Energy Efficient Robust Approach to Detect and Prevent Gray-Hole Attack in MANET

Bhaskar Nandi
Asst.Professor,MCA, Seacom Engineering College
Howrah-711302

Prasun Chakrabarti
Professor, CSE, Sir Padampat Singhania University, Udaipur
313 601, Rajasthan

Binoy Sasmal
Asst.Professor, IT,
Seacom Engineering College,
Howrah-711302

ABSTRACT
Mobile Ad-hoc Network (MANET) is typical wireless ad hoc networks which don't have any fixed topology due to the mobility of the nodes. The nature of these networks is dynamic and don't have any pre-existing security infrastructure to prevent various routing attacks and to protect from malicious nodes. There are mainly two approaches to isolate security threats in MANET, Proactive and Reactive. Proactive methods are based on various cryptography techniques which takes more bandwidth and resource such as battery power. Our approach is basically a simple and robust Reactive method than different security solution to prevent Black-Hole and Gray-Hole attack by detecting malicious nodes dynamically. In our schema the range of verification is wider than the previous available approaches, so the possibility of correct decision is maximized yet the resource utilization and unnecessary packet transfer is minimized.

Keywords
MANET, Security, Malicious nodes, Reactive, Routing attacks, Simple, Robust, Attack Strategy

1. INTRODUCTION
Mobile Ad-Hoc Network (MANET) is based on wireless peer to peer ad-hoc connection. It operates without any pre-existing infrastructure. The networks are self-organized and self-configuring. The structure i.e. the Topology changes dynamically as the nodes are mobile. The nodes are not just host but also routers and use multi-hop data forwarding. The range of application of MANET is from military networks to emergency awareness telecommunication [2, 3]. MANET doesn't come with any pre-existing security infrastructure. The wireless channel is vulnerable to attacks as there is no well-defined traffic monitoring or access control mechanism [5]. Standard MANET routing protocols typically assume a trusted and cooperative environment, as a result, a malicious attacker can readily become a router and disrupt network operations. There are several attacks possible, which are normally classified into Passive and Active attacks. In passive attack malicious nodes doesn't attempt to perform data modification, normally indulge in eavesdropping or monitoring. Active attack is based on modification of the original message or creation of false message. MANET Routing and Packet forwarding operation are exposed to malicious attacks, leading to various types of malfunction in the Network layer. The sophisticated attacks are GRAYHOLE in which nodes either drop packets selectively or drop packets in statistically and BLACKHOLE in which nodes drop almost all the packets [7].There are mainly two approaches to secure MANET: Proactive and Reactive.[1] Normally all the approaches for providing security in MANET are the proactive approaches that attempts to prevent an attacker from launching attacks in the first place, typically through various cryptographic techniques. The reactive approach seeks to detect security threats posteriori and react accordingly. To deal with various sophisticated attacks we need to detect as well as prevent the attackers (malicious node). There are some basic reactive approaches available to detect the Black-Hole and Gray-Hole attacks using some statistics [6, 8], but normally it doesn't verify the wide range of characteristics of the malicious nodes and the decisions are mainly monotonic. It also may propagate useless packets while detecting. The proposed approaches [8] can detect the malicious nodes with different strategy and wide range of characteristics, with a dynamic threshold range of misbehavior. The Leader node is responsible for sending all the control packets to generate suspicion level. A Game is to be played according to the suspicion level to predict the right cases [8]. The key features in our schema is that it doesn't waste packets by resending where the objective (i.e. the decision) is already available. It also provides a new range to identify malicious nodes with varying characteristics and also can detect malicious node with different drop strategy.

2. SECURITY THREATS IN MANET AND PREVIOUS SCHEMA:
MANET is based on wireless Ad-Hoc network where each node relies on another node and the network should be cooperative in nature. MANET Routing and Packet forwarding operation are exposed to malicious attacks, leading to various types of malfunctioning in the Network layer [9]. Attacks are of mainly four types i.e. Interception, Fabrication, Modification and Interruption. For the last few years various network layer attacks for MANET have been identified and studied, according to which MANET Network Level attacks can be classified into Passive Attacks and Active Attacks. Passive attacks are generally Eavesdropping, Traffic Analysis, and Snooping etc. Worm-hole, Black-hole, Gray-hole are various Active attacks. Passive Attacks are Easy to prevent but detection is uneasy where as, for Active Attacks Detection is Easy but prevention is not easy [9, 10]. Our approach basically concentrates on two sophisticated Network Layer Passive attacks, which are Black-Hole and Gray-Hole [7].

