A Secure AdHoc Wireless Clustering Scheme for Improving Security

Basant Kuamr Verma[#1], Dr. Binod Kumar[*2]
[#1]Computer Science & Engineering,
Truba Group of Institute, Bhopal, MP - India
[#1]*contact_basant@rediffmail.com*
[*2] Director
JSPM's Jayawant Technical Campus, Pune, INDIA
[2] *binod.istar.1970@gmail.com*

Abstract—wireless communication is easy to use, rapid implementable and low cost communication technique as compared to the traditional wired communication.Therefore a number of different applications are consumes the wireless communication technology. In wireless ad hoc technology the networks are supporting the mobility and ad hoc configuration of topology development. Therefore the on demand nature of routing is much helpful. Such kind of networks are suffers from the performance and security issues. Therefore the given paper addresses the key security issues and a solution is redesigned to incorporate the security solutions. This method utilizes the weighted clustering algorithm for demonstrating the security solution and the performance issues. In addition of that the implementation strategy and the obtained outcomes of the proposed secure weighted clustering algorithm is also provided.

Keywords— *wireless ad hoc networks, routing algorithm, weighted clustering algorithm, security implementation, results analysis.*

*****

I. INTRODUCTION

The wireless technology is growing rapidly and a number of variants are enclosed with the progress of network such as wireless sensor networks, mobile ad hoc networks and others. These technologies are enabling a network user to access the network services when they are mobile. The use mobility in network devices are makes it more essential for different applications. But during the mobility the data transmission and the connectivity is the major problem in such networks. In addition of these performance issues the malicious user can be join the network without any prior information [1]. In this work the security and performance of network are targeted to find an optimal solution.

During the literature collection a number of research articles are studied and that is concluded. The security and performance can be regulated using the routing strategy [2]. Basically the routing protocols are responsible for route discovery, joining of nodes in a path and route maintenance [3]. Therefore most of the attackers are utilizing the routing information for deploying the attacks in network. Therefore in this presented paper a clustering technique is proposed to optimize the performance and the security of network. The proposed cluster based routing technique is based on the concept of quality of service parameters to construct the clusters.

This section provides a general overview of the proposed concept and their basic need for design.In the further sections the proposed algorithm, implementation environment and the obtained results are demonstrated.

II. BACKGROUND

This section reports the proposed work and the algorithm which is used for implementation.The main objective of the proposed work is to develop more stable and efficient cluster head selection algorithm by which the performance of network is significantly increases and security constrains are implementable. Therefore the modular development strategy is presented in this section.

A. Node Quality

In order to find the stable and more efficient network cluster the following solutions are suggested to implement.

1. **Energy:** the node which having higher remain battery power having long life and able to participate in communication [4].
2. **Connectivity:** Maximum numbers of nodes are in connected through this node causes the more serving capability.
3. **Buffer length:** buffer length demonstrate the low load on node, therefore less loaded node can serve better [5].
4. **Mobility:** low mobile nodes are able to form more stable clusters [6].

B. Clustering Algorithm

In this section proposed clustering approach are discussed in detail. The proposed WCA algorithm that includefresh route information is described in two different modules first the primary calculation and secondly the cluster head selection.

Weight Calculation Algorithm

1. For each node in network
2. Find remain energy E
3. Find mobility using

$$M = \frac{1}{T}\sum_{i=1}^{T}\sqrt{(X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2}$$

4. find buffer remain for all nodes as B
5. find number of neighbour nodes as C

6. calculate the weights

$$W = w_1 * c + w_2 * e + w_3 * M + w_4 * d$$

Cluster Head Selection Algorithm

1. Find the memory, buffer, connectivity and mobility for each node
2. Find weights for all the nodes
3. For each node in network
4. If node weight is maximum than
    a. cl-head =1
5. Else
    a. cl-head=0
6. End if
7. End for
8. Broad cast the massage to neighbour nodes where cl-head=1
9. Mobile nodes
10. Determine new role of nodes
11. Repeat process to step 1

C. Security Integration

In this section the layered detection and removal of different kinds of targeted attacks are provided. More specifically black hole [7], wormhole [8], DDOS [9] and the Grayhole attack [10]. During security integration first the entire network nodes are evaluated on the basis of their number of request broadcasts. Thus using the previous sessions the broadcasting threshold is prepared. That can be evaluated using the given formula.

$$B_t = \sum_{i=1}^{S} RREQ\ broadcast_i$$

Where B_t the broadcasting threshold for decision making and the S is the number of historical sessions analysed. And $RREQ\ broadcast_i$ is the number of connectivity request of node I.

