Dynamic Source Routing under Attacks

Abdelshafy, M. & King, P. J. B.

DOI 10.1109/RNDM.2015.7325226

Publisher: IEEE

Dynamic Source Routing under Attacks

Mohamed A. Abdelshafy
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
Email: ma814@hw.ac.uk

Peter J. B. King
School of Mathematical & Computer Sciences
Heriot-Watt University
Edinburgh, UK
Email: P.J.B.King@hw.ac.uk

***Abstract*—MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the routing protocol. A large number of attack types of varying severity are threatening MANET. Dynamic Source Routing (DSR) is a well-known reactive MANET routing protocol that does not support security of routing messages. In this paper, we study the performance of both DSR and its flow-state extension routing protocols in the presence of blackhole, grayhole, selfish and flooding attacks. We conclude that the performance of flow-state DSR is better than DSR in the presence of all attacks. Flooding attacks are found to dramatically impact all the standard performance metrics. Blackhole attacks significantly worse the packet delivery ratio in a static network using unmodified DSR. All the attacks greatly increase the end-to-end delay; an effect particularly marked in a static network.**

***Keywords*—MANET, Routing, DSR, Flow-state, Security, Attack, Flooding, Grayhole, Blackhole, Selfish**

I. Introduction

A Mobile Ad Hoc Network (MANET) is a decentralized infrastructureless network in which nodes cooperate to forward data from a source to a destination. Each node in a MANET acts both as a router and as a host. Several routing protocols have been designed for MANETs [5] to optimize network routing performance. The major issues involved in designing a routing protocol for MANET are nodes mobility, bandwidth constrained and error prone wireless channel, resource constrained nodes, and dynamic changing of the network topology [1].

MANET routing protocols can be classified as proactive or reactive routing protocols. In proactive (table-driven) routing protocols, each node maintains one or more tables containing routing information to every other node in the network. While in reactive (on-demand) routing protocols, routes are created whenever a source requires to send data to a destination node which means that these protocols are initiated by a source on-demand. In this paper, we focus on the Dynamic Source Routing protocol (DSR) [18] which is an extensively studied reactive protocol.

Conventional MANET routing protocols assume that all nodes cooperate without maliciously disrupting the operation of the protocol and do not provide defense against malicious attackers. However, the existence of malicious nodes cannot be ignored in computer networks, especially in MANETs because of the wireless nature of the network. MANET inherits security threats that are faced in wired as well as wireless networks and also introduces security attacks unique to itself [13] due its characteristics. Nodes in MANET have limited computation and power capabilities that make the network more vulnerable to Denial of Service (DoS) attacks. It is difficult to implement cryptography and key management algorithms which need substantial computations like public key algorithms. Node mobility introduces also a difficulty of distinguishing between stale routes and fake routes. A malicious node can attack the network layer in MANET either by not forwarding packets or by changing some parameters of routing messages such as sequence number and IP addresses, sending fake messages several times and sending fake routing information to disrupt routing operations. A large number of attacks on MANET [21] are known and much effort has been made to solve them. Simulation studies have shown the impact of such attacks and the effectiveness of proposed defence mechanisms [17] [22].

Security mechanisms are added to existing routing protocols to resist attacks. Cryptographic techniques are used to ensure the authenticity and integrity of routing messages [12]. A major concern is the trade off between security and performance, given the limited resources available at many MANET nodes. Both symmetric and asymmetric cryptography have been used as well as hash chaining. Examples of these security enhanced protocols are Authenticated Routing for Ad-hoc Networks (ARAN) [19], Secure Link State Routing Protocol (SLSP) [16], and Secure Ad-hoc On-demand Distance Vector routing (SAODV) [23]. In addition to the power and computation cost of using cryptographic techniques, the performance of secured mechanism is worse than non-secured in the presence of some attacks [3]. Securing the routing messages does not guarantee the detection of these malicious nodes.

The rest of the paper is organized as follows. In Section II, an overview of the DSR and its flow-state extension routing protocols is presented. In Section III, the impact of some attacks on MANET is discussed. In Section IV, the simulation approach and parameters is presented. In Section V, simulation results are given. In Section VI, conclusions are drawn.

