Modelling and Performance Analysis of Personalized DSR Routing Protocol to discover a selfish and Inimical Node in MANETs Using NS-2

Arjun Saini
M.Tech.(CSE)
Amity University Rajasthan (ASET)
Jaipur,Rajasthan,India
er.sainiarjun@gmail.com

Vijander Singh
Amity School of Engineering & Technology
Amity University Rajasthan
Jaipur,Rajasthan,India
vijan2005@gmail.com

Abstract- In this paper we activated the default dynamic source routing protocol with a selfish and inimical node and compared the performance of this code with default dynamic source routing protocol. The performance of this code is degrades in contrast with default dynamic source routing protocol. To escape from this attack we introduced a personalized dynamic source routing protocol which perform better compare to dynamic source routing protocol with selfish and inimical nodes. For the implementation and analyse the performance NS-2.34 was used. For comparison of the both routing protocols throughput, end to end delay, PDR, packet loss and routing overhead parameters are used with Random waypoint mobility model.

Keywords*:* MANET, Routing Protocols, Network simulator NS-2.34, Selfish node, Inimical Node.

I. INTRODUCTION

MANETs stands for Mobile Ad hoc Networks. Mobile Ad hoc Network is a collection of mobile nodes in wireless technique. In Mobile Ad-hoc networks, direct communication between nodes is possible without any access points. Mobile Ad hoc networks serve the issue of mobile nodes, due to its inherent properties such as self-organizing, self-healing, multi-hopping, dynamic nature [1], [4] and [12]. MANETs facilitates communication among the mobile users in collaborative and distributed computing, emergency operations, wireless sensor networks, wireless mesh networks and hybrid wireless network architectures [2]. MANETs are capable of handling topology which changes dynamically due to mobility. Malfunctioning nodes and network configuration bring great challenges to the security through inimical attack of Ad hoc Network [1], [3] and [4].

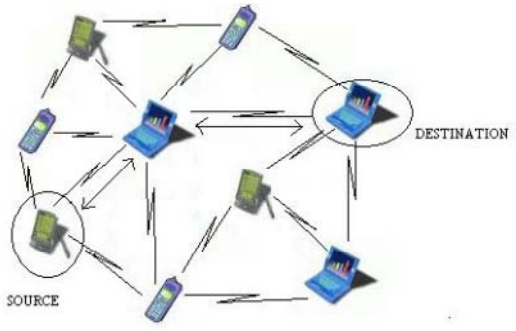

Fig. 1 General Mobile Ad hoc Network Architecture

In MANETs, routing protocols are categorized as table driven and on demand. Table driven routing protocol which is also known as proactive protocol maintain consistent and up to date routing information among the nodes in a routing table. On demand routing protocols also known as reactive protocol, discover a new route when a route is required from the source to the destination node. Also combinations of the features of above two types turn out hybrid routing protocol [1], [2] and [3]. Ad hoc networks setup is not expensive and no access points or base stations are needed for it. A geographical area in which there are a number of mobile devices or

users are present makes Wireless multi hop Ad hoc network. Devices or mobile user which makes wireless multi hop Ad hoc network is called as nodes. Examples of proactive routing protocols for Ad hoc networks include Destination Sequenced Distance Vector (DSDV), Optimised Link State Routing (OLSR) and Topology dissemination Based on Reverse-Path Forwarding (TBRPF).Examples of reactive routing protocols include Ad hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR).Example of hybrid routing protocol for Ad hoc network include Temporary ordered routing algorithm (TORA) and Zone routing protocol (ZRP) [1], [3] and [12]. This paper introduce about the misbehaviour of selfish node and inimical node on the Dynamic source routing protocol (DSR), the selfish and inimical node are those which refuse to forward the packet to next hop in source route. These nodes are implemented in the route request function and handle forward function of dynamic source routing protocol. This paper also introduces the performance which degraded by selfish and inimical node misbehaviour and also introduces the personalized code of Dynamic source routing (DSR) for better performance over the misbehaviour of nodes.