2.1. Black Hole
A black hole is a malicious node that falsely replies for route requests without having an active route to the destination. It exploits the routing protocol to advertise itself as having a good and valid path to a destination node, but at transmission time it consumes or drops the data packets. In general algorithm these types of attacks are difficult to detect. Normally any nodes that have entered in MANET network can act as a black hole, so pre determination is impossible

2.2. Gray Hole

A grey hole may forward all packets to certain nodes but may drop packets coming from or destined to specific nodes. So sometimes it may act normally but sometime it act maliciously. Due to the uncertain behavior this type of attack is not easy to detect.

Black-Hole and Gray-Hole attacks are specified with several characteristics. Normally the node that drops packets is called to be misbehaving node. But not all the nodes that drop packets are malicious node as packets can also be lost. Black-hole normally use to drops all the packets even the RREQ (Route Request) for any other nodes. Gray-Hole use to drop packets for a selected node or packets for a specific protocol (i.e. drops all the UDP packets while forwarding all the TCP packets). Gray-Hole can also drop packets using some statistics (i.e. drops 60% of the packets). As there are no specified characteristics for Gray-Hole we need to assume a dynamic nature. So we can't fix any statistic that defines Gray-Hole i.e. the nodes that drops 20% of the packets can also be a Gray-hole.

Considering those dynamic characteristics of malicious nodes it becomes very complex and costly to secure the Network using proactive security approach by several cryptography schemas. It is better to use reactive approach (Runtime detection) for attacks like Gray-Hole and Black-Hole.

Some previous schema [8] that is based on reactive approach to detect the malicious node has used a Suspicion level. It used two phases where in the first phase the Leader node determine the Suspicion Level based on the number of packet drops, it also detects the possible type of attack (i.e. Detect whether the node is Black hole or Gray Hole). In the Second Phase, to increase the accuracy of detection 'probe' packets are used and also a game has played to detect the right case.

This approach has several shortcomings like it can't deal with different drop strategies. It doesn't give any clue about the determination of the threshold level. Any node that drops at least 50% of packets can affect the normal working of the network and can launch DOS (denial of Service) i.e. it can be declared as malicious (Gray-Hole) [11]. In this case this schema wastes packets where the decision is already available (e.g. If threshold level is 50% of the highest possible Suspicion level and already more than half of the 'probe' packets that has been send and dropped then it must be a Gray-hole so we don't need more packets to send [11]). Here the game is played only if the suspension level is greater than the threshold level otherwise the node is declared as safe. As the Gray-hole comes with varying characteristics and as in MANET where cooperation is a main factor, if any Node drops 40% of the packets it also can affect the network operations. A Gray-hole node that selectively drops packets can drop less than 50% of packets (e.g. the ratio of UDP packets that the Gray-hole drops is 30% of the Total packets) and in these case the previous algorithm can't detect. The game is played to determine the right case inside the new threshold range in our approach [4, 8].

3. NEW SCHEMA

As it was proposed earlier a 'Packet Transfer Information' (PTI) table is maintained for each node in the MANET for its one hop neighbors. For a fixed intervals [12] if the "Packet From" and "Packet To" entries of any node's 'N' PTI table for no 'S' found zero then node 'N' aware the master node about the suspicious node 'S'. Then the master node send's a RREQ message to the suspicious node 'S' for a reliable one hop neighbor node 'R' of 'S'. As the black hole drops all the packets, in the schema if RREP doesn't arrive then the Black-Hole detection process starts, else it checks for possible Gray-hole.

Node ID	Packet From	Packet To	Suspicion Level (S)

Figure 1. PTI Table

In the previous papers [8] we have seen that the suspension level has been checked to a threshold value and no clue has been given about how to find out the threshold value. In our schema we are declaring nodes as malicious when it drops greater than or equal to 50% of the packets. A new range of suspicion has been introduced to detect the varying characteristic within which the game is played to predict the right case. If the range starts from 'Sp' and ends at 'Ep' then,

$$0\% < \text{'Sp'} < \text{'Ep'} < 50\%$$

Let we are checking a suspicious node 'Sn' whether it is malicious or not. To check we will send a fixed no of Probe packet to determine the nodes behavior. Let the no of total 'Probe' Packet that is predefined is 'U'. At any given time if the Suspicion Level is 'S' then the number of packets Dropped is (S/2) [As for each drop packet the suspicion level is increased by 2]. So the Current Dropping Percentage 'Cp' of Dropped packet is ((S / (U * 2)) * 100). Let the Threshold Suspicion Level from which the range will start is 'Ss'. Then the starting percentage 'Sp' be '((Ss / (U * 2)) * 100)' where (0 < 'Ss' <= 'U - 2') must hold. Here 'Ep' in suspicion level is 'U – 2'.