II. DSR and its Improvements

DSR [10] is one of the most well-known MANET reactive protocols. The protocol is an on-demand source routing protocol which means that the data packets contain a list of nodes representing the route to be followed and the routes are created whenever a source node requires to send data to a destination node. The protocol consists of two mechanisms which are route discovery and route maintenance. Nodes using DSR may cache multiple routes to a single destination, and may use any of these routes at any time for any packet being sent. When a source node aims to send a packet, it firstly

consults its route cache. If the required route is available, the source node includes the routing information inside the data packet before sending it. Otherwise, the source node initiates a route discovery operation by broadcasting a route request RREQ packet. Receiving a RREQ packet, a node checks its route cache and replies from its cache if it has a route to the destination. If the node does not have routing information for the requested destination, it appends its own address to the route record field of the RREQ packet and locally rebroadcasts the RREQ packet to its neighbors. The destination node generates a route reply RREP packet that includes the list of addresses received in the RREQ and unicasts it back along this path to the source and stores this route in its route cache for possible use on subsequent packets. Each node on the route is responsible for confirming that the packet has been received by the next node in the route and retransmitting the packet if necessary. If no confirmation is received after a limited number of retransmission attempts for the packet, the link from this node to the next hop is considered to have broken, and the route maintenance mechanism sends a route error RERR packet to the source node identifying this broken link. The source node then removes this broken link from its route cache; for subsequent packets to this same destination, and uses an alternate route that it may already have in its route cache or may re-invoke route discovery to discover a new route to this destination.

A number of optimizations that improve the performance of the basic DSR have been introduced [11] [8]. If a node receives RREQ has a route to the source in its route cache, it may reply from its cache by appending its cached route to the received RREQ route. A node may also update its route cache based on source routes or other routing information that it forwards by optionally operating its network interface hardware in "promiscuous" receive mode. After a node detects a broken link and returns a RERR to the source, the node may attempt to salvage the packet if it has a different route to the destination in its own route cache; it replaces the original route with the route from its cache and transmits the packet to the new next hop node. DSR can support automatic route shortening to allow source routes in use to be shortened when possible, for example when nodes move close enough together so that one or more intermediate hops are no longer necessary. If a node is able to promiscuously receive a packet not intended for it as the next hop, then this node returns a "gratuitous" RREP to the source of the packet; this reply gives a shorter route that does not include the intermediate nodes between the node that transmitted the packet and this node.

One of the most important optimizations of DSR is a flow state extension [9]. It allows the routing of most packets without an explicit source route header in the packet. A source node sending packets to a destination node uses implicit source routing to establish a route to that destination as a flow. Each node participating in implicit source routing has a flow table, with one entry for each flow forwarded by that node. The flow table has to record the next hop address to which a packet for this flow should be forwarded, in addition to the source address, destination address, and flow identifier for this flow. A source can establish a new flow by sending a flow establishment packet that has two headers: one containing the flow identifier, and the other containing a source route and a timeout for the flow. When an intermediate forwards this packet, in addition to forwarding it according to the source route information, it creates a flow table entry for this flow and inserts the necessary information from the packet. A node is required to remove a flow entry from the flow table when that node has not forwarded packets for that flow for a period of time specified by the timeout for the flow. A node forwarding a packet sent using implicit source routing checks its flow table for an entry corresponding to the flow identifier in the packet. When a packet is sent using implicit source routing forwarding, it still requires some small amount of overhead in the packet. These additional header bytes in the packet can be entirely eliminated by the use of default flows. From a given source to a destination, any number of different flows may exist and be in use. One of these flows may be considered to be the "default" flow from that source to that destination. A node receiving a packet, with neither a DSR header specifying the route to be taken nor a DSR Flow State header specifying the flow to be followed, is forwarded along the default flow for the source and destination addresses specified in the packet's IP header [11].

III. DSR Security Flaws

MANETs are more vulnerable to security attacks than fixed networks due their inherent characteristics. MANET routing protocols are designed based on the assumption that all nodes cooperate without maliciously disrupting the operation of the protocol. However, the existence of malicious nodes cannot be disregarded in any system, especially in MANETs because of the wireless nature of the network. A malicious node aims to cause congestion, propagate fake routing information or disturb nodes from providing services. The behavior of a malicious node is to disrupt the operation of the DSR routing protocol [2]. The malicious node can spoof source or destination IP address, modify and/or generate fake routing packets. Attacks against MANET are classified based on modification, impersonation or fabrication of the routing messages. While there is large number of existing attacks, our paper is focused on flooding, grayhole, selfish and blackhole attacks.