II. DYNAMIC SOURCE ROUTING (DSR) PROTOCOL

DSR is a reactive routing protocol which utilizes source routing algorithm and able to manage a MANET without using periodic table update message.In source routing algorithm, each data packet contains complete routing information to reach its destination. Additionally, in DSR each node uses caching technology to maintain route information that it has learnt [1]. It is an on-demand routing protocol without any periodic routing advertisement messages. In DSR routing, the source node appends the complete routing path to each data packet before transmitting. Additionally, each node uses a caching technique to maintain the route information [1] and [2]. DSR was specifically designed for use in multi hop wireless Ad hoc networks. Ad hoc protocol allows the network to be completely self-organizing and self-configuring which means that there is no need for an existing network infrastructure or administration [2], [3] and [12]. For restricting the bandwidth, the process to find a path is only executed when a path is required by node (on-demand routing). In DSR the Sender (source, initiator) determines the whole path from the source to the destination node (source routing) and deposits the address of the intermediate node of the route in the packets.

Route source is the sequences of hops that the packet has to follow on its way to the destination node the intermediate nodes are stored in the header. All the route sources are stored in the route cache. Every node has its own route cache. The route cache can store the learned source routes. After an execution time, source routes are defined from the route cache.DSR is an on-demand routing protocol that uses source routing rather than hop-by-hop routing approach [12]. Each packet to be routed carries in its header, a complete ordered list of nodes through which the packet will pass through. The advantage of DSR is that intermediate nodes do not need to maintain up-to-date routing information in order to route the packets they forward. Due to the on-demand characteristics of DSR, periodic route updates and neighbour detection are eliminated to minimize bandwidth consumption.DSR (Dynamic Source Routing) can be used which follows two mechanisms Route Discovery, Route Maintenance. It is an on-demand routing protocol without any periodic routing advertisement messages. Through DSR protocol hardly provides any QoS support, multicasting and security, it can easily adapts to changes like host movement without requiring considerable protocol overheads [12]. DSR can switch easily between the extreme situations where movement of hosts is quick and frequent i.e. where flooding may be the best strategy, as well as infrequent movements which are almost static i.e. where conventional routing protocols are most suitable [1] and [3].

In DSR, when a node has a packet to send to some destination and does not currently have a route to that destination in its Route Cache, the node initiates Route Discovery to discover a route; this node is known as the initiator of the Route Discovery. It is also a mechanism for finding the route to transmit data packets to a destination when the exact route is unknown to the sender. It uses flooding for through route request (RREQ). After receiving route request, each node rebroadcasts it further, till the original destination is reached. After receiving the packet the destination replies back to the source with route reply (RREP) [1], [3] and [12]. The route request records the route traversed so far in the route record list (RRL) for future use. The RREP follows that path backward to back to the source. Route Maintenance is the means by which a node sending a packet along a particular route to some destination detects if that route has wrecked, for example because two nodes in it have moved too apart. DSR is based on source routing when sending a packet, the initiator lists in the header of the packet the complete sequence of nodes through which the packet is forwarded. DSR provides two types of packets for maintaining these routes which are route error packets (RERR) and ACKs. Route error packets are used to tell about any broken link in the network and acknowledge the receipt of the Reply [3].

DSR is used in many performance comparisons, implementation, evaluation studies, and is used for other newer personalized protocols. In this paper firstly we implemented the code with misbehavior nodes which are selfish and inimical nodes and after evaluate the performance over varying parameter. After that implemented the personalized code and evaluate the performance.

III. RELATED WORK

In MANET over the selfish and inimical node we implemented Dynamic source routing protocol (DSR) and evaluated the performance. The selfish and inimical nodes of dynamic source routing on the Ad-hoc network which degrades the performance of installed dynamic source routing protocol. The selfish node is the categorized in following way

1) They do not take part in source routing process, it means a selfish nodes refused to forward the packet to next hop in the source route and drops route request and route reply packets.
2) They deliberately delay route request packets, by avoiding ourselves from random way point paths.
3) They may take part in routing messages but may not relay data packets over the source route path.

