VOL. 11, NO. 21, NOVEMBER 2016 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences
©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.
www.arpnjournals.com

A SECURE MULTICAST ROUTING PROTOCOL AGAINST GREY HOLE ATTACK

Geetanjali Rathee and Hemraj Saini
Department of Computer Science and Engineering and Information Technology, Jaypee University of Information Technology Waknaghat, Solan, Himachal Pradesh, India
E-Mail: geetanjali.rathee123@gmail.com

ABSTRACT

Security in multicast routing is one of a key challenge area in mesh networks because of its broadcasting and dynamic nature. Several multicast routing protocols have been proposed by different researchers but leads to certain parametric issues (i.e. packet delivery ratio, throughput and various security concerns) because of unique characteristics of mesh. The aim of this manuscript is to propose a secure multicast routing protocol for Wireless Mesh Network based on link state quality to identify and recover from routing attacks. The proposed mechanism ensure the security against grey hole attack which would be identified by calculating the packet delivery percentage of each node where the node having less packet delivery percentage than predefined threshold value (i.e. 95%) is considered as grey hole affected node. Further, to recover against grey hole attack, a 2-hop preceding node phenomenon is used which immediately select another path to re-route the data packets. The proposed routing mechanism is analysed over NS2 simulator beside different network metrics over static and dynamic environments having scalable network sizes.

Keywords: grey hole attack, multicasting, routing protocols, packet delivery percentage.

1. INTRODUCTION

Wireless Mesh Network (WMN) is considered as a next generation key technology and has gained a substantial prominence in research community due to its self-healing and self-organizing characteristics [1, 2]. As depicted in Figure-1, Mesh Routers and Mesh Clients are two different components of mesh technology. Mesh Routers offer multi-hop connectivity and acts as internet backbone to connect the access points while Mesh Clients are the devices who access the internet services via mesh routers. Because of dynamic and broadcasting nature of WMNs where nodes are free to mobile from one domain to another domain, the most important factor that impacts the network performance is the nature of fundamental routing process [3-5].

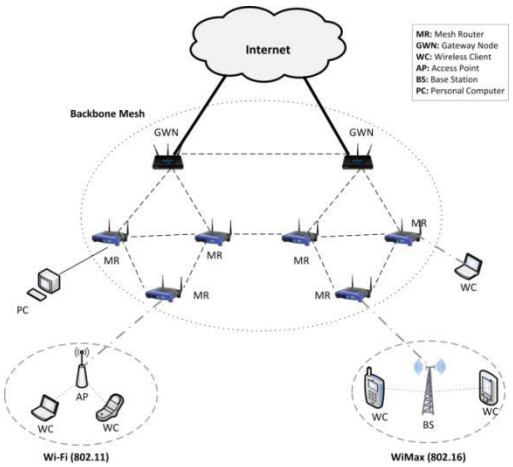

Figure-1. Wireless mesh network.

To provide a communication among the entities, routing process plays a significant role and is considered as the current topic of research in today's era. In business communities where data is transmitted to multiple destinations through a single source, multicast routing came into existence. Multicast routing is the one where data is delivered to multiple destinations through a single entity. The Successful delivery of data packets to the anticipated destinations depends upon generous nature of routing nodes [6]. Presence of any malevolent node within routing process may disrupt the network activities and invite a number of security vulnerabilities to come [7-9]. Further, any node/link failure within the routed path may drastically affect the network throughput. Although a number of techniques have been proposed by several researchers for MANETs and WSNs [10-12], but these techniques can't be adopted well in mesh environments because of its unique nature. Hence, there is a need to establish a routing mechanism which identifies misbehaving nodes in the routing process to securely transfer and to re-route the data packets during failures to their intended destination nodes [13-14].

The aim of this manuscript is to propose a multicast link state routing protocol which is resilient against grey hole attack and recover during node/link failure. Grey hole attack is considered as most dangerous attack in routing process because it selectively drop the data packets and difficult to identify in the beginning and drastically affect the network performance. The proposed protocol uses the concept of link quality which is measured by sending the periodic probes to their neighbouring nodes. The technical contribution of this paper is as follows:

- A link state quality and two-hop proceeding node phenomenon is used to route and recover the data packets during threat and node/link failure.
- Packet delivery percentage is used to identify the grey hole affected node in the routing process.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

- The network performance is measured against various metrics over static and dynamic environments in small and large network sizes.

