Volume 5, Issue 1, January 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Attack Detection using Reward Matrix for Mobile Ad-hoc Networks

[1]Rajani M.Gadade, [2]Ashok M. Kanthe, [3]Dina Simunic
[1, 2] Sinhgad Institute of Technology, Lonavala, Pune, India
[2, 3] Faculty of Electrical Engineering and Computing, University of Zagreb, Croatia

Abstract—For Mobile ad hoc networks (MANETs) security is a critical & thoroughly examined scientific area which is interest of many researchers. Due to wireless network, limited resources and lack of centralized administration, dynamically changing position, MANETs are vulnerable to various types of denial of Service (DoS) attacks on network layer. In black hole attack all data packets are consumed or lost at malicious node. In this paper, we have proposed black hole attack detection technique which uses the concept of reward matrix. Reward matrix is the matrix which stores the packet routing information. Source node forms reward matrix for malicious node from the input data. This mechanism improves the network performance in terms of Packet delivery ratio, delay, control overhead, Throughput.

Keywords—Black Hole Attack, MANETs, Mobility, Reward Matrix, Source nodes.

I. INTRODUCTION

There are two types of wireless networks known as Ad-hoc networks and Sensor networks. Mobile ad hoc networks are multi-hop wireless network which is dynamically formed amongst groups of mobile users. It has different characteristics such as lack of centralized administration, distributed user, dynamically changing topology and there is no fixed infrastructure. Without router or access point wireless clients connect directly together. Nodes with ad hoc networks are mobile and they communicate with each other within the radio range through wireless links. There are different study areas in MANET such as routing, power management, bandwidth management, radio interface and security issues [1]. There are different applications of mobile ad hoc networks such as tactical networks, emergency services, commercial and civilian environments, home and enterprise networking, education, entertainment etc.Security services for MANET are authentication, availability, confidentiality and integrity to the mobile users. The security solution should provide complete protection to the entire protocol. Security in MANET is in different layers such as application layer, transport layer, network layer, link layer and physical layer. MANET is suitable for applications such as military battlefield, emergency rescue etc [2]. There are 2 types of routing attacks namely Black hole attack and Gray hole attack. In a black hole attack malicious node (called black hole) replies to every route request by falsely claiming that it has a fresh enough route to the destination. In this way all the traffic of the network are redirected to that malicious node which then dumps them all. A gray hole attack is a variation of black hole attack, where an adversary first behave as an honest node during the route discovery process, and then silently drops some or all of the data packets sent to it for further forwarding even when no congestion occurs. Detection of gray hole attack is harder because nodes can drop packets partially not only due to its malicious nature but also due to overload, congestion or selfish nature.

This paper presents the solution to black hole attack for RMMP protocol and improves the performance of the network. The paper is organized like section 2 discusses about literature survey, section 3 discusses about proposed snemd protocol, section 4 discusses about proposed security technique, section 5 simulation and finally section 6 concludes the paper.

II. LITERATURE SURVEY

Security in Mobile Ad-hoc network is the most important concern for the basic functionality of the network. The availability of network services, confidentiality and honesty of the data can be achieved by assuring that security issues have been met. MANETs frequently suffer from security attacks because of its features like open medium, varying its topology dynamics, lack of central monitoring and administration, cooperative algorithms and no apparent defense mechanism. These issues have changed the control zone situation for the MANETs against the security fear.

E. A. PANAOUSIS et.al used game theory to model non-ooperative security games between a MANET, which is defended by IDS operating at each node as well as a group of collaborative malicious coalition. This work innovates by

finding the defending & attacking probability distributions, of any MANET & malicious coalition that maximize the utility of a non-cooperative security game between the aforementioned entities [3].

A. M. Kanthe et.al proposed mechanism that uses effective way of providing security in AODV against gray hole attack. It is used to detect gray hole attack and eliminate the normal nodes with higher sequence number to enter in the black list. Effective decision making regarding black listing of nodes by keeping track on switching activity. Effective use of peak value and implementation of fresh approach of current elapsed time of adhoc network to make the proposed mechanism more efficient. It is not sending any alarm packets to other nodes when gray hole detected. Hence it is reducing extra routing overhead incurred by sending alarm packets [4].