So our research is based on evaluation of result to control high affect over change of code with the selfish and inimical nodes in DSR protocol and also with the personalised DSR code. We implemented the normal dynamic source routing protocol which is installed code given in the network simulator with the new code with misbehaviour nodes and also with the personalized code.

With the selfish and inimical code of dynamic source routing and personalized code of dynamic source routing we implemented the code and analysis the performance over the simultaneously varying nodes and pause time in the scenario file with the equivalent nodes traffic file of CBR type in network simulator.

A. Personalized Dynamic source routing protocol Algorithm

Step-1 Test the selfish and inimical node by broadcast request to neighbouring nodes in personalized dynamic source routing protocol code file which is Dsragent.cc.

Step-2 Test whether the node in personalized code of dynamic source routing protocol is inimical or not

Step-3 Forward packets or given request and reply to next node otherwise drop data packets when node is selfish and inimical.

Step-4 Else insert to route information of RREQ (Route request) and forward all request, reply and data packets.

Step-5 On the particular selfish and inimical nodes which is take part personalized dynamic source routing Protocol its effect being reflected in performance on results.

B. Implementation of Personalized Dynamic source routing protocol Algorithm

In this paper we implemented the dynamic source routing protocol with personalized dynamic source routing protocol and selfish and inimical nodes dynamic source routing protocol on two calling function in protocol of agent.cc file.

1) handleRouteRequest(SRPacket &p): In which we implement and bypass the selfish and inimical nodes. At this function we test the node is selfish and inimical or not.
2) handleForwarding(SRPacket &p):In which we implement how the data packet is dropped over the route request and route reply when the nodes is read as a selfish and inimical nodes and when node is not selfish and inimical than forward the packets over the route request and route reply.

IV. SIMULATION APPROACH

The simulation approach packages are extensively used to develop a simulation model. We have setup this by using Network Simulator (NS-2) and evaluation the performance of selfish and inimical nodes dynamic source routing protocol and with personalized Dynamic source routing protocol. Implemented the protocol by adding a collection of C++ and oTcl code to installed code of dynamic source routing protocol to NS-2 's source base. We have generated the scenario files by taken an area of 1200m*800m and divide them into four categories.

1) Vary Pause time(10,20,30,40,50)
2) Fix Max Speed (20 m/s) and fix Simulation Time (200 sec) constant.
3) Vary number of nodes are (10, 20, 30, 40, 50).
4) Performances evaluate to all code with the fix Rate (10.0) and simultaneously change in number of nodes and pause time.

Now after generating the scenario files, we have generated traffic files using cbrgen utility of ns-2. The no of maximum connections were mentioned as fix for all result and no of nodes for a particular file in traffic file as the number of node of scenario file and data communication rate was defined as 10 packets per second.

For simulation, the computer system was having a good processing speed and large storage capacity as trace files were generated and each file was of the capacity in the range of 1gigabyte to 50 gigabytes. Tcl script was run over to generate the trace files for protocols DSR. After analysing these traces files with *awk* script we concluded the results for various parameters to be calculated.

A. Simulation Parameter Metrics

Table. 1 Simulation Parameters

Protocols	DSR
Simulation Area	1200 *800
Simulation Time	200 sec
No of Nodes	10, 20, 30, 40 ,50
Mobility Model	Random way point
Maximum Speed	20 m/sec
Vary Pause Time	10, 20, 30, 40, 50 sec
Type of Traffic	CBR
Size of Payload	512 bytes
Packet Rate	10 packets/sec
Maximum Connection	20

V. RESULT DISCUSSION

In this section the simulation result is shown for varying number of nodes and pause time based performance of DSR routing protocol, selfish and inimical nodes Dynamic source routing protocol and personalized Dynamic source routing protocol. These are some performance parameter are analysed on both code.

1) Packet Delivery Ratio: It tells about the number of packets delivered from the whole packets.