4. ALGORITHM

Let the Suspected node is 'Sn'

'P' the no of 'Probe' packet has been sent

'S' the current suspicion level

Step 1:

Send RREQ to node 'Sn' for a route to

reliable node 'Rn';

Step 2:

If (RREP received from 'Sn') Then

For each of the total of 'U' Probe packets to

node 'Rn' via node 'Sn';

If (S < (U*2) / 2)

If ((((U – P) * 2) + S) < (U*2)/2 AND S > As)

Then

Raise 'P'

Else

Send the Probe Packet

Raise 'P'

If (Probe message doesn't reaches node 'Rn')

Then

Raise the Suspicion Level 'S' of the Node

'Sn' by Two

Else

Do Nothing

Else

For each of the total of 'U' Probe packets to

node 'Rn' via node 'Sn';

If (probe message reaches node 'Rn')

Raise the Suspicion Level(S) of

node 'Sn' by unit value ;

Else

The node 'Sn' may be a black hole.

Raise the suspicion level by a higher

value than unity;

Step 3:

If ('Cp' is Greater than or Equal to 50%)

Declare the Node as Malicious

Else If ('Cp' is Greater than 'Sp')

Play the Game to Determine the Right case

Else

Treat the node as non-malicious for the

next 4 Beacon of time

In the following algorithm two inspections are being done before sending the probe packet.

(U*2)/2 is the 50% suspicion Level of the Maximum possible. It is checking whether it has reached the 50% dropping percentage. If it has, then no probe packet will be send as the highest possible decision is already available.

(((U – P) * 2) + S) is the Maximum possible suspicion level that can be achieved considering current suspicion level S. So where we can't reach the 50% drop ratio but have already reached the bellow range then no probe packet will be send.

5. GAME

In the Previous approach [8] the Game that has been applied was done by tossing an unbiased Coin. According to the result the decision is being taken whether the node Showing an attack or not. In our approach we have done it by changing the unbiased Coin with a biased one. The way it is biased depends on the drop ratio of the particular node.

Let we have a function 'f()' that generate a random number in the range of Zero to Ten. 0 < value of 'f()' < 10.

Now we take a middle value 'M'.

If (value of f() is >'M') then

It's Not showing an attack

Else

Showing an Attack

In the previous approach [8] the value of 'M' is always '5' as it is always unbiased. But in our approach the value of 'M' depends on the current dropping percentage 'Cp'. The 'M' is equal to ('Cp' / 10) * 2.

So if the 'Cp' is 40% then the 'M' is (40 / 10) * 2 = 8. So the range of showing attack becomes 0 -> 8. So the possibility of showing attack increases. Where, if the 'Cp' is 20% then the 'M' is (20/10)*2 = 4 and the range of showing attack becomes 0 -> 4. So the possibility of showing attack decreases.

The dropping percentage represents a vital characteristic of the malicious node. So as the decision is being effected by the dropping percentage, the possibility of correct decision increases.

As per the previous game 'Head' in the toss was showing an attack and Tail was not showing an attack. For Head and Tail two different no 'a' and 'b' was shown. A random number x, such that x ~ N (0, 1) (meaning: x follows a standard normal distribution N → normal (mean, variance)) [Figure 2]

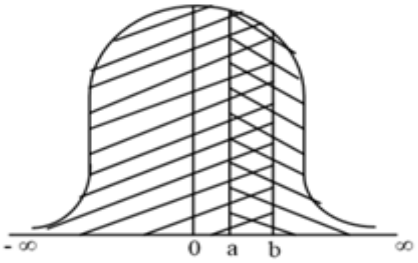

Figure 2.

The correct decision was determined as the probability of getting x within a and b.