M. K. MARINA et.al proposed an on-demand multipath protocol called AOMDV that extends the single path AODV protocol to compute multiple paths. AOMDV ensures that the set of multiple paths are loop-free and the alternate paths at every node are disjoint. Other novel features of AOMDV include: low inter-nodal coordination overheads, ability to discover disjoint paths without using source routing, minimal additional overhead over AODV to obtain alternate paths [5].

A. Patcha et.al modeled the interactions between a host-based IDS and an attacker as a basic signaling game which can be seen as a dynamic non cooperative game with incomplete information. The authors have not however considered colluding attackers or any malicious coalition [6].

H. Otrok et.al proposed a distributed mechanism which extends the lifetime of a cluster IDS model by electing different IDS leaders each time. The paper proposes a cooperative game model to catch the misbehaving IDS leaders while minimizing the false positive rate. On the other hand, a zero-sum non-cooperative game model has been proposed in order to maximize the probability detection done by the leader-IDS. The model helps the leader-IDS to use its optimal sampling strategy when intrusion detection takes place [7].

Y. Liu et.al have proposed a Bayesian game formulation to support intrusion detection in wireless ad hoc networks. According to this paper the defender tries to maximise his defending capabilities with respect in his energy cost while the attacker tries to damage the network without being detected. The authors have considered both static and dynamic games. For the static game they have derived the mixed-strategy Bayesian NE (BNE) and the pure-strategy BNE. They have additionally derived the mixed-strategy Perfect Bayesian Equilibrium (PBE) of the dynamic game proposing at the end a hybrid detection approach which uses the dynamic game model to compute equilibrium strategies for the players [8].

III. REWARD MATRIX MULTIPATH ROUTING PROTOCOL (RMMRP)

Protocol Overview

Each node broadcast hello message with neighbour list of node and its initial LDC value 0 (Link disconnection count to protect the route). Neighbor nodes receive hello message and update entry in neighbour table with neighbour list and LDC value.Packet send count and recv count is updated in all nodes. Source node start sending data, Initially it doesn't have path to forward data packet. It initiats route discovery process.

Source node sending route req with its uA value (uA is inverse of its nbr count) Nbr nodes recv route req and update its uA value in packet. If current node is destination then it send route reply by constructing reverse path, and set link broken flag as zero and uA value as recv request msg. If intermediate node has route to destination then, send reply constructing reverse path, and uAD value in reply message.

Route reply message is unicasted through reverse path, each intermediate node update its nnj value (nnj - nbr count)
Once reply message reaches source node then, it calculates its DC value. Replace DC_i by old DC value. Ui value and Ni value is computed & PD value is computed from U_t() - nnj / ni.

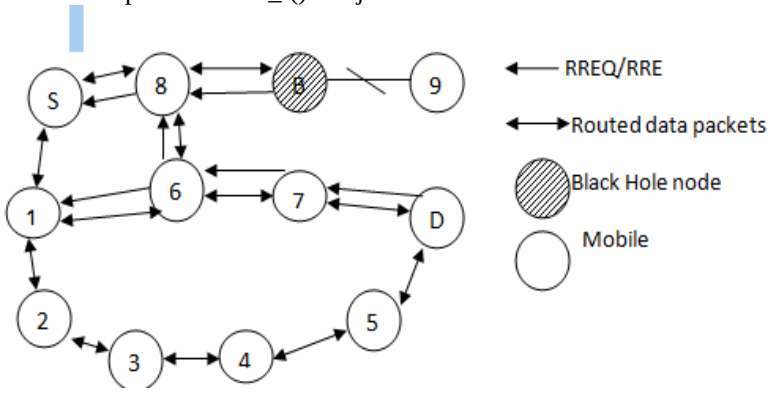

Figure1.Black Hole Attack Detection

Black hole attack is kind of DoS attack where black hole node can attract all packets by pretending shortest route to the destination .It drops all traffic destined for that node when traffic is received by it. The effect of this attack completely degrades the performance of the network because the destination node never receives any information from the source.

IV. IMPLEMENTATION DETAILS

MANET nodes must cooperate with each other to accomplish specific goals and thus selfish behaviour can introduce several problems such as a node might drop legitimate packets launching a black hole (Denial of Service) attack. The Algorithm proposes a way to derive the attack effort that a MANET or a malicious coalition, correspondingly, have to give in respect with their energy costs. Parameters such as Attack cost, RESIST cost and alarm cost used effectively.