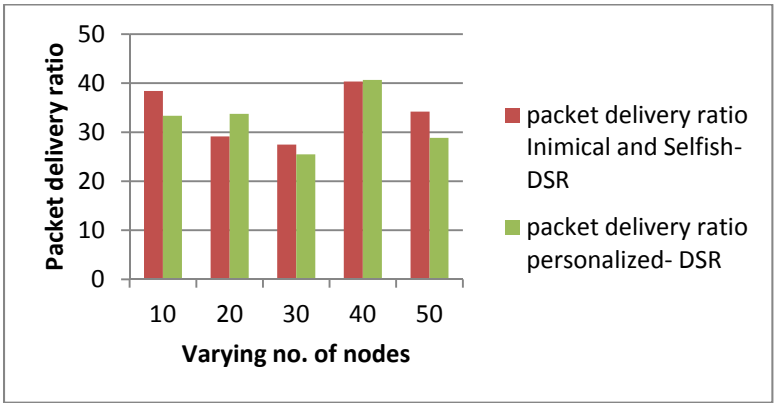

Fig. 2: Packet delivery ratio with varying no. Of nodes and pause time

So by our simulation result we can say packet delivery ratio of selfish and inimical nodes Dynamic source routing is way less well than personalized dynamic source routing protocol on the default dynamic source routing protocol. But when faced with inimical node the PDR reduces. It is also seen that on applying Improved DSR performance becomes slight better.

2) Average end-end delay: This metric is crucial in understanding the delay introduced by path discovery. As we have noticed the time difference between the packets sent and received, divide the total time among total CBR packets gives the average end to end delay for received packets.

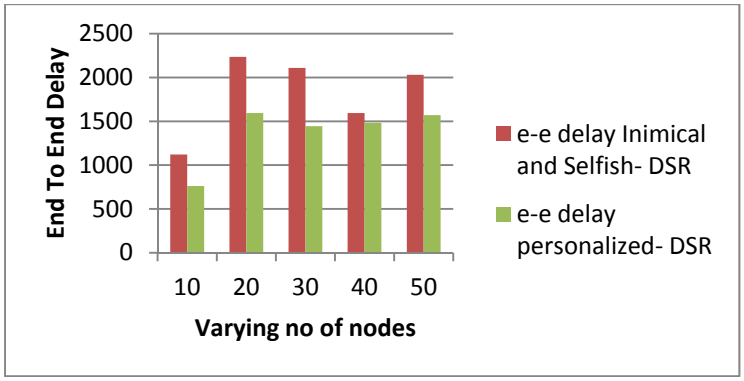

Fig. 3: end to end delay with varying no. of nodes and pause time

As per the variation in pause time and number of nodes, it is noticed that personalized Dynamic source routing protocol performs better than selfish and inimical Dynamic source routing.

3) Packet Loss: When a valid route is discovered, the routing protocols send the packets to destination; otherwise it is buffered until a route is discovered. Packet is dropped in two stages, if buffer is full or the time limit exceed when the packets are buffered.

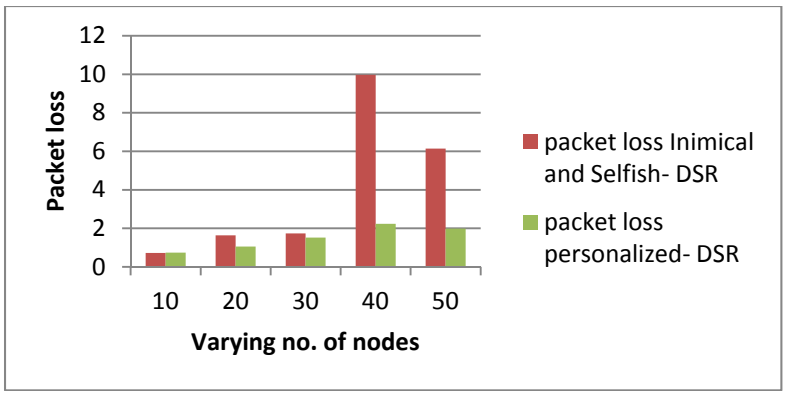

Fig. 4: Packet Loss with varying no. of nodes and pause time

Personalized dynamic source routing protocol packet loss is minimum in all the cases as compared to selfish and inimical nodes dynamic source routing protocol by varying pause time and number of nodes.