The remaining structure of the paper is organized as follows. A literature survey of various multicast routing protocols is briefed in section 2. The proposed Secure Multicast Protocol (i.e. SMP) is discussed in section 3. Section 4 evaluates the performance of SMP over certain metrics and finally section 5 concludes the paper.

2. RELATED WORK

Although a number of researchers have proposed several secure multicast routing protocols but existing techniques imply a reduction in security process and strongly affect the network performance because of its additional communication process [15]. Hop count and link quality are the two basic methods to transmit the multicast data to destination nodes. The route selection in hop count is chosen against the path having minimum hop count but the drawback of this method is poor link quality used to transmit the data packets [16, 17]. Further the routes are selected on the basis of highest link quality in which the link quality is measured by sending the periodic probes to their neighbouring nodes. ODMRP [18], ODMRP link quality [19] and S-ODMRP [20] are the mesh based multicast protocols where multicast routes are selected and packets are transmitted through selected paths. The main focus of these protocols is to provide a high throughput metric.

ODMRP is an on-demand multicast routing protocol which uses a mesh of nodes for each multicast group. In this, the source node periodically updates the membership information by recreating the JOIN QUERY in the network. Although the protocol is resilient against data paths but is vulnerable against redundant re-transmission overheads. Further *ODMRP Link Quality* is the extended version of ODMRP where each node has a neighbouring table having the cost of their neighbour to it-self which is nothing but a probability value. In this, whenever a JOIN QUERY is received by a receiver with the cost of total path travelled by it, receiver node waits for't' period of time and compares the cost of multiple JOIN QUERY costs. The JOIN QUERY message having high link quality would be selected as the best path route.The major limitation with this approach is the waiting time. The QUERY REPLY will be sent back only after setting all JOIN QUERY requests. In addition to this, *S-ODMRP,* a secure ODMRP protocol is used where join query messages are signed by the source node and is propagated through weighted flood suppression approach. The nodes having signed signature along with the JOIN QUERY message are allowed to process.

Although the above discussed approaches are able to multicast the data packets using multiple methods but all these approaches are vulnerable against several security attacks i.e. black hole, worm hole and grey hole attacks in which attacker's aim is to reduce the network throughput by disrupting the data packets. So, the aim of this manuscript is to overcome the mentioned limitation and highlights some improvements in output results.

3. PROPOSED WORK

This section deliberates a secure and fault tolerant routing mechanism which is resilient against grey hole attack. A high throughput multicast routing protocol HT-ODMRP is used which selects the path using link quality concept.

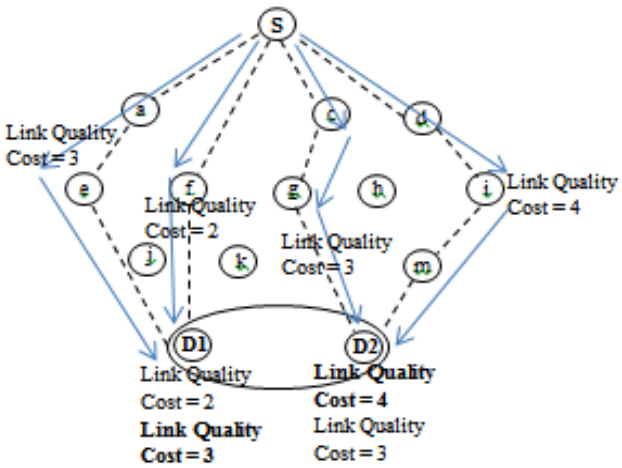

Figure-2. Multicast routing.

HT-ODMRP is similar to ODMRP but instead of using hop count field for route selection, a link quality criterion is used. Link quality is measured by sending the periodic probes to their neighbouring nodes, the path having the highest link quality would be considered as the best routed path. As depicted in Figure-2, there exist two different paths to send the data packets between S-D1 and S-D2.

Table-1. The path evaluation of HT-ODMRP.