STEP I Total send and recv utility value for attack and RESIST case is calculated.
STEP II Source node forms reward matrix from the input data. From reward matrix potential for attack and RESIST case is computed.
STEP III Source node forms reward matrix for malicious from the input data. From reward matrix potential for attack* and RESIST* case is computed.
STEP IV From periodical monitoring send recv and drop count is updated. Attack cost, RESIST cost and false alarm cost is estimated from packet count, and from these values rf, rd, ra is calculated respectively. From RESIST, attack value, probability of attack and its defense is estimated.

Reward matrix is the matrix which stores the Packet routing information. There are 2 malicious nodes attack_1 and attack_2. For RESIST case the values for attack_1 and attack_2 is calculated first. Then the values for non attack_1 and non attack_2 is calculated. Similarly the values for non RESIST case is calculated. From these values Reward matrix will formed which stores the packet routing information.

The utility functions of the MANET and the malicious coalition for the different strategy tuples $0 < Vn \leq 1$ indicates the loss of security when an attack against a node is successful.

Then reward matrix is updated as follow

```
RESIST_attack_1 = -(1-rd) * Vn - rf * cost_f * Vn - cost_d * Vn;
RESIST_attack_2 = (1-rd) * Vn - cost_a * Vn;
RESIST_non_attack_1 = -rf * cost_f * Vn - cost_d * Vn;
RESIST_non_attack_2 = 0;
non_RESIST_attack_1 = -Vn;
non_RESIST_attack_2 = Vn - cost_a * Vn;
non_RESIST_non_attack_1 = 0;
non_RESIST_non_attack_2  = 0;
reward matrix[RESIST][ATTACK] = RESIST_attack_1;
reward matrix[RESIST][NON_ATTACK] = RESIST_non_attack_1;
reward matrix[NON_RESIST][ATTACK] = non_RESIST_attack_1;
reward matrix[NON_RESIST][NON_ATTACK] = non_RESIST_non_attack_1;
reward matrix_[RESIST][ATTACK] = RESIST_attack_2;
reward matrix_[RESIST][NON_ATTACK] = RESIST_non_attack_2;
reward matrix_[NON_RESIST][ATTACK] = non_RESIST_attack_2;
rewardmatrix_[NON_RESIST][NON_ATTACK]= non_RESIST_non_attack_2;
```

STEP VI Overall utility function for both player is computed.
STEP VII Attack RESIST case is derived.
STEP VIII. pd_star is calculated from RESIST cost. From pd_star value node is classified as malicious node.

V. RESULTS

From graphs we can see that there are three conditions for simulation scenario without Attacker, without attack detection, with attack detection. Proposed attack detection technique gives the results which are improved than under attack condition & approximate to normal. We can use simulator NS-2.35[13] for simulation.

Performance of RMMPR protocol is measured by varing the parameters in simulation like number of mobile nodes, speed, traffic.

Results by changing number of nodes

The impact of the number of nodes on different performance metrics is depicted from figures 2 to 5. Moreover in each graph, the number of nodes varies from 50 to 100 with all other configurations are fixed.

