iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** VII **Month of publication:** July 2017

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

Trust Based Routing for Dynamic Source Routing Protocol

Kiran Luhach[1]
[1] *M. Tech Scholar Department of Computer Science & Engineering BPS Mahila Vishvavidyalya Khanpur Kalan, Sonipat, Haryana, India*

Abstract: ***A Mobile ad hoc network (MANET) is a collection of nodes where each node transfer (forward) packets to each other for communication. Ad hoc Networks exposed to different attacks due to its characteristic like dynamic topology open medium, no central authority and no clear defence mechanism. One popular type of attack is blackhole attack where nasty node claim of having route of shortest length. It does so by sending a fake reply of route to the originator node. Due to this loss of data occurs & effects the network performance badly. In this propose work we determine the affect of presence of black hole in ad hoc network routing protocol Dynamic Source Routing (DSR) under the light of various parameters such as packet loss, throughput, and end-to-end delay with black hole and without black hole on DSR in MANET.***
Keywords: ***Adhoc Networks, Routing Protocols, DSR, Blackhole***

I. INTRODUCTION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connects and transfer information. A Mobile ad hoc network [1] is a group of wireless mobile computers (or nodes); in which nodes collaborate by forwarding packets for each other to allow them to communicate outside range of direct wireless transmission. The ad hoc networks does not require access point such as predetermined infrastructure. They also does not require any centralized administrator such as base station. The ad hoc networks can be set up easily whenever required and that too with low cost.

A Mobile Ad hoc Network is an independent group of mobile users communicating with each other on wire-less links. As the nodes on MANET are mobile therefore topology of these networks change frequently from time to time. In MANET, a node can acts as either intermediate node or source/destination node. When it acts as intermediate node then it receives the packets for some destination node and send back to closet neighbour. As the nodes are not fixed therefore the topology of ad hoc networks is not fixed and not changes over time.

There are different application areas of MANET. Some of them are- battlefield communication, emergency search-rescue operations and meeting events. From the above applications we can conclude that MANET becomes the essential part of mobile computation. In this propose work we determine the affect of presence of black hole in ad hoc network routing protocol Dynamic Source Routing (DSR) under the light of various parameters such as packet loss, throughput, and end-to-end delay with black hole and without black hole on DSR in MANET.

II. ROUTING IN MANET

A Mobile ad hoc network (MANET) is a collection of nodes where each node transfer (forward) packets to each other for communication. Ad hoc Networks exposed to different attacks due to its characteristic like dynamic topology open medium, no central authority and no clear defence mechanism [2][3].

A. Properties of Ad-Hoc Routing Protocols

The properties that are desirable in Ad-Hoc Routing protocols are:

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

i) Distributed operation: The protocol should be distributed. It should not be dependent on a centralized controlling node. This is the case even for stationary networks. The dissimilarity is that the nodes in an ad-hoc network can enter or leave the network very easily and because of mobility the network can be partitioned.

ii) Loop free: To improve the overall performance, the routing protocol should assurance that the routes supplied are loop free. This avoids any misuse of bandwidth or CPU consumption.

iii) Demand based operation: To minimize the control overhead in the network and thus not misuse the network resources the protocol should be reactive. This means that the protocol should react only when needed and should not periodically broadcast control information.

iv) Unidirectional link support: The radio environment can cause the formation of unidirectional links. Utilization of these links and not only the bi-directional links improves the routing protocol performance.

v) Security: The radio environment is especially vulnerable to impersonation attacks so to ensure the wanted behavior of the routing protocol we need some sort of security measures. Authentication and encryption is the way to go and problem here lies within distributing the keys among the nodes in the ad-hoc network [4].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

vi) Power conservation: The nodes in the ad-hoc network can be laptops and thin clients such as PDA_s that are limited in battery power and therefore uses some standby mode to save the power. It is therefore very important that the routing protocol has support for these sleep modes.

vii) Multiple routes: To reduce the number of reactions to topological changes and congestion multiple routes can be used. If one route becomes invalid, it is possible that another stored route could still be valid and thus saving the routing protocol from initiating another route discovery procedure.

viii) Quality of Service Support: Some sort of Quality of service is necessary to incorporate into the routing protocol. This helps to find what these networks will be used for.

B. Problems in routing with Mobile Ad hoc Networks

Main problems in routing with MANETs are explained below [3]:

1) *Asymmetric links:* Most of the wired networks rely on the symmetric links which are always fixed. But this is not a case with ad-hoc networks as the nodes are mobile and constantly changing their position within network.
2) *Routing Overhead:* In wireless ad hoc networks, nodes often change their location within network. So, some stale routes are generated in the routing table which leads to unnecessary routing overhead.
3) *Interference:* This is the major problem with mobile ad-hoc networks as links come and go depending on the transmission characteristics, one transmission might interfere with another one and node might overhear transmissions of other nodes and can corrupt the total transmission.
4) *Dynamic Topology:* Since the topology is not constant; so the mobile node might move or medium characteristics might change. In ad-hoc networks, routing tables must somehow reflect these changes in topology and routing algorithms have to be adapted. For example in a fixed network routing table updating takes place for every 30sec. This updating frequency might be very low for ad-hoc networks [5].

III. MANETS ROUTING PROTOCOLS

Classification of routing protocols in mobile ad hoc network can be done in many ways, but most of these are done depending on routing strategy and network structure. The routing protocols can be categorized as flat routing, hierarchical routing and geographic position assisted routing while depending on the network structure. According to the routing strategy routing protocols can be classified as Table-driven and source initiated (figure 1) [6].