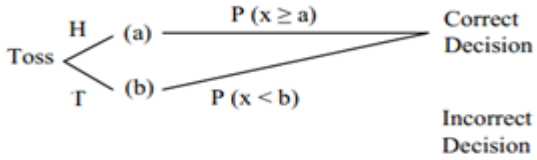

Figure 3. Correct Decision

Probability of correct decision:

P [correct] = ½ [P (x ≥ a) + P (x < b)]

= ½ [P (-∞ < x < ∞) + P (a < x < b)]

= ½ [1 + P (a < x < b)]

Therefore, P [correct] > ½ (always)

As in our game, as the coin is biased for some event, so the probability for 'Head' and 'Tail' changes. Here 'drop-ratio' determines the way the coin is biased. We are defining the coin's biased-ness according to a mid-value 'M' in a range from '0' to '100'. Let the lower part is defined as 'Head' and the upper part is defined as 'Tail'. As the coin made biased according to the drop ratio we can fairly say that the coin is biased towards right decision.

0	Head	M	Tail	100

When we define the range from drop-ratio it is:

0	Head	M = (Dr*2)	Tail	100

E.g. If the drop-ratio is 20% then the probability for 'Head' becomes (40 – 0)/100 = 4/10 and the probability for 'Tail' is (100 – 40)/100 = 6/10. So we can see here the coin is biased towards 'Tail'. So in this case the 'Tail' is the right outcome.

Again, for drop-ratio 40% the probability for 'Head' becomes (80 – 0)/100 = 8/10 and the probability for 'Tail' is (100 – 80)/100 = 2/10. So we can see here the coin is biased towards 'Head'. So in this case the 'Head' is the right outcome.

For drop-ratio 25% the coin will be unbiased as the probability of 'Head' and 'Tail' will be same.

Let us take the range for the game is from drop-ratio 20% to drop-ratio 49%. As in this particular range we can take 30 different drop-ratios, so we can say 30 different coins that are differently biased. For our calculation we have taken 15 of it for drop-ratios 21, 23, 25, 27, 29, 31, 33, 35, 37, 39, 41, 43, 45, 47 and 49 for 15 individual events.

Let P be the probability of the coin towards the right outcome. As in the previous game an unbiased coin is considered for 'n' no of event the probability of correct decision would be:

$\sum (1/n) * Pn * [1 + P (a < x < b)] = ½ [1 + P (a < x < b)]$ [As Pn = ½ is all events]

In case of our game let us consider 15 events i.e. n = 15. The varying probability for 'Right outcome' is P which is determined by the drop-ratios Dr.

Dr	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49
Pn	.58	.56	.50	.54	.58	.62	.66	.70	.74	.78	.82	.86	.90	.94	.98

P[correct] = $\sum (1/15) * Pn * [1 + P (a < x < b)]$

P[correct] = (1/15) * [1 + P (a < x < b)] *[.59 + .56 + .50 + .54 + .58 + .62 + .66 + .70 + .74 + .78 + .82 + .86 +.90 + .94 + .98]

Or, P[correct] = 0.71 * [1 + P (a < x < b)]

As, 0.71 > 0.5

Therefore, 0.71 * (1 + P (a < x < b)] > 0.5 * (1 + P (a < x < b)]

As For all the event 'P' is greater than 0.5 excluding a single Event for Dr = 25% where the probability of 'Right outcome' is 0.5.

So (our approach P [Correct]) > (old approach P [Correct]) > 1/2

6. DROPPING STRATEGY

To test our approach we customised several drop strategy that a malicious node may apply. We assumed that each malicious node has some drop percentage 'Dr' to achieve for a certain no of packets 'N' where 'N' is never known to other. Now the packet can achieve the drop percentage by several ways.

6.1. Random Strategy

In this strategy the malicious node take the decision whether to drop the packet or not by calling a random function f() that generate a value from the range 0->10. Now sets a middle value 'M' depends on the drop percentage 'Dr' to achieve and equal to (10 - (Dr/10)).

If (value of f() is >'M') then

Drop the packet

Else

Through the packet.

So if the drop percentage to achieve 'Dr' is 40% then the value of 'M' is (10 – (40/10)) = 6.

1 -> Through packet Range -> 6

7 -> Drop the packet Range -> 9

6.2. Points Strategy

Here the strategy based on Points which is determined by the dropping percentage 'Dr' to achieve.

Initially 'Old' is 0.

