, S.; Sardar, M. and Majumder, K., "AODV Based Black-Hole Attack Mitigation in MANET", in Proceedings of the International Conference on Frontiers of Intelligent Computing: Theory and Applications (FICTA). vol. 247, pp. 345-352, 2013.

[10] Dasgupta, M.; Santra, D. and Choudhury, S., "Network Modeling of a Black hole Prevention mechanism in MANET", 4th IEEE International Conference on computational intelligence and communication networks. pp. 734-738, 2012.

[11] Kurosawa, S.; Nakayama, H.; Kato, N.; jamalipour, A. and Nemoto, Y., "Detecting Black hole Attack on AODV-based Mobile Adhoc Networks by Dynamic Learning Method", in International Journal of Network Security. Vol. 5(3): 338-346, 2007.

[12] Jain, S.; Jain, M. and Kandwal, H., "Advanced procedure for monitoring and prevention of cooperative black and Grayhole attacks in mobile Adhoc networks", in International journal of Computer Applications. Vol. 1(7), pp. 37–42, 2010.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[13] Sun, B.; Guan, Y.; Chen, J. and Pooch, U., "Detecting Black-hole Attack in Mobile Adhoc Networks", in IEEE conference on Personal Mobile Communications, 5th European (Conf. Publ. No. 492), 2003.

[14] Li, X.; Jia, Z.; Zhang, P.; Zhang, R. and Wang, H., "Trust-based on-demand multipath communication in mobile Adhoc networks", in IEEE conference proceeding, IET Information Security. Vol. 4, Issue 4, 2010.

[15] Namdeo, M.; and Patheja, P., "Denial of Service (DoS) and Black Hole Attack Prevention by Enhanced WD Technique in MANET", in International Journal of Advanced Research in Computer Science and Software Engineering. Vol. 5, Issue 12, 2015.

[16] Cai, L.; Li, X. and Chong, P., **"**A novel self-checking Adhoc communication scheme against active black hole attacks", in Wiley online library, Security And Communication Networks. Vol. 9, pp: 943–957, 2015.

[17] Muhammad, I.; Khan, A.; Haider, A. and Mohsin, I., "Monitoring and Prevention of Black Hole Attacks in Mobile Adhoc Networks", in Springer, Adhoc, Networks and Wireless. Vol. 8629, pp 111-122.

[18] Chatterjee, R. and Routray, M., "Black Hole Combat Using node Stability System in MANET", in Social Informatics and Telecommunications Engineering. Vol. 62, pp 249-254.

[19] Ghathwan, K. and Yaakub, A., "An Artificial Intelligence Technique for Prevent Black Hole Attacks in MANET", Advances in Intelligent Systems and Computing. Springer International Publishing Switzerland, 2014.

[20] Rajesh, M. and Usha, G., "A Novel Honeypot Based Monitoring and Isolation Approach (NHBADI) to Detect and Isolate Black Hole Attacks in MANET", in Wireless Personal Communication. Springer, 2016.

[21] Kamatchi, V.; Mukesh, R. and Kumar, R., "Securing Data from Black Hole Attack Using AODV Communication for Mobile Adhoc Networks", in Advances in Computing& Inform. Technology, Springer, AISC 177, pp. 365–373, 2013.

[22] Mohammed, N.; Otrok, H.; Wang, L.; Debbabi, M. and Bhattacharya, P., "Mechanism Design-Based Secure Leader Election Model for Black Hole Monitoring in MANET", in IEEE transactions on dependable and secure computing. Vol. 8, no. 1, 2011.

[23] Ritchie, L.; Richa, W. and Reisslein, M., "Cluster Overlay Broadcast (COB): MANET Communication with Complexity Polynomial in Source-Destination Distance", IEEE transactions on mobile computing. Vol. 5, No. 6, 2006.

[24] Chang, J., "Defending against Collective Attacks by Malicious nodes in MANETs: A Cooperative Bait Monitoring Approach", *IEEE Systems Journal*, pp.65-75, 2015.

[25] Djenouri, D. and Badache, N., "Struggling against Selfishness and Black hole Attacks in MANETs", in *Wireless Communications and Mobile Computing*, UK: Wiley Online Library, pp.689-704, 2008.

[26] Kaushik, N. and Dureja, A., "Performance Evaluation of modified AODV against Black Hole Attack in MANET", in *European Scientific Journal*, Portugal: University of the Azores; .pp.182-193, 2013.

[27] Gong, T. and Bhargava, B., "Immunizing mobile Adhoc networks against collective attacks using cooperative immune model", in Wiley Online Library, *Issue: Security and Communication Networks*, pp.58-68, 2013.

[28] Ying, S., "Prevention of Selective Black hole Attacks on MANETs through black hole monitoring systems", in *Computer Communications (ELSEVIER)*, The Netherlands.pp.107-117, 2011.

[29] Arathy, K. and Sminesh, C., "A Novel Approach for Monitoring of Single and Collective Black Hole Attacks in MANET", in Elsevier, Recent Advancements and Effectual Researches in Engineering, Science and Technology – RAEREST Vol. 25, pp. 264–271, 2016.

[30] Babu, M.; Dian, S.; Chelladurai, S. and Palaniappan, M., "Proactive Alleviation Procedure to Handle Black Hole Attack and Its Version", The Scientific World Journal, Hindawi publications, vol.2015, 2015.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

[31] Casado, L.; Fernández, G.;Teodoro, P. and Carrión, R., "A model of data forwarding in MANETs for light aggregation monitoring of malicious message dropping", in Computer Networks: The International Journal of Computer and Telecommunications Networking, Vol. 87, Issue C, 2015.

[32] Jalil K.; Ahmad Z. and Manan J., "Mitigation of Black Hole Attacks for AODV Communication Technique", in International Journal on New Computer Architectures and Their Applications (IJNCAA),Vol. 1. Issue 2, pp.336-343, 2011.

[33] Shi, F.; Liu, W. and Jin, D., "AA cluster-based countermeasure against black hole attacks in MANETs", in Telecommunication systems. Vol. 57, Issue 2, pp. 119-136, 2014.

[34] Batham, G. and Sejwar, V., "Implementation of Dempster-Shafer Theory for Trust based Communication in MANET", in International Journal of Computer Applications. Vol. 150-No.11, 2016.

[35] Olmos, M.; Orallo, E.; Cano,J.; Calafate, C. and Manzoni, P., "A novel approach for the fast monitoring of black holes in mobile Adhoc networks", in SAGE, Concurrent Engineering: Research and Applications. September 2013, vol. 21, pp.: 177-185, 2013.

[36] Arunmozhi, S. and Venkataramani, Y., **"**Black Hole Attack Monitoring and Performance Improvement in Mobile Adhoc Network", in Information Security Journal: A Global Perspective. Vol. 21, Issue 3, pp. 150-158, 2012.

[37] Vasudevan V.; and Anita E., "Prevention of Black Hole Attack in Multicast Communication Techniques for Mobile Adhoc Networks Using a Self-Organized Public Key Infrastructure", Information Security Journal: A Global Perspective. Vol. 18, pp: 248-256, 2009.