The estimated threshold is used to remove the DDOS floodingbased malicious attacker in network. thus if at the time of receiving request from another node if any node send RREQ packets more than estimated threshold than add these nodes to blacklist and do not receive any request from this node. After implementing the desired first phase security checks the nodes are evaluated for the further malicious node detection for wormhole.

Thus the following procedure is utilized to detect and prevent an attacker in ad hoc network.

1. Source node S broadcast RREQ for route discovery and store sending time t
2. If S receive RREP form destination then capture time t'
3. S calculate $Att = t' - t$
4. If $Att \geq 6 * NodeTT$
5. Nodes may be malicious;
6. Run algorithm 2.
7. Else
8. S considers the route among source and destination is safe and sends data.
9. End if

In above given algorithm steps the NodeTTis the maximum expected wireless propagation latency on a single hop [11]. The second algorithm consumes the DH algorithm for cryptographic solution of the secure data transmission and remaining node identification for Grayhole, Black hole and Wormhole detection.

Now when the route contains the malicious nodes than the cryptographic technique is utilized for secure data transmission and therefore Diffie–Hellman key exchange technique [12] is utilized for securing the communication and prevention of targeted attack.That is a specific method of securely exchanging cryptographic keys over a public network. D–H is one of the earliest practical examples of public key exchange implemented within the field of cryptography. The Diffie–Hellman key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communication channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher. And the second algorithm for identifying the attacker is taken place in the following manner.

1. Sender sends dummy packets
2. For five dummy packets
3. Send encrypted packet by using sender key
4. Wait for 6*NodeTT
5. If send get RREP from other route
6. If time of receiving and sending vary by number of hops
7. Node is malicious wormhole attack detected
8. Add in blacklist
9. Else if get reply = 0
10. Black-hole attack detected
11. Else if get reply <= 3
12. Grayhole attack detected
13. End if
14. End if
15. End for

After locating the entire attackers in network the network becomes secure and trustworthy thus the proposed secure cryptographic weighted clustering scheme for secure communication is prepared.

III. IMPLEMENTATION

 ISSN: 2321-8169
1035 - 1041

The implementation of the proposed system is provided using the NS2 network simulation tool. That is a discrete event simulator used for real world simulation of network and their communication. This section includes the simulation environment and desired network scenarios.

A. network setup

In order to simulate the effectiveness of the proposed attack analyses following network parameters are setting up for network simulation.

Simulation properties	Values
Antenna model	Omni Antenna
Dimension	750 X 550
Radio-propagation	Two Ray Ground
Channel Type	Wireless Channel
No of Mobile Nodes	20, 40, 60, 80, 100
Routing protocol	AODV
Time of simulation	10.0 Sec.

Table 1 simulation setup

B. simulation scenario

To implement and properly simulate the effectiveness of the proposed secure cluster routing technique the following network scenarios are prepared.

1. Simulation of normal network under attack: in this simulation scenario the network is configured using the AODV routing protocol and the different attacks namely black-hole, wormhole, Grayhole and DOS attacks are deployed. After attack deployment the network performance is measured and simulated.

2. Simulation of proposed network under attack:in this phase of simulation development the routing is configured with the proposed modification in AODV routing protocol and the similar attacks are deployed in network. After attack deployment the network performance is measured and compared with the previously implemented scenario.

The next section provides the results and comparative performance study.