For each packet:

If (old + 'Dr') < 100 then, through packet - set (old + 'Dr') as old

Else drop packet - set (old + 'Dr' - 100) as old

TEST 1: The Test is done for a Node with 75% Drop percentage to achieve.

Old=0

0+75 = 75 -> Through Old = 75

75+75 = 150 -> Drop Old = 150-100=50

50+75 = 125 -> Drop Old = 125-100=25

25+75 = 100 -> Drop Old = 100-100=0

Total Packet Send = 4

Total Packet Dropped = 3

Drop Percentage = 75%

TEST 2: The Test is done for a Node with 40% Drop percentage to achieve.

Old=0

0+40 = 40 -> Through old = 40

40+40 = 80 -> Through old = 40

80+40 = 120 -> Drop old = 120-100=20

20+40 = 60 -> Through old = 60

60+40 = 100 -> Drop old = 100-100=0

Total Packet Send = 5

Total Packet Dropped = 2

Drop Percentage = 40%

7. EXAMPLE AND TESTING

A virtual MANET network is formed with nodes linked with each other working on a satisfactory environment condition.

Table 1. Initial PTI table of N(7)

Node ID	Packet From	Packet To	Suspicion Level (S)
N(1)	0	0	0
N(6)	0	0	0
N(8)	0	0	0

Table 2. Initial the PTI table of N(2)

Node ID	Packet From	Packet To	Suspicion Level (S)
N(1)	0	0	0
N(5)	0	0	0
N(3)	0	0	0

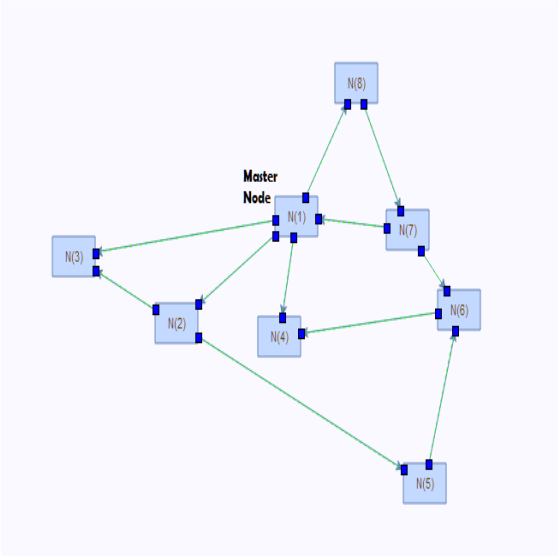

Figure 4. The Topology of the Current Network

As per Figure 4. N(1) is the master node in this network with 8 nodes in total i.e. N(1)->N(8) . Now each node is added with its characteristics that will define its behaviour throughout the network and its not known to anyone.

Assume that N(6) and N(8) is intended to return RREP and to drop 67% and 40% of a Certain no of packets during the communication, where N(6) follows RANDOM drop strategy and N(8) follows POINTS drop strategy. N(5) has 56% of intended Drop Percentage and RREP will be dropped.

Now each node maintains a PTI table with entry of each of its one hop neighbours.

7.1. Phase 1 (Generation of PTI entry and informing master)

Phase 1: After 4 beacons of time of communication (packet transfer) the PTI table has been modified:

Table 3. Modified PTI table of N(7)

Node ID	Packet From	Packet To	Suspicion Level (S)
N(1)	80	40	0
N(6)	0	0	0
N(8)	0	0	0

Table 4. Modified PTI table of N(2) :

Nod ID	Packet From	Packet To	Suspicion Level (S)
N(1)	80	40	0
N(5)	0	0	0
N(3)	20	40	0

So from this three PTI table of node N(2) 'Table 3' and N(7) 'Table 4', Node Entry for N(5), N(6), N(8) has 'Packet From' and 'Packet To' entry as '0'. So node N(1), N(2) and N(7) will inform the Master Node N(1) about the Suspicious Nodes. Master Node will treat the other nodes as Reliable to determine the Suspicious Nodes true characteristics and make necessary decision. Master node also sets the other node status as Reliable 'Figure 5.'