4) Routing Overhead: Total number of routing packets divided by total number of delivered data packets

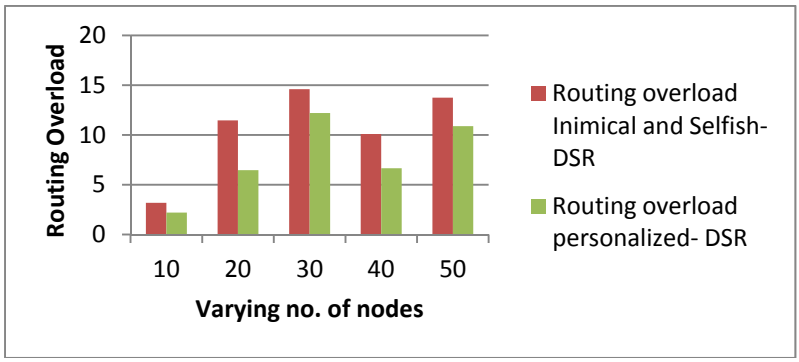

Fig. 6: Routing Overload with varying no. of nodes and pause time

The performance of personalized dynamic source routing protocol is much better when faced with selfish and inimical misbehaviour on the default dynamic source routing protocol.

5) Throughput: As according to varying number of nodes and varying pause time with fix maximum connection and rate.

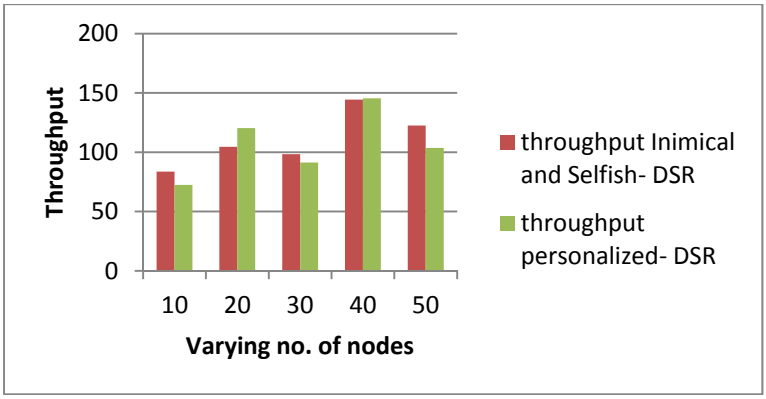

Fig. 7: Throughput with varying no of nodes and pause time

The throughput of personalized dynamic source routing protocol is way better compared to the selfish and inimical nodes dynamic source routing protocol when nodes are increase.

VI. CONCLUSIONS

In this paper we have implemented and analysed the performance of Dynamic source routing protocol over the selfish and inimical dynamic source routing protocol and personalized dynamic source routing protocol on the default dynamic source routing protocol installed in the network simulator. First performance is for introducing selfish and inimical nodes and finally through our personalized dynamic source routing protocol. The personalized dynamic source routing protocol reduce the end-to-end Delay and packet loss in the simulation result. In future we can introduce some more attacks and their remedies using other routing protocols.

REFERENCES

[1] G.Lavanya, A. Ebenezer jeyakumar," An Enhanced Secured Dynamic Source Routing Protocol for MANETs",Internation journal of soft computing and engineering(IJSCE) ISSN:2231-2307,volume X,Issue-4,September 2011.

[2] H. ZAFAR, L. HASAN, A. KHATTAK, Z. MUFTI, S. JAN, "Implementation of dynamic source routing protocol in network simulator 2",Sindh Univ. Res. Jour. (Sci. Ser.) vol.44(3) 491-496,2012.

[3] Sourav Ghosh & Chinmoy Ghorai," Evaluating the Performance of Modified DSR in Presence of NoisyLinks using QUALNET Network Simulator in MANET", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) ISSN No. 2248-9738 (Print) Volume-1, Issue-2, 2011.