IV RESULTS ANALYSIS

This section provides the performed experiments and the results analysis of the implemented secure network. The performance evaluation of the proposed technique is given in terms of various performance parameters those are listed as:

A. end to end delay

The end to end delay in network demonstrates the time delay for propagating the data from one end to other. The figure 1 shows the performance of network under black-hole attack

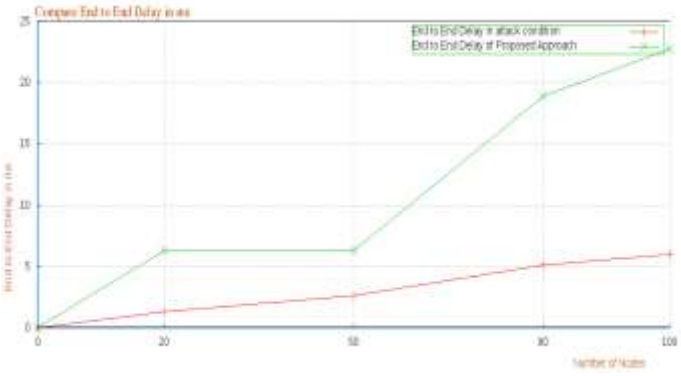

Figure 1 black-hole end to end delay

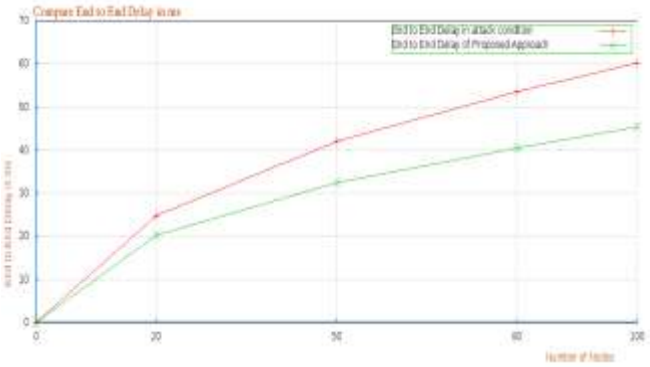

Figure 2 DOS end to end delay

The figure 2 shows the performance of both networks under dos attack deployment. In the same way the figure 3 and 4 shows the performance of networks under Grayhole and wormhole attack.

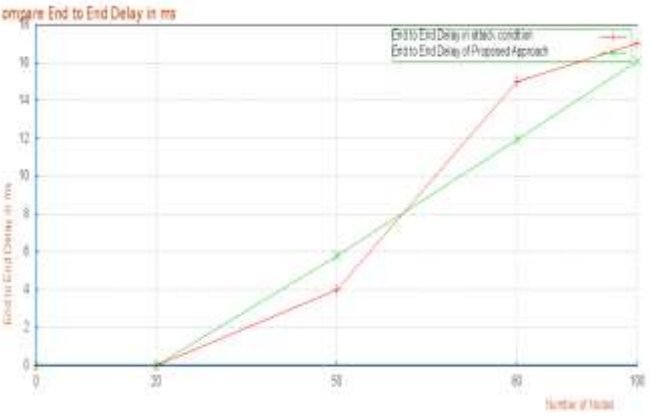

Figure 3 Grayhole end to end delay

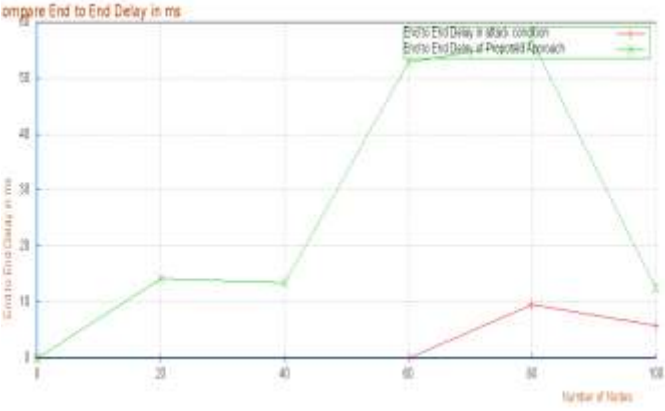

Figure 4 wormhole end to end delay

 ISSN: 2321-8169
1035 - 1041

In order to represent the performance of both the network the green line shows the performance of proposed approach and the red line shows the performance of traditional network. In these diagrams the X axis shows the number of nodes in network during experimentations and the Y axis shows the end to end delay in terms of milliseconds.