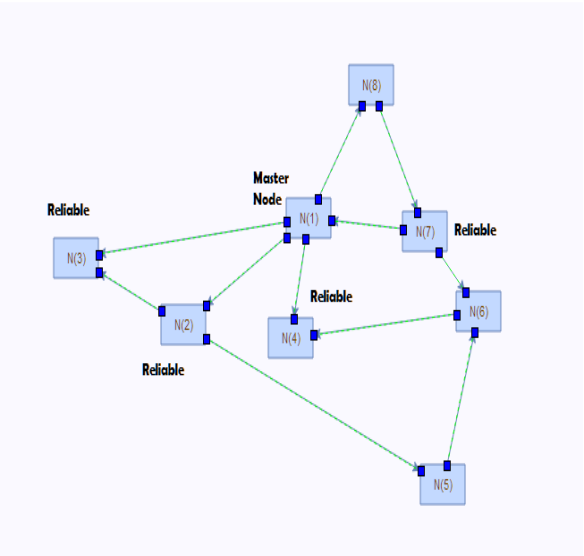

Figure 5. The Topology after 1nd phase

7.2. Phase 2 (Run Algorithm)

To run the algorithm with fixing 20 nos. of probe packets. So the maximum possible suspicion level is (20*2) = 40. Now the suspicion level range for malicious node is: 50% of 40 -> 20

i.e. 20 <= malicious suspicion level <= 40

The below range is defined as 20% dropping percentage. So the range starts from 20% of 40 -> 8 and the range ends on 20 – 2 = 18.

i.e. 8<= suspicion level to play game <= 18

So the total range of decision becomes:

0 < reliable suspicion level < 8 <= suspicion level to play game < 20 <= malicious suspicion level <= 40

Checking For N(6):

Step 1:

Master Node N(1) sends a RREQ to suspicious node N(6) for a route to reliable node N(4). RREP returns from N(6) so it's not a Black-Hole.

Step 2:

Master node then run the algorithm to determine the suspicion level of N(6) which has a intended packet drop percentage 67% in a RANDOM strategy.

It drops 11 packets of the first 14 packets and the suspicion level 'S' is already 22 which is greater than 20 i.e. the 50% of the maximum suspicion level. So the master node stops probe packet sending immediately and go for the decision phase. Here 6 probe packets have been saved.

Step 3:

In this phase the 'Cp' i.e. ((S/(N*2))*100) is ((22/(14*2))*100) = 78.57%. As the 'Cp' is greater than 50% the decision is 'Gray-hole'.

Later Activities:

The master node informs the other nodes about the Gray-Hole to block or remove the node from the network.

Checking For N(5):

Step 1:

Master Node N(1) sends a RREQ to suspicious node N(5) for a route to reliable node N(2). RREP doesn't return from N(5) so it's a Black-Hole.

Step 2:

Master node then run the algorithm to determine the suspicion level of N(5) which has a intended packet drop percentage 56% in a POINTS strategy. The Master node sends the probe packet to determine the suspicion level using Black-Hole detection strategy (As mentioned in the previous paper []).

It has dropped 11 packets out of 20. So the total suspicion level is [(11*2) + (20 – 11)] = 31

Step 3:

In this phase the decision is taken for playing a game strategy as it is a possible Black-Hole.

Later Activities:

The master node informs the other nodes about the Black-Hole to block or remove the node from the network.

Checking For N(8):

Step 1:

Master Node N(1) sends a RREQ to suspicious node N(8) for a route to reliable node N(7). RREP returns from N(8) so it's not a Black-Hole.

Step 2:

Master node then run the algorithm to determine the suspicion level of N(8) which has a intended packet drop percentage 40% in a POINTS strategy.

It drops 6 packets of the first 17 packets and the suspicion level 'S' is 12 which is greater than 8 i.e. the 20% of the maximum suspicion level and it can never reach the range of 50%. So the master node stops probe packet sending immediately and go for the decision phase. Here 3 probe packets have been saved.

Step 3:

In this phase the 'Cp' i.e. ((S/(N*2))*100) is ((12/(17*2))*100) = 36%. As the 'Cp' is less than 50% and greater than 20% the decision is to be taken by a Game in phase 3.

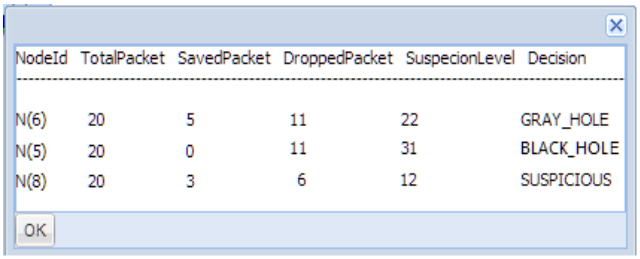

Figure 6. The Result after 2nd phase

7.3 Phase 3 (Play Game)

The decision for N(8) should be taken via Game. The 'Cp' is 36% so the middle value 'M' of the decision range 0 -> 10 is (36*2/10) = 7.6. The random function f() generates a value 7.8 which is greater than 7.6, so no attack is showing.