{S-D} pair/Path	Path 1	Link quality of path 1	Path 2	Link quality of path 2
{S-D1}	S-a-e-D1	2	S-f-D1	3
{S-D2}	S-c-g-D2	4	S-d-i-m-D2	3

According to Table-1, S-a-e-D1, S-f-D1 path for S-D1 and S-c-g-D2, S-d-i-m-D2 path for S-D2 are selected as two routing paths. Let us consider the link quality for path S-a-e-D1 is 2 and S-f-D1 is 3 likewise S-c-g-D2 and S-d-i-m-D2 is 4 and 3 respectively. According to HT-ODMRP, the route having highest link quality would be selected as the best path, so the packets would be routed through S-f-D1 in case of S-D1 and S-c-g-D2 path for S-

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

D2. Further in case of any node or link failure, the second highest link quality cost path (i.e. S-f-D1 for S-D1 and S-d-i-m-D2 for S-D2) would be selected for packet transmission as depicted in Figure-3. The below mentioned scenarios highlights the proposed mechanism to identify and recover from grey hole attack.

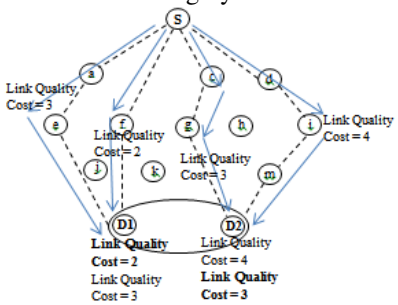

Figure-3. Routing against node/link failure.

3.1 Scenario 1: Attack identification by calculating the percentage of Packet Delivery (% of PD)

The HT-ODMRP protocol is enhanced by incorporating the packet delivery percentage (% of PD) of each node to detect grey hole attack as depicted in eq. 1. Each node 'x' calculates the Packet Delivery (PD) percentage of its preceding node and should satisfy the following condition i.e. 95% <=x<=100% to forward the data packets. The node having PD percentage less than 95% would be considered as malicious node. The current node $'x_c'$ will immediately send an alarm message to its 2-hop preceding node to re-route the data packets. The formula for identifying the packet delivery of a node 'x' is given as:

$$PD_x = Number\ of\ Packets_{received} - Number\ of\ Packets_{Transmiited} \begin{cases} if\ 95\% \le x \le 100\%, \\ \quad Idle\ node \\ else\ if \\ \quad x < 94\%, \\ \quad Attacker\ Node \end{cases} \quad (1)$$

Scenario 2 discusses the case of re-routing the data packets when a node is affected by grey hole attack in the selected routed path.

3.2 Scenario 2: Re-routing of packets during from a grey hole affected node

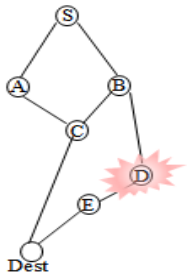

Figure-4. Routing against grey hole attack.

A single destination node is selected to clearly understand the path recovery process during grey hole attack. Let us consider a scenario as depicted in Figure-4, where 'S' is the source node, $Dest$ is the destination node and $A, B, C, D\ and\ E$ are the intermediate nodes. Let node is 'E' is a grey hole node which selectively forwards the incoming data packets from its preceding node.

Let the source node 'S' sends 50 packets to transmit to destination node $Dest$ through $S-B-D-S-Dest$ path using link quality mechanism. As node 'D' is a grey holeaffected node, so the number of packets sends by node 'D' would be less than expected delivery ratio. The PD % of routing path at each node is depicted in Table-2.

As node 'E' calculates the PD % of node 'D' which is less than 95%, so immediately node 'E' sends an alarm message to its 2-hop preceding node i.e. node 'B' to re-route the data packets through some other path. Node 'B' will immediately change the routed path and send the data through $B-C-Dest$ path.

The same phenomenon is to be used in multicasting where a single source sends the message to multiple destinations. An algorithm for successful packet transmission for single destination is depicted in Table-3.

Table-2. Packet delivery percentage of each node in routing path.

Node	Receive	Transmit	PD%
	$PD_x = (Packets_{received} - Packets_{transmited})$, where 95% <= x <= 100%		
S	-	50	100%
B	50	50	100%
D	50	35	<=95%

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

Table-3. The successful packet transmission through SMP routing protocol.