[4] Disha G. Kariya,Atul B. Kathole,Sapna R. Heda,"Detecting Black and Gray Hole Attacks in Mobile Ad Hoc Network Using an Adaptive Method", International Journal of Emerging Technology and Advanced Engineering Website: www.ijetae.com (ISSN 2250-2459, Volume 2, Issue 1, January 2012).

[5] Reena Sahoo, Dr P.M khilar,"Detecting malicious nodes in manet based on a cooperative approach,", IJCA Special Issue on "2nd National Conference- Computing, Communication and Sensor Network" CCSN, 2011

[6] Dr. Nakkeeran, B.Partibane, S.Sakthivel Murugan, N.Prabagarane," Detecting the malicious faults in MANET".

[7] Payal N Raj, Prashant B. Swadas, "DPRAODV: A Dynamic Larning System Against Blackhole Attack in AODV Based MANET,"in IJCSI International Journal of Computer Science Issues, Vol. 2, 2009.

[8] Frank Kargl, Andreas Klenk, Stefan Schlott, Michael Weber, "Advanced Detection of Selfish or Malicious Nodes in Ad hoc Networks,"in University of UIm, Dep. Of Multimedia Computing, UIm, Germany.

[9] Aishwarya Sagar Anand Ukey, Meenu Chawla," Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET,"in IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 4, No. 1, July 2010.

[10] Radhika Saini and Manju Khari,"Defining Malicious Behavior of a Node and its Defensive Methods in Ad hoc Network, "in International Journal of Computer Applications (0975 – 8887) Volume 20– No.4, April 2011.

[11] Abdelaziz Babakhouya, Yacine Challal, and Abdelmadjid Bouabdallah, "A Simulation Analysis of Routing Misbehaviour in Mobile Ad hoc Networks," in Proc. of the Second International Conference on Next Generation Mobile Applications, Services, and Technologies, September 2008, pp. 592-597.

[12] D.B. Johnson, D.A. Maltz and J. Borch, "DSR : The Dynamic Source Routing Protocol for Multi-Hop Wireless Ad hoc Networks," Computer science department Carnegie Mellon university, Pittsburgh.

[13] NS-2, the NS Manual, Available at http://www. isi.edu/nsnam/ns/doc.

[14] J. Sen, M.G. Chandra, S.G. Harihara, H. Reddy, and P. Balamuralidhar, "A mechanism for detection of gray hole attack in mobile Ad hoc networks," in Proc. of the 6th International Conference on Information, Communications & Signal Processing, December 2007, pp. 1-5.

[15] Satoshi kurosawa ,Hidehisa Nakayama,Nei kato,Abbas Jamalipour, and Yoshiaki Nemoto," Detecting Blackhole Attack on AODV-based Mobile Ad hoc networks by Dyanamic Learning method," International Journal of Network Security, Vol.5, No.3, PP.338–346, Nov. 2007.

[16] D.B. Johnson, D.A. Maltz, and Y. Hu, "The Dynamic Source Routing Protocol for Mobile ad-hoc Networks (DSR)," IETF Internet Draft, July 2004.

[17] Muhammad Zeshan, Shoab A. Khan, Ahmad Raza Cheema, and Attique Ahmed, "Adding Security against Packet Dropping Attack in Mobile Ad hoc Networks," in 2008 International Seminar on Future Information Technology and Management Engineering, November 2008, pp. 568-572.

[18] Mohammad Al-Shurman, Seong-Moo Yoo, and Seungjin Park, "Black hole attack in mobile Ad hoc networks," in Proc. of the 42nd annual Southeast regional conference, ACM Southeast Regional Conference, April 2004, pp. 96–97.

[19] P. N. Raj and P. B. Swadas,"DPRAODV: A dynamic learning system against blackhole attack in AODV based MANET", Intl. Journal of Computer Science Issues (IJCSI), Vol. 2, Issue 3, pp: 54-59, 2009.

[20] J.W. Cai; P. Yi, Y. Tian, Y.K. Zhou, N. Liu," The Simulation and Comparison of Routing Attacks on DSR Protocol[C]", WiCOM 2009, in press.