A. DSR under Flooding Attack

In a flooding attack [7], a malicious node floods the network with a large number of RREQs to non-existent destinations in the network. Since the destination does not exist in the network, a RREP packet cannot be generated by any node in the network. When a large number of fake RREQ packets are broadcast into the network, new routes can no longer be added and the network is unable to transmit data packets. This leads to congestion in the network and overflow of route table in the intermediate nodes so that the nodes cannot receive new RREQ packet, resulting in a DoS attack. Moreover, unnecessary forwarding of these fake RREQ packets has serious effects in MANET [4] as a result of limited computational and power resources of nodes.

B. DSR under Blackhole Attack

In a blackhole attack [20], a malicious node absorbs the network traffic and drops all packets. Once a malicious node receives a RREQ packet from any other node, it immediately sends a false RREP with a high sequence number and hop count equals 1 to spoof its neighbours that it has the best

route to the destination. Thus, the malicious node reply will be received by the source node before any other replies and will be selected to send data packets through the route that includes the malicious node. When the data packets routed by the source node reach the blackhole node, it drops the packets rather than forwarding them to the destination node.

C. DSR under Selfish Attack

In a selfish attack [6], a malicious node saves its resources; such as battery, by not cooperating in the network operations. A selfish node affects the network performance as it does not correctly process routing or data packets based on the routing protocol. The selfish node drops all data and control packets even if these packets are sent to it. When a selfish node needs to send data to another node, it starts working as normal DSR operation. After it finishes sending its data, the node returns to its silent mode and the selfish behavior.

D. DSR under Grayhole Attack

In a grayhole attack [14], a malicious node behaves normally as a truthful node by replying with true RREP packets to the nodes that started RREQ packets. After the source node starts sending data through the malicious node, the malicious node starts dropping these data packets to launch a (DoS) denial of service attack. So, the malicious node forwards routing packets and drops data packets which makes grayhole attacks much more difficult to detect.

IV. Simulation Approach

NS-2 simulator [15] is used to simulate grayhole, blackhole, flooding and selfish attacks. The simulation is used to analyse the performance of DSR and its flow-state extensions routing protocols under these attacks. The parameters used are shown in Table I. Node mobility was modelled with the random waypoint method. Our simulation results are obtained from 3 different movement scenarios, 3 different traffic scenarios and 3 different node-type (malicious or non-malicious) scenarios which means that each metric value is the mean of the 27 runs. The node-type scenario is created randomly. In all cases, the 90% confidence interval was small compared with the values being reported. While we examined the effects of the attacks on both UDP and TCP traffic, in this paper we focused on their impact on the TCP traffic only. We also examined the effect of these attacks for different node speeds (0, 5, 10, 15, 20, 25 and 30 m/s). The paper results are focused only on the static network and the highest mobility nodes (30 m/s).

TABLE I. Simulation Parameters

Simulation Time	180 s
Simulation Area	1000 m x 1000 m
Number of Nodes	100
Number of Connections	70
Number of Malicious Nodes	0 - 10
Node Speed	0 - 30 m/s
Pause Time	10 s
Traffic Type	TCP

Packet Delivery Ratio (PDR): The ratio of packets that are successfully delivered to a destination compared to the number of packets that have been sent out by the sender.
Throughput: The number of data bits delivered to the application layer of destination node in unit time measured in bps.
End-to-End Delay (EED): The average time taken for a packet to be transmitted across the network from source to destination.
Routing Overhead: The number of routing packets for route discovery and route maintenance needed to deliver the data packets from sources to destinations.
Route Discovery Latency (RDL): The average delay between the sending RREQ from a source and receiving the first corresponding RREP.
Sent Data Packets: The total number of packets sent by all source nodes during the simulation time which can represent the bandwidth capacity of the wireless channel under attacks.

V. Simulation Results

A. DSR under Flooding Attack

Figure 1 shows the effect of flooding attack on the network throughput. In static networks, flow extension DSR achieves approximately double the throughput of original DSR. However when the network is highly mobile, the two protocols are almost identical in terms of throughput. The figure shows that the throughput of the network decreases 6% approximately for each malicious node in the static network.

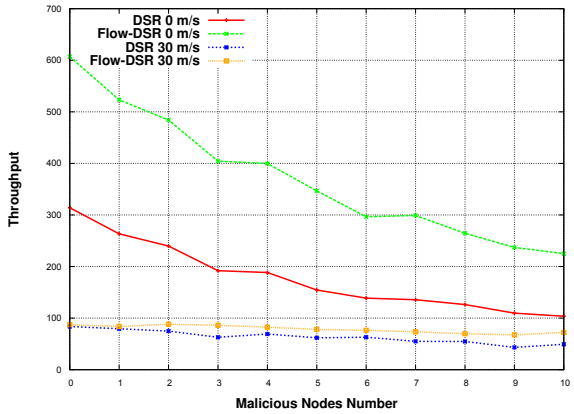

Fig. 1. Throughput under Flooding Attack

The effect of flooding attack on the packet delivery ratio is shown in Figure 2. While the flooding attack has small impact on the PDR of the flow extension of DSR, its effect is remarkable on the PDR of the original DSR specially for large number of malicious nodes. Figure shows that the PDR of the network decreases 1% approximately for each malicious node regardless the nodes mobility.