Input: Source node 'S' wants to transmit the packets to destination node Dest *Output:* Packets are successfully reaches to destination node
Assumption: if ($95\% \leq PD_x \leq 100\%$) Node is idle and able to forward the data packets Else Node is grey hole affected node
Procedure: Step 1. Network N consist of x_i number of nodes where x=1,2,…n Step 2. **If**(source node 'S' wants to forward the packets to destination node 'Dest') *In ideal case where there exist no link/node failure during packet transmission* 'S' selects the highest link quality path to route the data packets For each (x=1; x<=n; x++) Calculate PD % using $PD_x = packets_{received} - packets_{transmitted}$ **If** ($95\% \leq PD_x \leq 100\%$) Then Go to Step 3 **Else if** Go to Step 4 **End else if** **End if** **Else** *During any node/link failure* Second highest link quality path will be selected **End else** **End if** Step 3. Node is idle and able to forward the data packets Step 4. Node is grey hole affected node and the succeeding node will send an alarm message to its 2-hop preceding node to re-route the data packets through another path.

4. PERFORMANCE EVALUATION

The SMP protocol is simulated over NS2 simulator and the performance results are analysed against certain parameters. The simulation environment sets over the network is shown in Table-4 and the parametric values considered for result analysis are discussed below.

Table-4. The simulation parameters of proposed mechanism.

Parameters	Size
Number of nodes	10-70 (small), 150-700 (large) network size
Area size	400*400
MAC	802.11
Routing Protocol	AODV
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Attacker	4,6,10, 15, 20,25
Antenna	Omni Antenna

- **Throughput:** It is defined as total number of packets successfully reaches to the destination node at a given period of time.

  $Throughput = \sum_{i=1}^{n} \frac{Totalnumberofpackets}{T_{tdp} - T_{rdp}}$, where T_{tdp} are the transmitted data packets and T_{rdp} are received data packets.

- **Packet Delivery Ratio (PDR):** PDR is defined as the ratio of received data packets to generated data packets.

$$PDR = \frac{ReceivedDataPacket}{GeneratedDataPacket}$$

- **End to end delay***:* The time taken by all the data packets successfully reaches to its destination node.
- **Security attack:** The security is measured against packet loss ratio where number of packets loses during transmission after existence of a grey hole attack.

All the mentioned parameters are discussed against static and mobile environments.

4.1Results and discussions

The performance metrics results are measured against mobility of mesh clients over different network sizes. The simulation values are measured by considering both dynamic and static environment over all metrics as shown in Table-5 and 6.

4.2 Dynamic simulation environment (where number of clients are mobile in nature)

Table-5 shows the simulation results of listed parameters over dynamic environment of network where mesh clients are mobile in nature and transmit some data packets to other mobile nodes. The number of clients is

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

varied from 10 to 70 with a maximum mobility speed of 10m/s and the grey hole affected nodes are increasing with the increase in mobile clients i.e. 5, 10, 20, 30 and 40 in 10, 25, 40, 55 and 70 network size.

Table-5. Simulation values in dynamic environment.

Simulation parameters with their approaches			**Mobile mesh clients**				
Network parameters		**Approach**	**10**	**25**	**40**	**55**	**70**
End to end delay(ms)	**During idle case**	Basic Approach	17	20	22	27	32
		Proposed Approach	17	18	21	24	28
	During grey hole attack	Basic Approach	22	25	27	32	37
		Proposed Approach	22	23	26	29	33
Average throughput (in kbps)	**During Idle Case**	Basic Approach	16.77	16.72	16.67	16.63	16.61
		Proposed Approach	16.80	16.76	16.74	16.71	16.66
	During grey hole Attack	Basic Approach	16.52	16.50	16.47	16.45	16.42
		Proposed Approach	16.75	16.71	16.68	16.65	16.60
Packetdelivery ratio (%)	**During Idle Case**	Basic Approach	97.7	97.5	97.2	97.1	97.0
		Proposed Approach	98.8	98.5	98.2	98.1	98.0
	During grey hole Attack	Basic Approach	93.9	93.5	93.1	92.7	92.3
		Proposed Approach	97.7	97.4	97.2	97.1	96.9