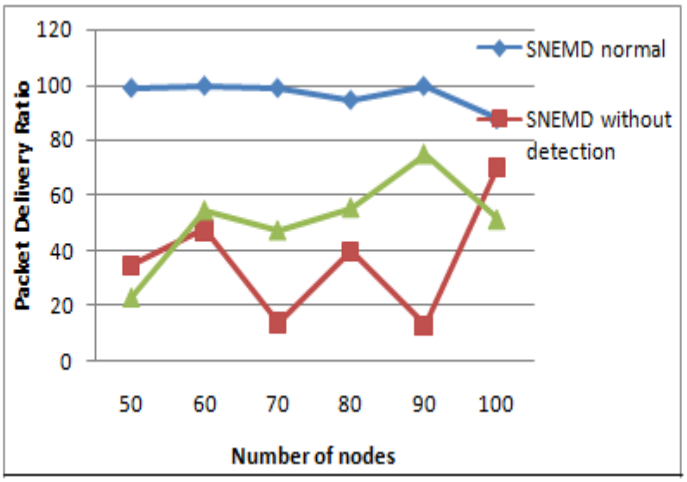

Figure.2 Node vs PDR

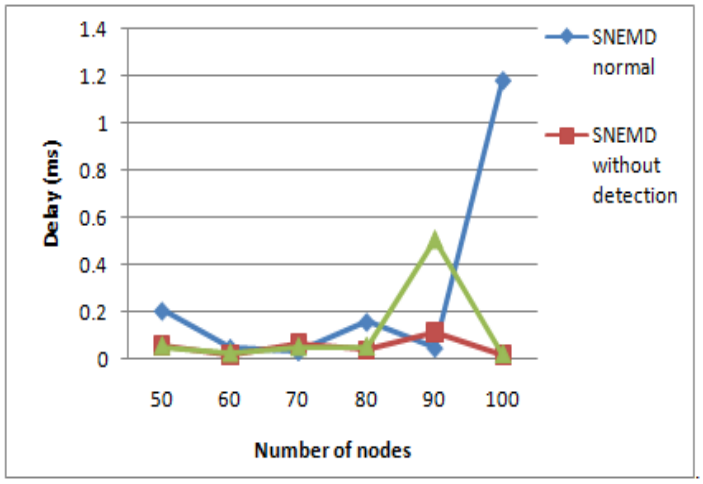

Figure.3 Node vs Delay

Figure 2 demonstrates the impact of the number of nodes on PDR for protocols SNEMD and SNEMD with attack including our solution. The first observation is that, SNEMD with detection protocol has a high PDR as compared to others since it take safer attack free route for data delivery. The second observation is that, SNEMD with attack having very less PDR i.e approximately 40% decrease, since it does not have any mechanism to prevent from data loss. The third observation is that the PDR is high even though number of nodes is increasing.

Figure 3 demonstrates the impact of the number of nodes on end-to-end delay. The first observation is that our protocol has a little bit of more end-to-end delay compared to a safe and attack free route. Therefore this will trade off between packet loss and attack free route. Second Observation is Average End-to-End Delay under attack reduces as the packets are dropping as they are not sent to destination.

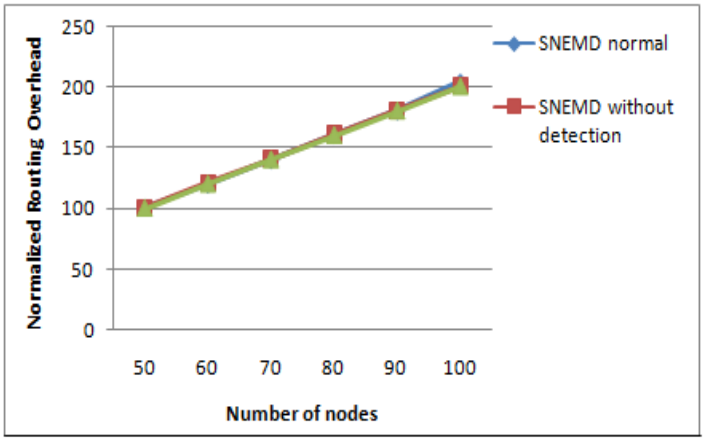

Figure.4 Node vs Normalized Routing Overhead

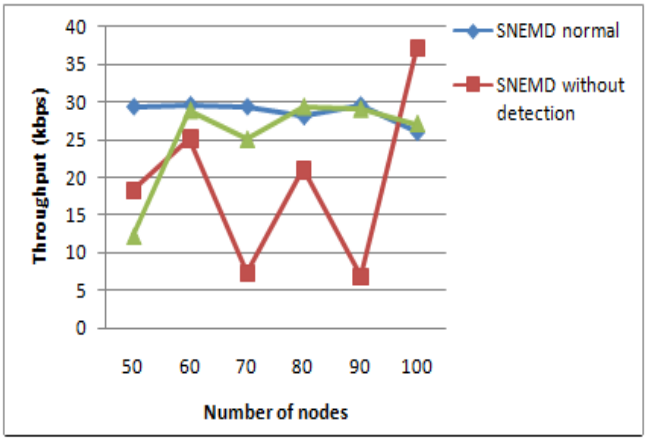

Figure.5 Node vs Throughput

Figure 4 demonstrates the impact of the number of routing overhead. The first observation is that Normalized Routing Overhead is same for all three protocols. The second observation is that as the number of node increases control_overhead also increases due to extra calculation of ra, rf and rd.

Figure 5 demonstrates the impact of number of nodes on throughput. The first observation is that SNEMD with attack protocol suffer a lot from the black hole attacks since this protocol does not have any provision that prevent black hole attack.