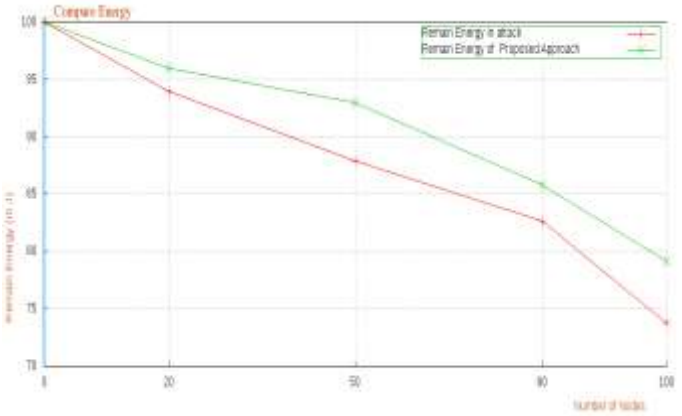

Figure 5 energy black-hole

According to the evaluated results during the attack conditions thus the average end to end delay of network is found optimum and increases when the traffic in network is increases in high number of nodes.

B. Energy consumption

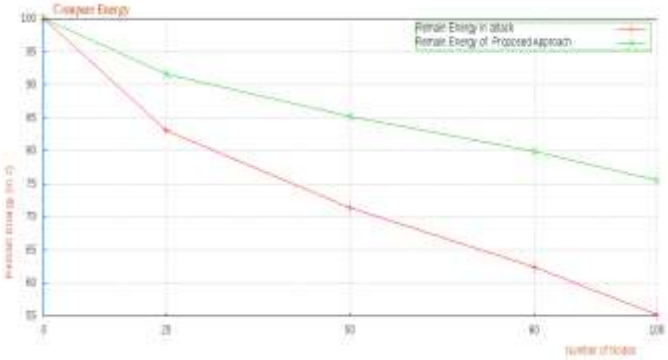

Figure 6 energy drop DOS attack

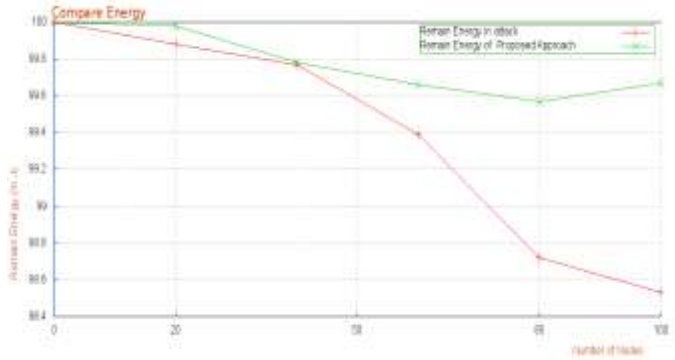

Figure 7 energy drop Grayhole attack

To simulate the performance of the network the X axis contains the number of nodes in increasing order and the Y axis shows the percentage energy drop during attack. According to the obtained results the performance of the proposed technique is much efficient in terms of energy consumption as compared to normal AODV routing protocol.

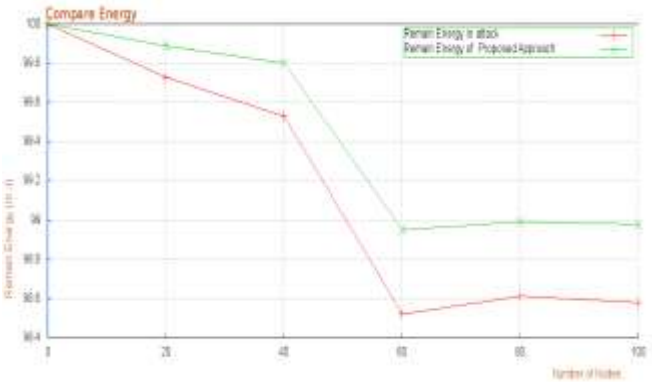

Figure 8 energy drop wormhole

C. packet delivery ratio

Packet delivery ratio provides information about the performance of any routing protocols, where PDR is estimated using the formula given

$$packet\ delivery\ ratio = \frac{total\ delivered\ packets}{total\ sent\ packets}$$