The effect illustrated by PDR is more noticeable if we combine it with the number of packets that can be sent which is shown in Figure 3. The figure shows that the total number of packets that can be sent is dramatically decreasing as the number of malicious nodes increases. By combining Figure 2 and Figure 3, we see that when the number of received packets is measured the effect of flooding is more dramatic. As the number of malicious nodes increases, the number of

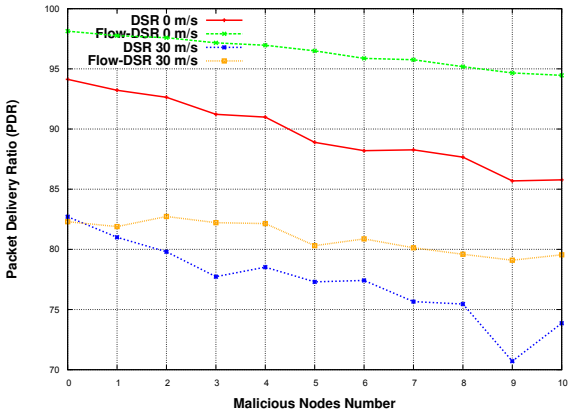

Fig. 2. PDR under Flooding Attack

received packets reduces. With 10 malicious nodes, the number is reduced to one third of the number received with no attack taking place.

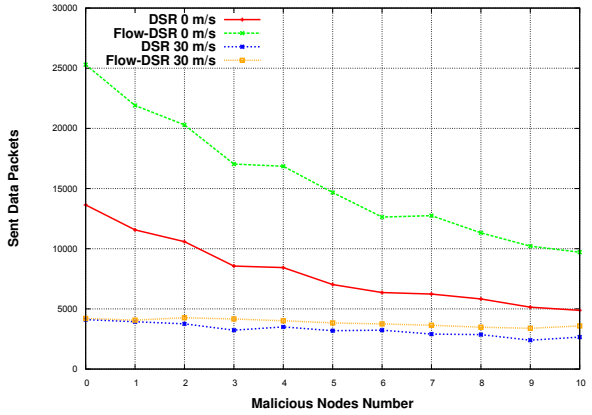

Fig. 3. Send Data Packets under Flooding Attack

The effect of flooding attack on the end-end-delay is shown in Figure 4. The result shows that there is no significant change between the delay of both DSR and its flow extension in high mobility nodes and this delay increases up to 15% if there are 10 malicious nodes. On the other hand, the two protocols increase the delay dramatically as the number of malicious nodes increases up to approximately 100% if there are 10 malicious nodes.

Figure 5 shows the effect of flooding attack on the routing overhead. While the routing overhead of both protocols has slightly increased as the number of malicious nodes increases in high mobility nodes, it increases dramatically as the number of malicious nodes increases in static nodes. The figure shows as well that the flow extension has a significantly lower overhead than original DSR irrespective of the number of malicious nodes in static network.

Figure 6 shows the effect of flooding attack on the routing discovery latency. The result shows that the routing discovery