Moreover the throughput of SNEMD with attack goes down by 50% regardless of the number of nodes in the network.

Results by changing Speed

The impact of the mobility on different performance metrics is depicted in figures 6 to 9 keeping on all prformance metrics discuss above as unchanged. Moreover in each graph, the mobility varies from 1 to 5 m/s with all other configurations are fixed.

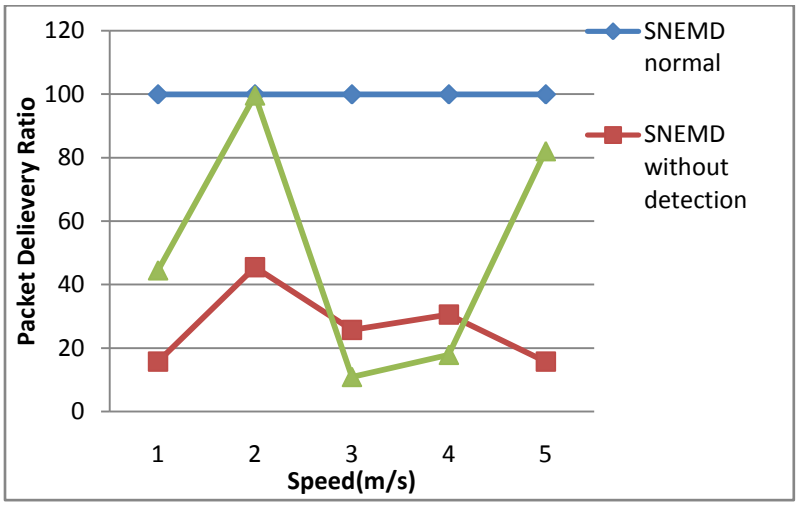

Figure.6 Speed vs PDR

Figure 6 demonstrates the impact of mobility on PDR. Important observation is that the PDR of SNEMD with detection is 30% higher compare to SNEMD without detection. Since it decide secure route before data transmission.

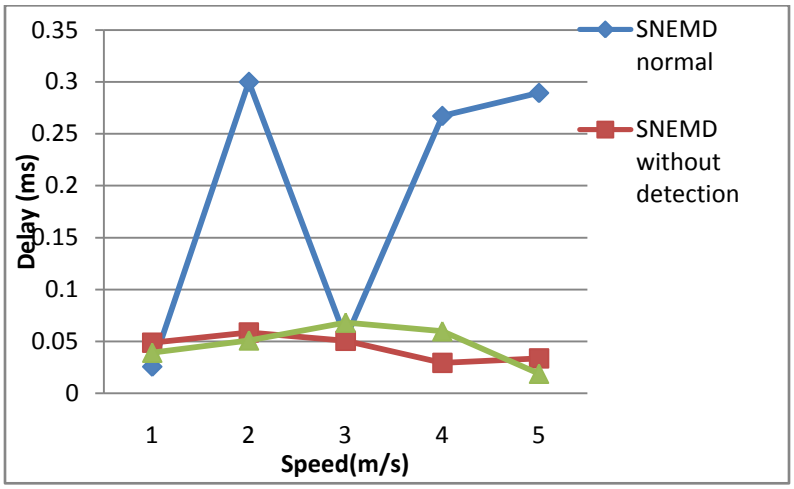

Figure.7 Speed vs Delay

Figure 7 demonstrates the impact of number of nodes on end –to-end delay. Average End-to-End Delay under attack reduces as the packets are dropping as they are not sent to destination. In normal scenario delay is maximum.