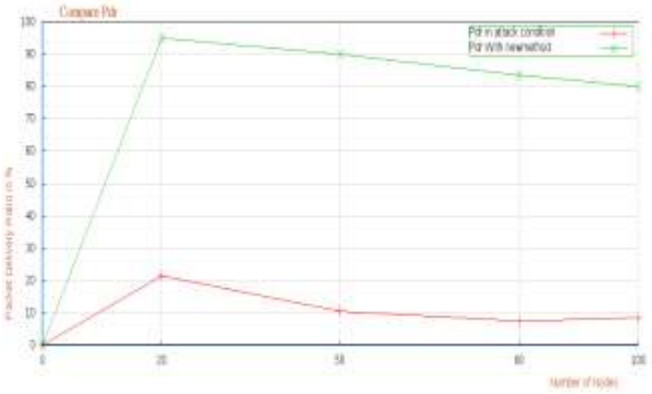

Figure 9 PDR black-hole attack

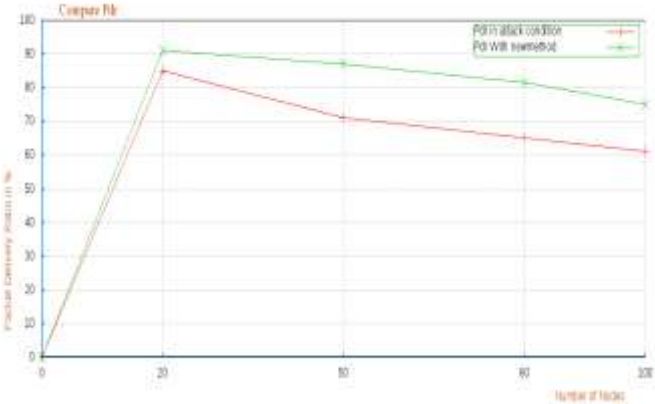

Figure 10 DOS packet delivery ratio

The packet delivery ratio of the network demonstrates the rate of data which is delivered to the target system. Figure 9, 10, 11, and 12 shows the performance of both the networks in terms of packet delivery ratio. According to theobtained results the packet delivery ratio of the network is affected in normal network conditions in addition of that the performance of the proposed network model is remain constant during the attack conditions.