4.2.1 End-to-end delay

As depicted in Figure-5 (a), SMP outperforms S-ODMRP against varied mobile clients. The latency increases with the increase of mobile clients. The more the number of number of hops between S and D, the more the possibility of node/link failure and this cause may results in re-routing the data packets and delay in end-to-end transmission. In case of SMP at network size of 70 nodes, the latency is less in comparison of S-ODMRP because packets are re-routed and transmitted by the node itself.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

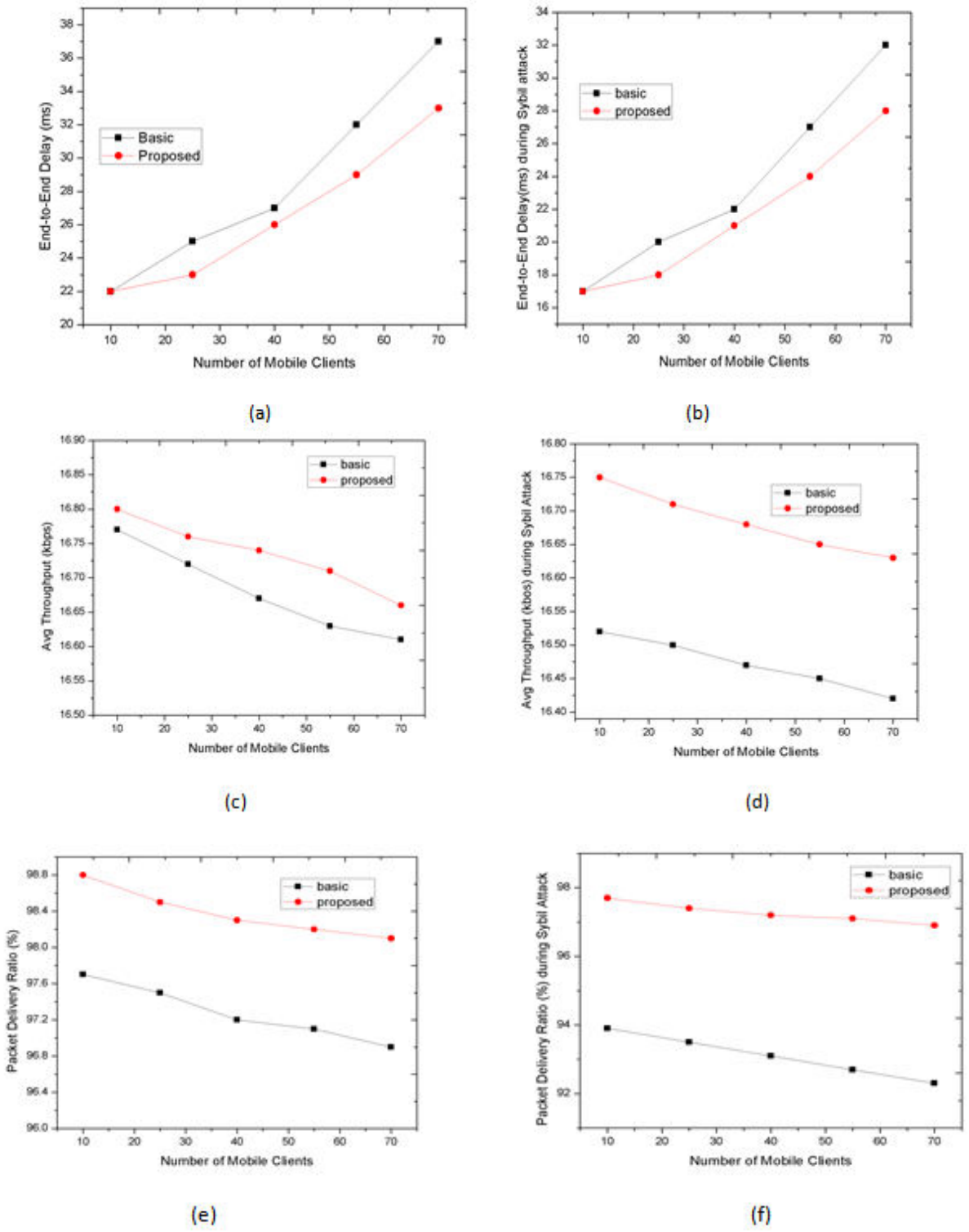

Figure-5. During dynamic environment (a) end-to-end delay without security, (b) end-to-end delay with security, (c) average throughput without security (d) average throughput with security (e) packet delivery ratio without security (f) packet delivery ratio with security.