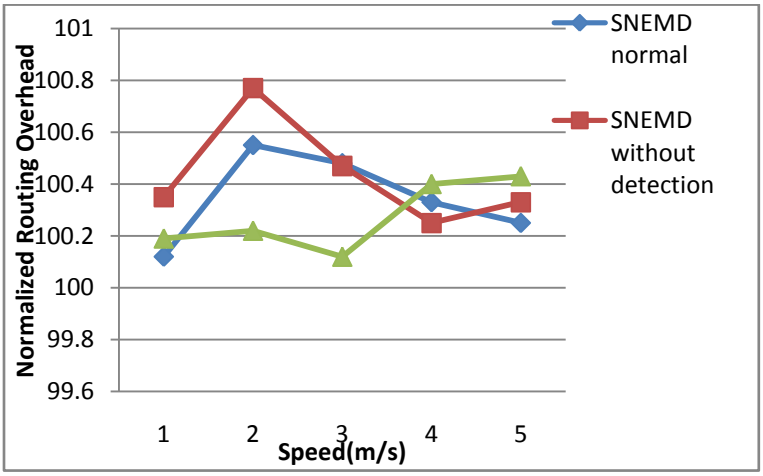

Figure.8 Speed vs Normalized Routing Overhead

Figure 8 demonstrates the impact of the speed on Normalized Routing Overhead. The first observation is that Normalized Routing Overhead decreases for speed 1,2,3 and it increases for speed 4,5 in Attack Detection than normal and under attack scenario.

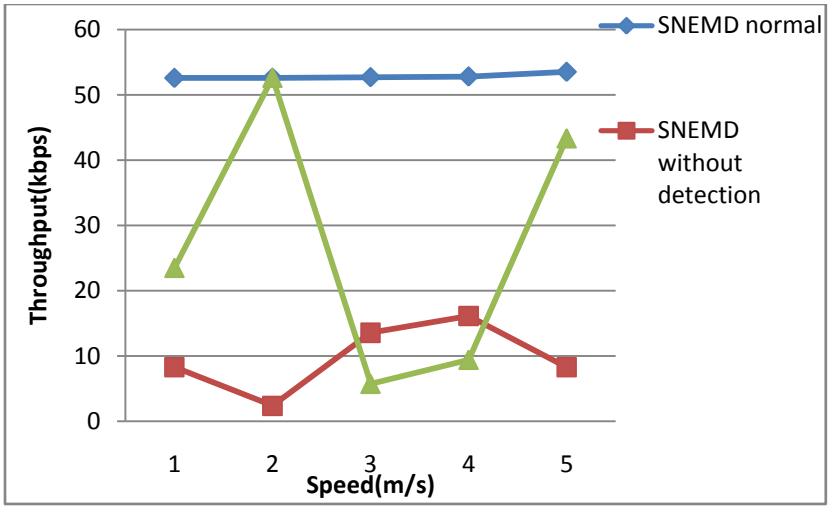

Figure.9 Speed vs Throughput

Figure 9 demonstrates the impact of speed on throughput. First observation is that as the speed increases throughput varies dynamically because density of node changes and more bits are received successfully in attack detection scenario. Second observation is that in normal scenario there is no disturbance in communication so throughput is constant for all cases.

Results by changing Traffic

Total traffic received by the entire network from higher layer which is accepted and queued for transmission. It indicates the quantity of traffic in entire network. It represents the total data traffic in bits per seconds. It does not include any higher layer data traffic rejected without queuing due to large data packet size.

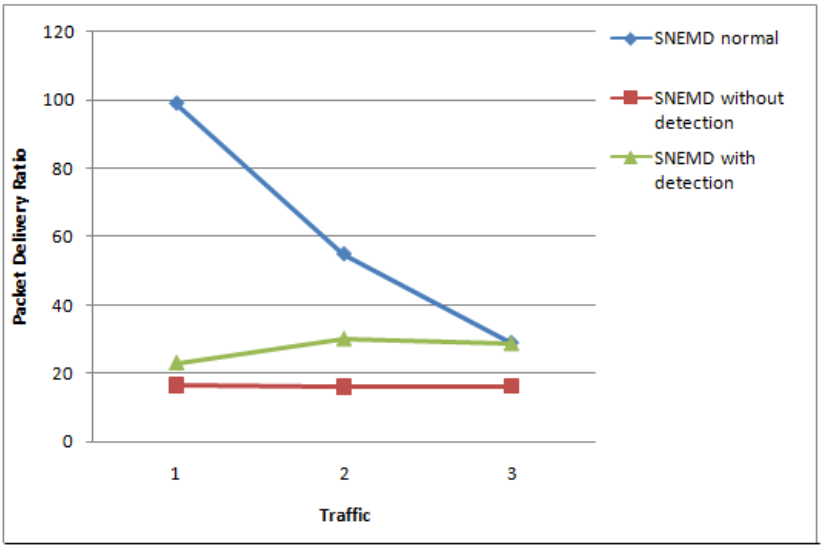

Figure.10 Traffic vs PDR

Figure 10 demonstrates the impact of traffic on packet Delivery ratio. Packet Delivery ratio is improved by 10% in Attack Detection than under attack scenario.