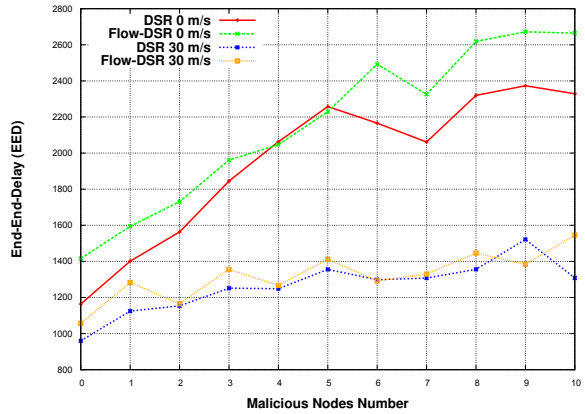

Fig. 4. Average End-End-Delay under Flooding Attack

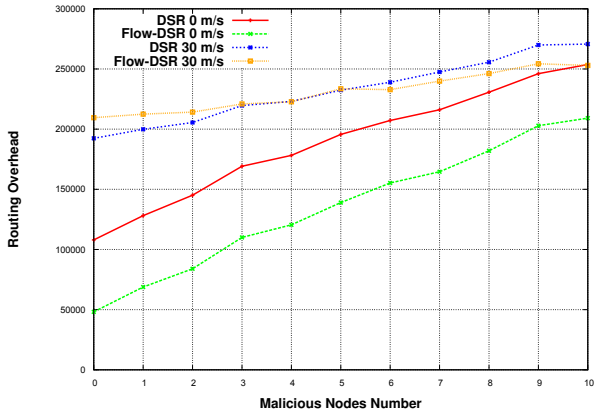

Fig. 5. Routing Overhead under Flooding Attack

latency of original DSR is better than its flow extension regardless of the nodes mobility. The figure shows as well that RDL is increases slightly as the number of malicious nodes increases.

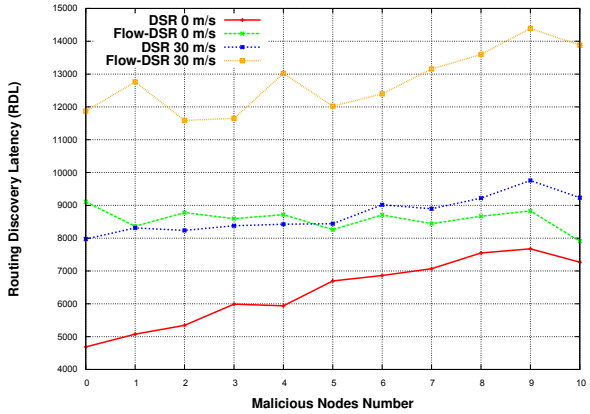

Fig. 6. RDL under Flooding Attack

B. DSR under Blackhole Attack

Figure 7 shows the effect of blackhole attack on the network throughput. While the throughput of the flow extension of DSR is better than original DSR in a static network, there is no observed difference in a high mobility network. The figure shows as well that the throughput slightly increases as the number of malicious nodes increases. This result is slightly confusing as the attack improves the throughput. This is because the blackhole nodes stop rebroadcasting the RREQ which decreases the number of RREQ packets that leads to free channel bandwidth for sending data.

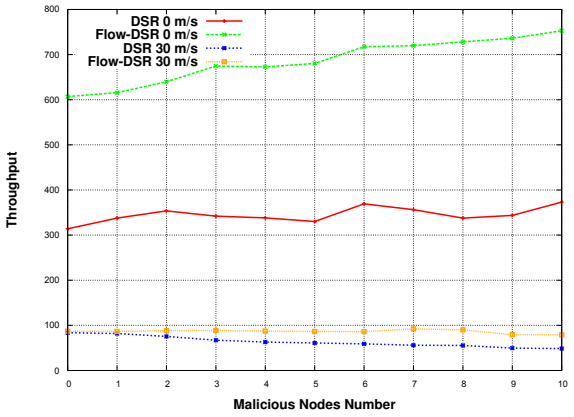

Fig. 7. Throughput under Blackhole Attack

The effect of blackhole attack on the packet delivery ratio is shown in Figure 8. While the blackhole attack has no impact on the PDR of both protocols in static nodes, the PDR of the original DSR is dramatically decreased as the number of malicious nodes increases by approximately 1% for each malicious node in high mobility nodes. As a result of the PDR being nearly constant, the effect of blackhole attack on the number of packets sent is represented by a graph which is very similar to the throughput graph.

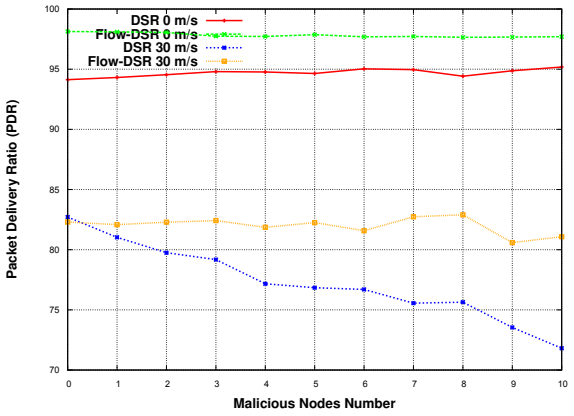

Fig. 8. PDR under Blackhole Attack

The effect of blackhole attack on the end-end-delay is shown in Fig 9. While the results show that the malicious nodes have severe impact on the delay in static networks, the delay in high mobility nodes is not affected so much by the malicious nodes presence. The results show that the delay of the two protocols is reduced as the number of malicious nodes increases which is slightly paradoxical as the attack improves the delay. This is a misleading result because the delay is only measured on packets that reach their destinations and since the blackhole nodes drop all the data routed through it, the number of packets that will be considered in calculating the delay decreases as the number of malicious nodes increases. So, the routes that avoid blackhole nodes suffer less competition, and hence reduced delay.