4.2.2 Throughput

In this, an average throughput is computed which is division of throughput of all the nodes divided by number of nodes. The average throughput of SMP outperforms S-ODMRP as depicted in Figure-5 (c) because the packet loss ratio in case of SMP is less due to its link quality mechanism. In case of S-ODMRP, during node/link failure, packets may re-route during faults but cannot be recovered by the loss error.

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

4.2.3 Packet Delivery Ratio (PDR)

The PDR of SMP shows a huge enhancement in comparison of S-ODMRP as shown in Figure-5 (e). The reason of improved PDR of SMP isdue to unique characteristic of mesh router where each node acts as source node and as has the ability to retransmit the data packets during failures.

The above discussed parameters are measured against security parameter by introducing the grey hole attack between the source and destination where compromised node receives all packets from its preceding node but forwards selected number of packets to its succeeding node. All the discussed metrics is analysed against security attack and re-measure the simulation values as depicted in Figure-5 (b), 5 (d) and 5 (f).

4.3 Static Simulation Environment (where number of nodes are varying)

Table-6 shows static environment simulation values where network is static in nature and results are measured by varying the network sizes.

Table-6. Simulation values in static environment.

Simulation Parameters with their Approaches		Different Network Size					
Network Parameters	Approach	150	250	350	450	550	700
End to End Delay (in ms)	Basic Approach	69	72	74	79	84	89
	Proposed Approach	58	59	62	63	69	73
Throughput (%)	Basic Approach	94	92	87	85	81	78
	Proposed Approach	97	96	94	91	89	86
Packet Delivery Ratio (%)	Basic Approach	91	86	80	75	69	65
	Proposed Approach	93	89	84	82	79	75

Further Figure-6 (a), (b) and (c) shows the end to end delay, throughput and PDR results against varied number of nodes in a static environment which proves that the SMP protocol is better than existing routing protocols.

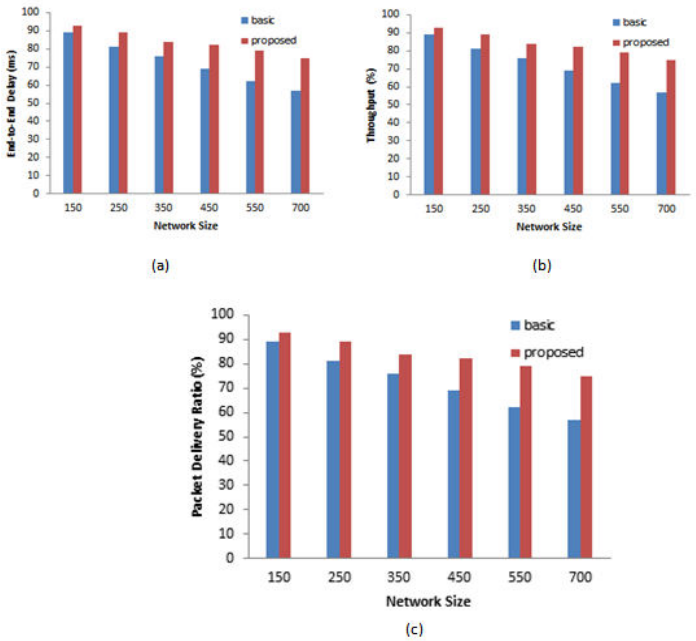

Figure-6. During static environment (a) end-to-end delay (b) throughput (c) packet delivery ratio.

5. CONCLUSIONS

The manuscript proposed a quality based secure routing protocol which is resilient against grey hole attack. The proposed protocol ensures security against grey hole attack by introducing the concept of Packet Delivery percentage. The node having the Packet Delivery between $95\% <= PD_x <= 100\%$ is considered as idle node and able to forward the data packets. The proposed routing protocol is measured against several network metrics. The simulation is done over NS2 and shows the performance

©2006-2016 Asian Research Publishing Network (ARPN). All rights reserved.

graphs of end-to-end delay, throughput and PDR against reported multicast protocol by considering static and dynamic environments under scalable network sizes.