ISSN: 2321-8169
1035 - 1041

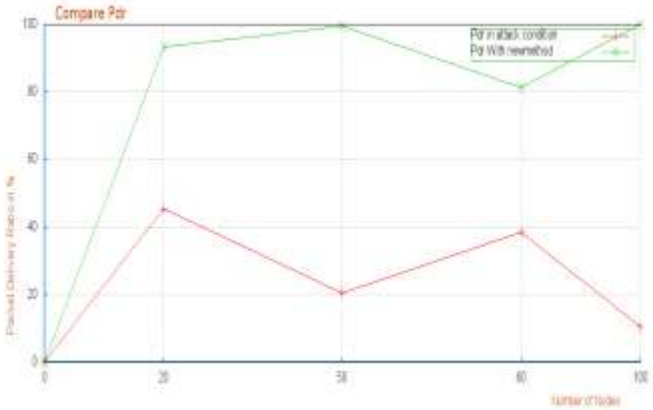

Figure 11 Grayhole packet delivery ratio

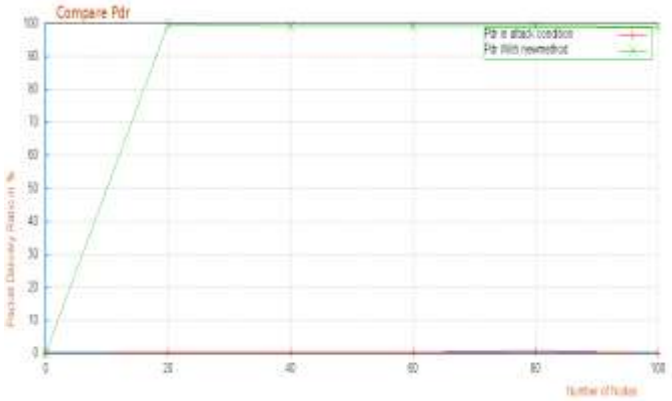

Figure 12 Packet delivery ratio wormhole

D. Routing overhead

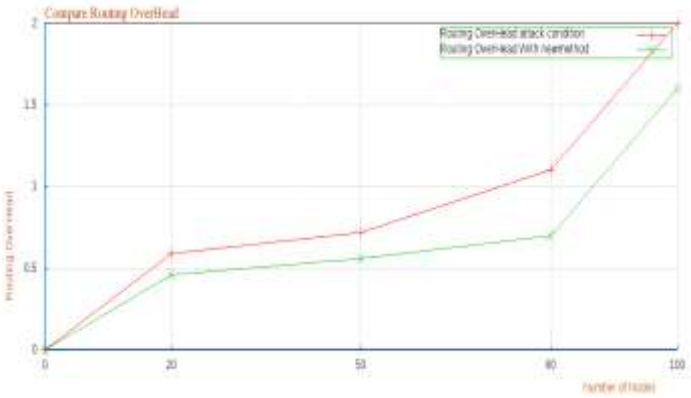

Figure 13 routing overhead black-hole

The amount of additional packets injected in network is known as routing overhead. The performance of both the network under attack conditions are simulated using figure 13, 14, 15 and 16. According to the obtained results the proposed cluster based routing technique added less amount of the routing overhead as compared to the traditional technique of routing.

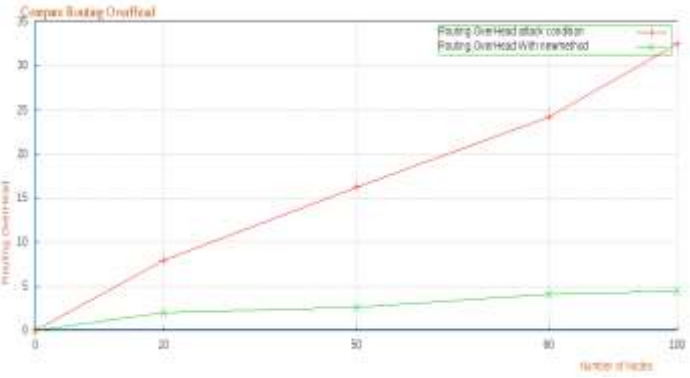

Figure 14 routing overhead DOS

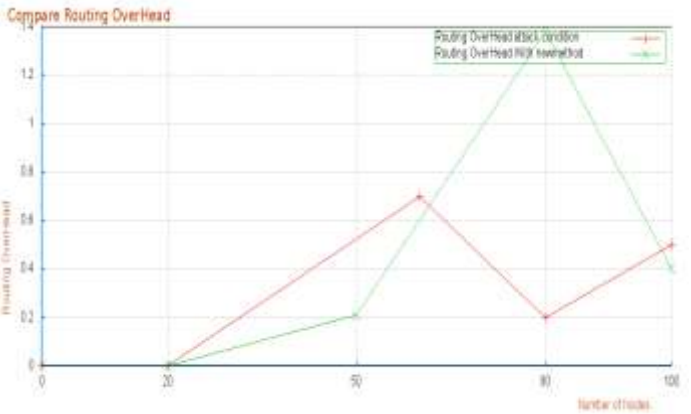

Figure 15 routing overhead Grayhole attack

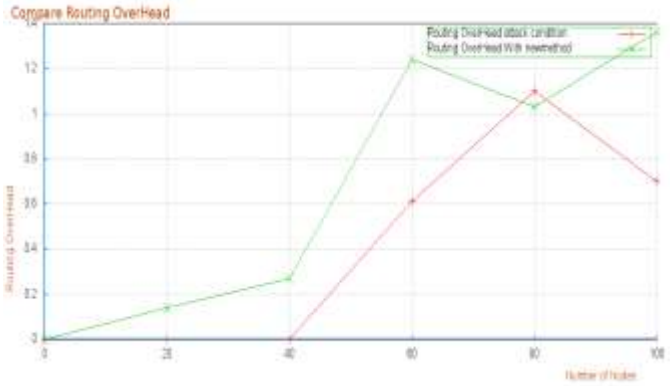

Figure 16 routing overhead wormhole attack

E. Throughput

Network throughput is the usual rate of successful delivery of a message over a communication medium. This data may be transmit over a physical or logical link, or pass by a certain network node. The throughput is calculated in terms of bit/s or bps, and occasionally in terms of data packets per time slot or data packets per second.