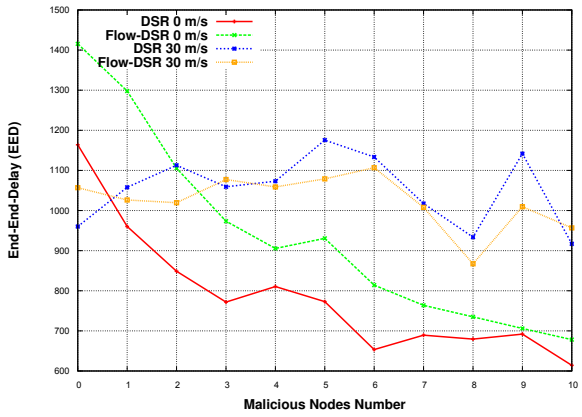

Fig. 9. Average End-End-Delay under Blackhole Attack

Figure 10 shows the effect of blackhole attack on the routing overhead. The routing overhead of DSR is approximately twice its corresponding value in its flow extension in static network while there is no significant change in high mobility nodes. In addition, the figure shows that while the routing overhead increases as the number of malicious nodes increases in high mobility nodes, it decreases as a result of malicious nodes in static nodes. The static network results are slightly confusing as the blackhole attack improves the routing overhead. This is because the blackhole nodes stop rebroadcasting the RREQ which decreases the number of RREQ packets, one of factors used to measure the routing overhead. On the other hand, the number of RREQ remains at the same level in high mobility nodes which leads to a logical result of increasing the total routing overhead.

Figure 11 shows the effect of blackhole attack on the routing discovery latency. The routing discovery latency of original DSR is better than its flow extension regardless the nodes mobility. The figure shows as well that RDL is decreased slightly as the number of malicious nodes increases. This slightly confusing result is achieved because the fast response of the blackhole nodes to RREQs decreases the delay time between the RREQ and its corresponding RREP which leads to improve the RDL as the number of malicious nodes increases.

C. DSR under Selfish Attack

The selfish attack simulation introduces very similar results to the blackhole attack as the blackhole and selfish nodes share

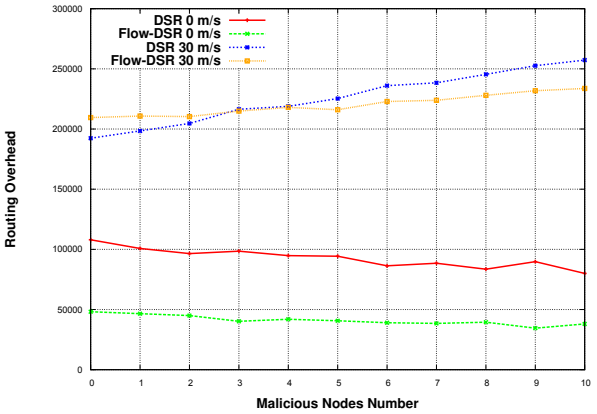

Fig. 10. Routing Overhead under Blackhole Attack

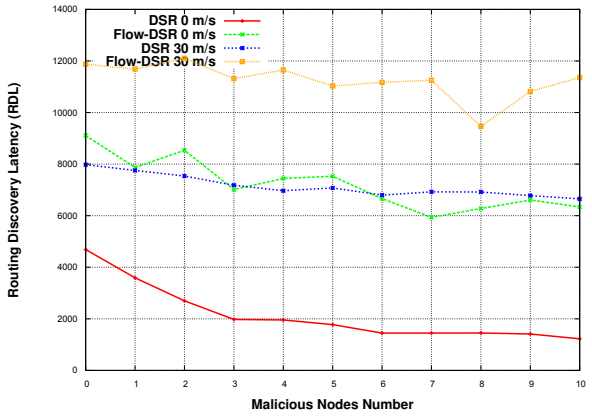

Fig. 11. RDL under Blackhole Attack

dropping data packets. This is because of the network throughput, end-end-delay and routing overheads are calculated based on the received data packets which are identical for the same simulation scenario. The difference between simulation results of selfish attack and blackhole attack is in the PDR and the routing overhead. Figure 12 shows that the PDR for both protocols is nearly constant in high node mobility and in static nodes.