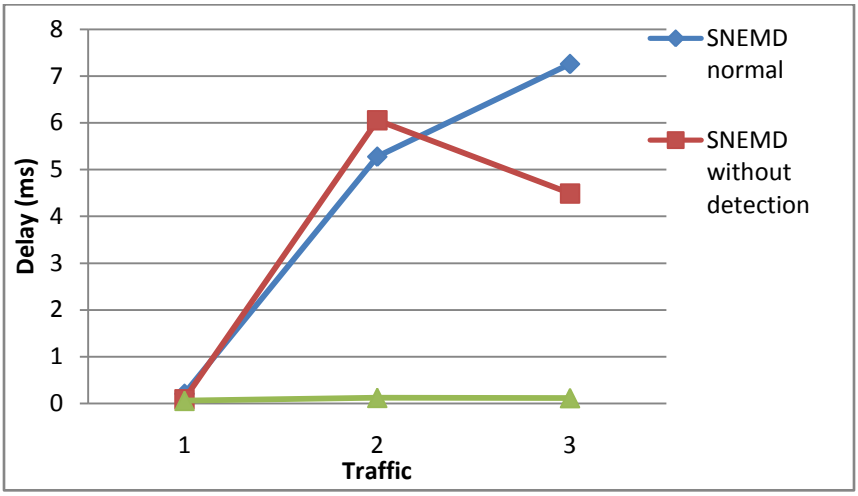

Figure.11 Traffic vs Delay

Figure 11 demonstrates the impact of traffic on average end-to-end delay. Delay decreases drastically in Attack Detection than under attack scenario and normal scenario.

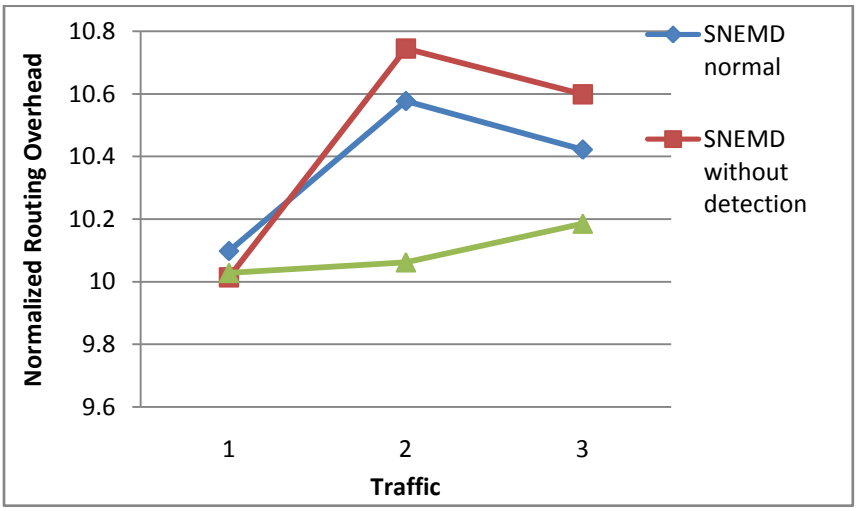

Figure.12 Traffic vs Normalized Routing Overhead

Figure 12 demonstrates the impact of traffic on Normalized Routing Overhead. It decreases in Attack Detection than under attack scenario and it is approximate to normal scenario.