ISSN: 2321-8169
1035 - 1041

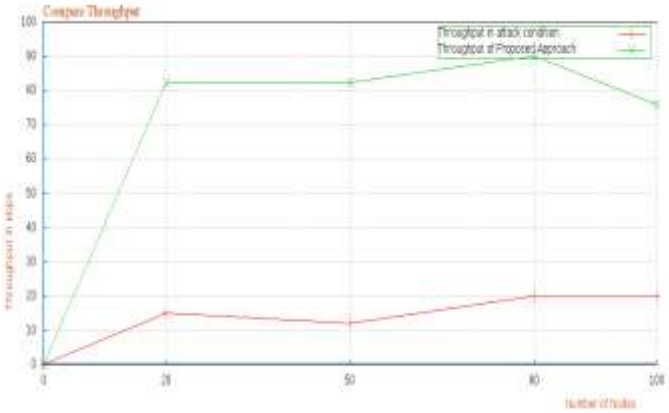

Figure 17 throughput black hole attack

The performances of both the network scenarios are given using figure 17, 18, 19 and 20. In these diagrams the available bandwidth for the proposed routing technique is found optimum as compared to the traditional routing technique. for representing the performance the X axis of diagram demonstrates the number of nodes in network and the Y axis shows the performance in terms of KBPS.

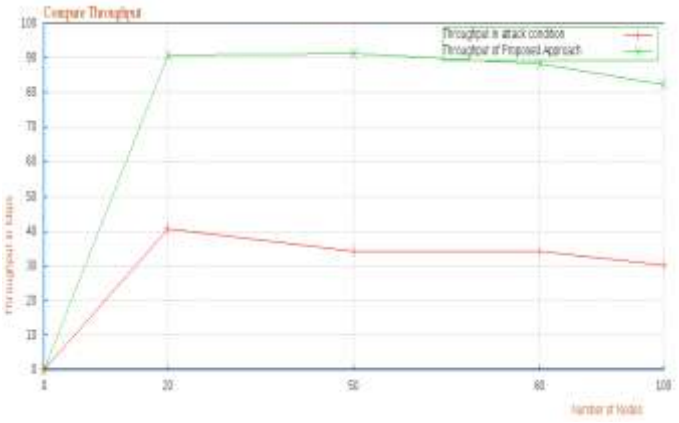

Figure 18 throughput DOS attack

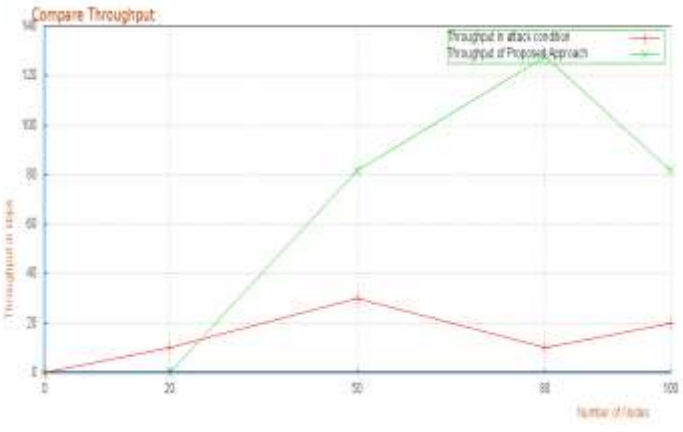

Figure 19 throughput Grayhole attack

This section demonstrates the comparative performance study of the proposed routing model and the traditional routing technique. According to the obtained technique the performance of the proposed routing is optimum and the next section provides the conclusion of the entire study.