Later Activities:

The master node informs the status for the node N(8) as reliable for 4 beacons of time.

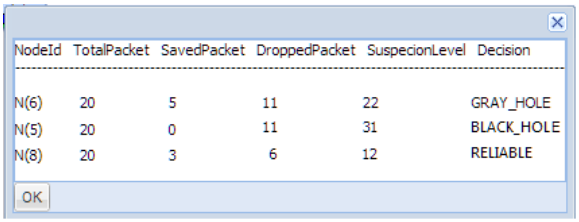

Figure 6. The Result after 3rd phase

8. OBSERVATIONS

As for detecting the Black-Hole previous algorithm has been used, so it will send all the probe packets and no packets will be saved.

It is always way to determine a attacking node it tends to drop packet at starting time rather than the ending time and it will also maximize the nos. of saved packet.

From observation the POINTS strategy is more affected as an attacker than the RANDOM strategy. Because to determine POINTS strategy attacks the no of saved packet decreases as the required time complexity increases.

The intended packet dropping percentage of a particular attacking node may not be same with the current dropping percentage 'Cp', as the 'Cp' depends on the algorithm and the way attacker going to drop the packets.

For a suspected Gray-Hole the inclusion of 'Dr' in the game makes the decision more accurate.

9. REFERENCES

[1] L. Zhou and Z. J. Haas, "Securing ad hoc networks", In IEEE Network Magazine, volume 13, page 24-30, Nov. 1999.

[2] Hassan A. Karimi, Prashant Krishnamurthy "Real-time routing in mobile networks using GPS and GIS techniques", Proceedings of the 34th IEEE Hawaii International Conference on System Sciences – 2001.

[3] Luiz A. DaSilva, Jeff H. Reed, William Newhall, Tutorial on "Ad hoc networks and automotive applications", Mobile and Portable Radio Group, Virginia Polytechnic Institute and State University, 2002.

[4] Murali Kodialam, T. V. Lakshman. "Detecting Network Intrusions via Sampling: A Game Theoretic Approach", In Proceedings of IEEE INFOCOM, 2003

[5] HongMei Deng, Wei Li, Dharma P. Agrawal, "Routing security in wireless ad hoc networks", IEEE Communications Magazine, October 2002, page 70-75.

[6] Jiejun-K, Petros-Z, Haiyun-Luo, Songwu-Lu, Lixia-Zhang, " Providing robust and ubiquitous security support for mobile ad-hoc networks", Proceedings Ninth International Conference on Network Protocols. ICNP 2001, Riverside, CA, USA, page 11-14 Nov. 2001.

[7] Y. Xiao, X. Shen, and D.-Z. Du (Eds.), "A survey on attacks and countermeasures in mobile ad hoc networks", Wireless/Mobile Network Security, chapter 12, page 1-38, Springer, 2006

[8] Abhijit Das, Atiqur Rahman, Soumya Sankar Basu and Atal Chaudhuri "Energy Aware Topology Security Scheme for Mobile Ad Hoc Network" . Proceedings of the 2011 International Conference on Communication, Computing & Security, Pages 114-118, ACM New York, NY, USA ©2011.

[9] Rashid Hafeez Khokhar, Md Asri Ngadi and Satria Mandala. "A Review of Current Routing Attacks in Mobile Ad hoc Networks". International Journal of Computer Science and Security, 2(3):18-29, 2008

[10] Oscar F. Gonzalez, God win Ansa, Michael Howarth and George Pavlou. "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc networks". Journal of Internet Engineering, 2:1, 2008

[11] G. S. Mamatha Dr. S. C. Sharma "A Robust Approach to Detect and Prevent Network Layer Attacks in MANETS" International Journal of Computer Science and Security, Volume (4): Issue (3)

[12] Soumya Sankar Basu and Atul Chaudhuri "Self Adaptive MANET: A Centralized Approach", Foundation of Computing and Decision Sciences, 2004, vol. 29, no. 4, page 271-286