Figure 13 shows the effect of selfish attack on the routing overhead. While the routing overhead increases as the number of blackhole nodes increases in the network as mentioned in figure 10, it decreases as the selfish nodes increase in the network. This is logical as the selfish node drops all routing messages routed through it.

D. DSR under Grayhole Attack

As the grayhole node drops all data packets and the selfish node drops all data and routing packets, the grayhole attack simulation introduces very similar results to the selfish attack. The only major difference between simulation results of grayhole attack and selfish attack is in the routing overhead. Figure 14 shows that the routing overhead for both protocols is nearly constant regardless the node mobility and malicious

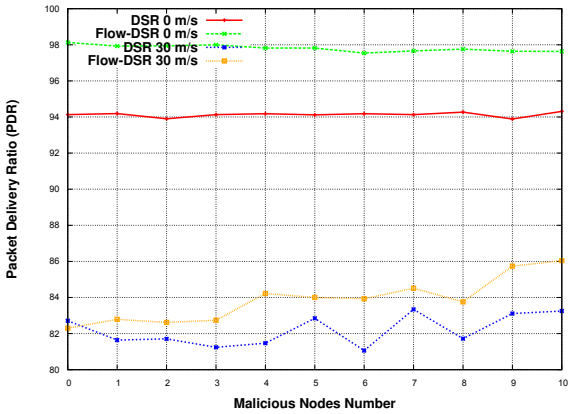

Fig. 12. PDR under Selfish Attack

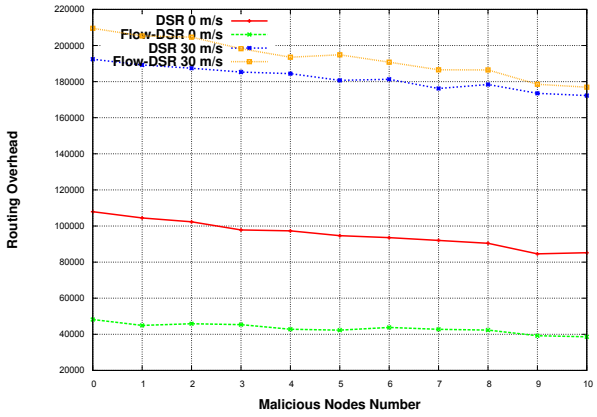

Fig. 13. Routing Overhead under Selfish Attack

nodes number and is slightly decreases for DSR in static network.

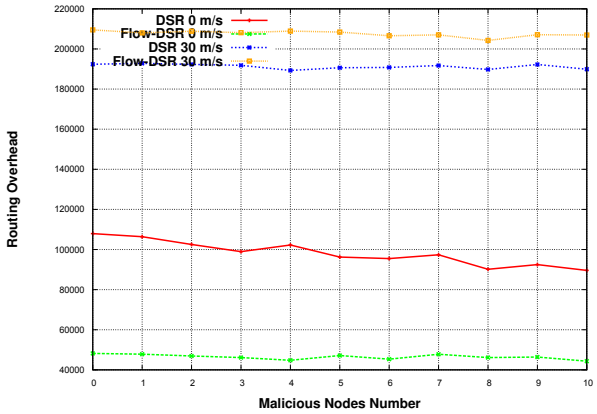

Fig. 14. Routing Overhead under Grayhole Attack

VI. Conclusion

In this paper, we analysed the performance of both DSR and its flow-state extension routing protocols under the blackhole, grayhole, selfish and flooding attacks for different mobility speeds. We conclude that the performance of the flow extension of the DSR is better than original DSR in the presence of blackhole, grayhole and selfish attacks. These attacks have a more severe effect on static networks than on high mobility networks.

We conclude as well that the flooding attacks have dramatic impact on the network performance for the all the performance metrics. On the other hand, all other attacks have remarkable negative impact on the end-end-delay specially for static nodes and less dangerous in the rest of the performance metrics. Blackhole attack has dramatic impact on the PDR of the original DSR in static network. As most of the performance metrics depend on the number of received data packets, little changes are observed in these metrics under blackhole, selfish and grayhole attacks because the malicious nodes drop data packets in these attacks.

References

[1] M. A. Abdelshafy and P. J. King. Analysis of security attacks on AODV routing. In *8th International Conference for Internet Technology and Secured Transactions (ICITST)*, pages 290–295, London, UK, Dec 2013.