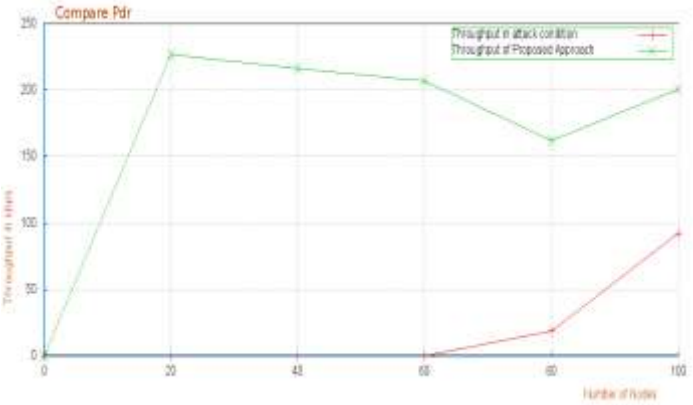

Figure 20 throughput wormhole attack

V. CONCLUSION AND FUTURE WORK

The wireless ad networks and their applications are growing rapidly. Therefore the improvement in their security and performance is a primary concern in this domain. During the literature collection and investigation there are a number of techniques are available for securing network or optimizing the performance of network in terms of a defined parameter. Therefore an efficient and secure communication technique is required to design for providing security and performance both. Thus in this presented work the traditional weighted clustering scheme is extended for optimizing the performance and security. The presented security algorithm is implemented with the help of network simulator 2 environment and their performance is compared with the traditional routing algorithm under attack conditions. The results demonstrate the performance of network is efficient and able to secure the network in different kinds of attack.

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for MobileAd-Hoc NETworks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013

[2] Aarti, Dr. S. S. Tyagi, "Study of MANET: Characteristics, Challenges, Applicationand Security Attacks",International Journal of Advanced Research in Computer Science and Software Engineering,Volume 3, Issue 5, May 2013

[3] DeepaliRaut,KapilHande, "Performance analysis and Prevention of Gray Hole andBlack Hole Attack in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 7, July 2014

[4] AnmolSuryavanshi,NiteshRastogi, "Improving Packet Transmission Rate of Ad hoc Network byBattery Power Awareness", International Journal of Advanced Research inComputer Science and Software Engineering,Volume 4, Issue 3, March 2014

[5] Chai KeongToh, Anh-Ngoc Le and You-Ze Cho, "Load Balanced Routing Protocols for Ad Hoc Mobile Wireless Networks", 0163-6804/09/$25.00 © 2009 IEEE IEEE Communications Magazine August 2009

[6] Ajay PrakashRai, PreetiShakya, VineetSrivastava, Anurag Gupta, PrashantKhare, "Effect of Mobility Models on the performance of Proactive and Reactive Routing Protocols", International Journal of Engineering and Innovative Technology (IJEIT) Volume 3, Issue 12, June 2014

[7] EiEiKhin, ThandarPhyu, "Comparative Analysis of Black Hole Attack Solutions in AODV Protocol", International Journal of

Computer & Communication Engineering Research (IJCCER) Volume 1 - Issue 2 July 2013

[8] Shiva Shamaei, and Ali Movaghar, "A Two-Phase Wormhole Attack Detection Scheme in MANETs", July 2014, Volume 6, Number 2 (pp. 183–191)

[9] MeghnaChhabra and B.B. Gupta, "An Efficient Scheme to Prevent DDoS Flooding Attacks in Mobile Ad-HocNetwork (MANET)", Research Journal of Applied Sciences, Engineering and Technology 7(10): 2033-2039, 2014

[10] JaspreetKaur, Vinod Kumar, "An Effectual Defense Method against Gray Hole Attack in Wireless Sensor Networks", International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4523-4528

[11] Emmanouil A. Panaousis, LevonNazaryan, Christos Politis, "Securing AODV Against Wormhole Attacks in Emergency MANET Multimedia Communications", Mobimedia'09, September 7-9, 2009, London, UK. Copyright 2009 ICST 978-963-9799-62-2/00/0004

[12] PoojaKolte, ReshmaGutal,PriyankaBhairat, "An Efficient Password Security Mechanism Using Two ServerAuthentication and Key Exchange", International Journal of Advance Research inComputer Science and Management Studies, Volume 3, Issue 1, January 2015