REFERENCES

[1] F. Akyildiz and X. Wang. 2005. A survey on wireless mesh networks. IEEE Communications Magazine. 43: 23-30.

[2] S. Khan and A. S. K. Pathan. 2013. Wireless networks and security: Issues, challenges and research trends. Springer Science & Business Media, London.

[3] S. Mohapatra and P. Kanungo. 2012. Performance analysis of AODV, DSR, OLSR and DSDV routing protocols using NS2 Simulator. Procedia Engineering. 30: 69-76.

[4] S. Dhenakaran and A. Parvathavarthini. 2013. An overview of routing protocols in mobile ad-hoc network. International Journal of Advanced Research in Computer Science and Software Engineering. 3(2).

[5] D. Amit, N. Kumar and S. Bawa. 2014. A systematic review on routing protocols for vehicular ad hoc networks. Vehicular Communications. 1(1): 33-52.

[6] D. Jiang, X. Zhengzheng, L. Wenpan and C. Zhenhua. 2015. Network coding-based energy-efficient multicast routing algorithm for multi-hop wireless networks. Journal of Systems and Software. 104: 152-165.

[7] B. Karthikeyan, N. Kanimozhi and S.H. Ganesh. 2016. Encrypt-security improved ad hoc on demand distance vector routing protocol. (En-SIm AODV), ARPN Journal of Engineering and Applied Science. 11(2): 1092-1096.

[8] B. K. Shirin and M. Seeth. 2016. TRPSD: Trustworthy Routing Policy for Service Discovery in MANETs. ARPN Journal of Engineering and Applied Science. 11(3): 1735-1744.

[9] F. Abbas and H. Oh. 2014. A step towards user privacy while using location-based services. Journal of Information Processing Systems. 10(4): 618-627.

[10] R. H. Jhaveri, and N. M. Patel. 2016. Attack-pattern discovery based enhanced trust model for secure routing in mobile ad-hoc networks. International Journal of Communication Systems. DOI: 10.1002/dac.3148.

[11] N. Bendimerad, and B. Kechar. 2015. Rotational wireless video sensor networks with obstacle avoidance capability for improving disaster area coverage. Journal of Information Processing Systems. 11(4): 509-527.

[12] S. Lu, L. Li, *et al.* 2009. SAODV: A MANET routing protocol that can withstand black hole attack. Proceedings of International Conference on Computational Intelligence and Security, Beijing, China. pp. 421-425.

[13] S. U. M. Kamal, R. J. A. Ali, et al. 2016. Survey and brief history on malware in network security case study: viruses, worms and bots. ARPN Journal of Engineering and Applied Science. 11(1): 683-698.

[14] H. Simaremare, A. Abouaissa, *et al.* 2013. Secure aodv routing protocol based on trust mechanism. Wireless Networks and Security, Springer Berlin Heidelberg.pp. 81-105.

[15] D. W. Kum, J. S. Park, *et al.* 2010. Performance evaluation of AODV and DYMO routing protocols in MANET. Proceedings of 7th IEEE Consumer Communications and Networking Conference (CCNC), Las Vegas, USA.

[16] T. Meng, W. Fan *et al.* 2016. Spatial reusability-aware routing in multi-hop wireless networks. IEEE Transactions on Computers. 65(1): 244-255.

[17] S. Wang, A. Basalamah, et al. 2016. Link-correlation-aware opportunistic routing in wireless networks. IEEE Transactions on Wireless Communications. 14(1): 47-56.

[18] Y. Zhao, L. Xu, and M. Shi. 2003. On-demand multicast routing protocol with multipoint relay (ODMRP-MPR) in mobile ad-hoc network. IEEE International Conference on Communication Technology Proceedings, ICCT. 2: 1295-1300.

[19] A. Adya, P. Bahl, *et al.* 2004. A multi-radio unification protocol for IEEE 802.11 wireless networks. IEEE First International Conference on Broadband Networks, BroadNets. pp. 344-354.

[20] P. Anitha, G. N. Pavithra and P. S. Periasamy. 2012. March. An improved security mechanism for high-throughput multicast routing in wireless mesh networks against Sybil attack. IEEE International Conference on Pattern Recognition, Informatics and Medical Engineering (PRIME).pp. 125-130.