[2] M. A. Abdelshafy and P. J. King. AODV & SAODV under attack:performance comparison. In *ADHOC-NOW 2014, LNCS 8487*, pages 318–331, Benidorm, Spain, Jun 2014.

[3] M. A. Abdelshafy and P. J. King. Resisting flooding attacks on AODV. In *8th International Conference on Emerging Security Information, Systems and Technologies (SECURWARE)*, pages 14–19, Lisbon, Portugal, Nov 2014.

[4] A. Bandyopadhyay, S. Vuppala, and P. Choudhury. A simulation analysis of flooding attack in MANET using ns-3. In *Wireless Communication, Vehicular Technology, Information Theory and Aerospace Electronic Systems Technology (Wireless VITAE), 2011 2nd International Conference on*, pages 1–5, 2011.

[5] A. Boukerche, B. Turgut, N. Aydin, M. Ahmad, L. Bölöni, and D. Turgut. Routing protocols in ad hoc networks: a survey. *Computer Networks*, 55(13):3032–3080, September 2011.

[6] P. Goyal, S. Batra, and A. Singh. A literature review of security attack in mobile ad-hoc networks. *International Journal of Computer Applications*, 9(12):11–15, November 2010.

[7] Y. Guo and S. Perreau. Detect DDoS flooding attacks in mobile ad hoc networks. *Int. J. Secur. Netw.*, 5(4):259–269, Dec. 2010.

[8] Y.-C. Hu and D. B. Johnson. Caching strategies in on-demand routing protocols for wireless ad hoc networks. In *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, MobiCom '00, pages 231–242, New York, NY, USA, 2000. ACM.

[9] Y.-C. Hu and D. B. Johnson. Implicit source routes for on-demand ad hoc network routing. In *Proceedings of the 2nd ACM International Symposium on Mobile Ad Hoc Networking &Amp; Computing*, MobiHoc '01, New York, NY, USA, 2001. ACM.

[10] D. B. Johnson and D. A. Maltz. Dynamic source routing in ad hoc wireless networks. *Mobile Computing*, pages 153–181, 1996.

[11] D. B. Johnson, D. A. Maltz, and J. Broch. DSR: The dynamic source routing protocol for multi-hop wireless ad hoc networks. In C. E. Perkins, editor, *Ad Hoc Networking*, pages 139–172. Addison-Wesley, 2001.

[12] P. Joshi. Security issues in routing protocols in MANETs at network layer. *Procedia CS*, 3:954–960, 2011.

[13] A. Kumar. Security attacks in MANET - a review. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, RTMC(11), May 2012.

[14] K. Manikandan, R.Satyaprasad, and K.Rajasekhararao. A Survey on Attacks and Defense Metrics of Routing Mechanism in Mobile Ad hoc Networks. *IJACSA - International Journal of Advanced Computer Science and Applications*, 2(3):7–12, 2011.

[15] The network simulator ns-2. http://www.isi.edu/nsnam/ns/.

[16] P. Papadimitratos and Z. J. Haas. Secure link state routing for mobile ad hoc networks. In *Symposium on Applications and the Internet Workshops*, pages 379–383. IEEE Computer Society, 2003.

[17] M. Patel and S. Sharma. Detection of malicious attack in manet a behavioral approach. In *IEEE 3rd International on Advance Computing Conference (IACC)*, pages 388–393, 2013.

[18] C. E. Perkins and E. M. Royer. Ad-hoc on-demand distance vector routing. In *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, pages 90–100, 1997.

[19] K. Sanzgiri and et al. Authenticated routing for ad hoc networks. *IEEE Journal On Selected Areas In Communications*, 23:598–610, 2005.

[20] N. Sharma and A. Sharma. The black-hole node attack in MANET. In *Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies*, ACCT '12, pages 546–550, Washington, DC, USA, 2012. IEEE Computer Society.

[21] M. Singh, A. Singh, R. Tanwar, and R. Chauhan. Security attacks in mobile adhoc networks. *IJCA Proceedings on National Workshop-Cum-Conference on Recent Trends in Mathematics and Computing 2011*, RTMC(11), May 2012.

[22] G. Usha and S. Bose. Impact of gray hole attack on adhoc networks. In *International Conference on Information Communication and Embedded Systems (ICICES)*, pages 404–409, 2013.

[23] M. G. Zapata. Secure ad hoc on-demand distance vector routing. *SIGMOBILE Mob. Comput. Commun. Rev.*, 6(3):106–107, jun 2002.