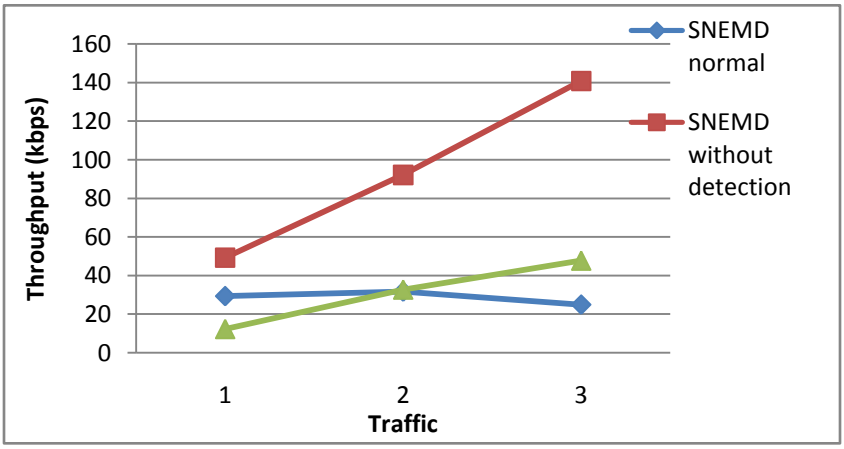

Figure.13 Traffic vs Throughput

Figure 13 demonstrates the impact of traffic on throughput. Throughput decreases in Attack Detection than under attack scenario due to increase in traffic. In our solution as the traffic increases throughput also increases.

V. Conclusion

In modified protocol, proposed approach uses effective way of providing security in RMMP protocol against black hole attack. Proposed mechanism is to detect black hole attack and uses the concept of reward matrix effectively. Proposed mechanism is more efficient due to calculation of attack cost, RESIST cost, false alarm cost. From graphs we can see that there are three conditions for simulation scenario without attacker, without attack detection, with attack detection. Proposed attack detection technique gives the results which are improved than under attack condition & approximate to without attacker nodes. From simulation result we can see the proposed mechanism improves the network performance in terms of packet delivery ratio, Delay, control overhead, throughput.

References

[1] S. M. Metev and V. P. Veiko, *Laser Assisted Microtechnology*, 2nd ed., R. M. Osgood, Jr., Ed. Berlin, Germany: Springer-Verlag, 1998. [1] C .K. Toh, "Ad hoc Mobile Wireless Network: Protocol and Systems", *Prentice Hall ,December 03,2001 Communication and Mobile Computing, Volume 6, Issue 7,pp.969-988, Nov. 2006*

[2] Jeroen Hoebeke, Ingrid Moerman, Bart Dhoedt, Piet Demeester, "An Overview of Mobile Ad Hoc Networks: Applications and Challenges"*Journal of the communication networks,July 2004.*

[3] Emmanouil A. PANAOUSIS and Christos POLITIS "Non-Cooperative Games Between Legitimate Nodes and Malicious Coalitions in MANETs*", IIMC International Information Management Corporation, 2011 ISBN: 978-1-905824-23-6*

[4] Ashok M.Kanthe, Dina Simunic, Ramjee Prasad "A Mechanism for Gray Hole Attack Detection in mobile Ad-hoc Networks", *International Journal of Computer Applicatons Vol.53,No.16, 2012,0975-8887*

[5] Mahesh K. Marina, and Samir R. Das, "Ad Hoc On-Demand Multipath Distance Vector Routing," *Wireless Communication and Mobile Computing, Volume 6, Issue 7,pp.969-988, Nov. 2006*

[6] A. Patcha and J. Park, " A game theoretic formulation for intrusion detection in mobile ad hoc networks," Int. Journ. of Netw. Sec., vol. 2, no. 2, pp. 131–137, 2006.

[7] H. Otrok, N. Mohammed, L. Wang, M. Debbabi, and P. Bhattacharya, "A game theoretic intrusion detection model for mobile ad hoc networks," Comp. Comm.,vol. 31, no. 4, pp. 708 – 721, 2008. Algorithmic and theoretical Aspects of Wireless ad hoc and Sensor Networks.

[8] Y. Liu, C. Comaniciu, and H. Man, " A bayesian game approach for intrusion detection in wireless ad hoc networks," in Proc. GAMENETS, (NY, USA), p. 4, 2006.

[9] Ashok M.Kanthe, Dina Simunic, Marijan Djurek, "Denial of Service (DoS) Attacks in Green Mobile Ad-hoc Networks" ,*MIPRO 2012,IEEE Conference, Proceedings of the 35th International Convention,978-1-4673-2511-6,Opatija,Croatia.*

[10] Elizabeth M.Royer, Santa Barbara, Chai-Keong Toh, "A Review of Current Routing Protocols for Ad Hoc Mobile Wireless Networks", *IEEE Personal Communication ,April 1999.*

[11] P.W.Yau, S.Hu and C.J.Mitchell, "Malicious attacks on ad hoc network routing protocol," *International Journal of Computer research ,15 no.1 (2007) 73-100.*

[12] The network simulator-ns 2.35 http:// www. isi. Edu / nsnam/ns.