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue VIII, July 2017- Available at www.ijraset.com

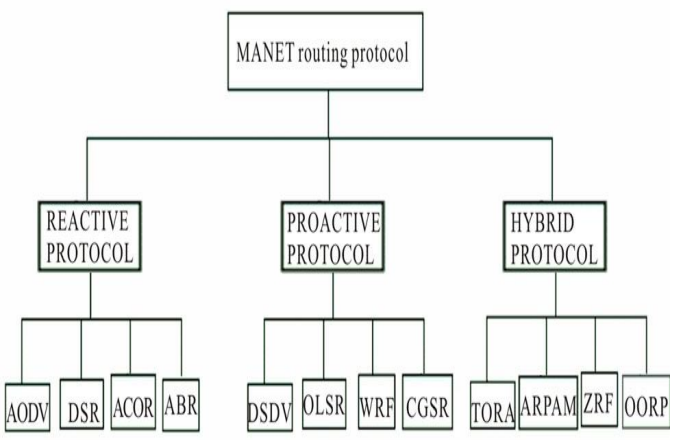


Figure 1: MANETs Routing Protocol

Flat routing protocols are divided mainly into two classes; the first one is proactive routing (table driven) protocols and other is reactive (on-demand) routing protocols. One thing is general for both protocol classes is that every node participating in routing play an equal role. They have further been classified after their design principles; proactive routing is mostly based on LS (link-state) while on-demand routing is based on DV (distance-vector).

A. Proactive Routing Protocols

Proactive MANET's protocols are also called as table-driven protocols and will actively determine the layout of the network. The nodes, however, continue to expend energy by continually updating these unused entries in their routing tables as mentioned, energy conservation is very important in a MANET system design. Therefore, this excessive expenditure of energy is not desired. Thus, proactive MANET protocols work best in networks that have low node mobility or where the nodes transmit data frequently.

Examples of Proactive MANET Protocols include

1) Optimized Link State Routing (OLSR)
2) Fish-eye State Routing (FSR)
3) Destination-Sequenced Distance Vector (DSDV)
4) Cluster-head Gateway Switch Routing Protocol (CGSR)

B. Reactive (On Demand) protocols

Portable nodes- Notebooks, palmtops or even mobile phones usually compose wireless ad-hoc networks. This portability also brings a significant issue of mobility. This is a key issue in ad-hoc networks. The mobility of the nodes causes the topology of the network to change constantly. Keeping track of this topology is not an easy task, and too many resources may be consumed in signaling. Reactive routing protocols were intended for these types of environments. These are based on the design that there is no point on trying to have an image of the entire network topology, since it will be constantly changing. Instead, whenever a node needs a route to a given target, it initiates a route discovery process on the fly, for discovering out a pathway .Reactive protocols start to set up routes on-demand. The routing protocol will try to establish such a route, whenever any node wants to initiate communication with another node to which it has no route. This kind of protocols is usually based on flooding the network with RouteRequest (RREQ) and Routereply (RERP) messages .By the help of Routerequest message the route is discovered from source to target node; and as the target node gets a RREQ message it send RERP message for the confirmation that the route has been established. This kind of protocol is usually very effective on single-rate networks. It usually minimizes the number of hops of the selected path. However, on multi-rate networks, the number of hops is not as important as the throughput that can be obtained on a given path.

The different types of On Demand driven protocols are

1) Ad hoc On Demand Distance Vector (AODV)
2) Dynamic Source routing protocol (DSR)
3) Temporally ordered routing algorithm (TORA)

4) Associativity based routing (ABR)
5) Signal Staility-Based Adaptive Routing (SSA)
6) Location-Aided Routing Protocol (LAR)

C. Hybrid Routing Protocols

As the size of the wireless network increases, the flat routing protocols may produce too much overhead for the MANET. In this case a hierarchical solution may be preferable. Since proactive and reactive protocols each work best in oppositely different scenarios, hybrid method uses both. It is used to find a balance between both protocols. Proactive operations are restricted to small domain, whereas, reactive protocols are used for locating nodes outside those doains. Examples of hybrid protocols are:

1) Zone Routing Protocol, (ZRP)
2) Wireless Ad hoc Routing Protocol, (WARP)

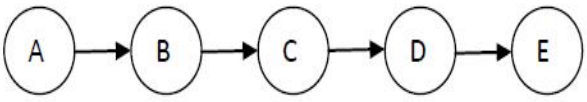
IV. DYNAMIC SOURCE ROUTING (DSR)

Dynamic Source Routing (DSR) [4] is a routing protocol for wireless mesh networks. It is similar to AODV [7] in that it establishes a route on-demand when a transmitting mobile node requests one. However, it uses source routing instead of relying on the routing table at each intermediate device. Dynamic source routing protocol (DSR) is an on-demand, source routing protocol, whereby all the routing information is maintained (continually updated) at mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. The protocol is composed of the two main mechanisms of "Route Discovery" and "Route Maintenance", which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network.

An optimum path for a communication between a source node and target node is determined by Route Discovery process. Route Maintenance ensures that the communication path remains optimum and loop-free according the change in network conditions, even if this requires altering the route during a transmission. Route Reply would only be generated if the message has reached the projected destination node (route record which is firstly contained in Route Request would be inserted into the Route Reply).To return the Route Reply, the destination node must have a route to the source node. If the route is in the route cache of target node, the route would be used. Otherwise, the node will reverse the route based on the route record in the Route Reply message header (symmetric links).

In the event of fatal transmission, the Route Maintenance Phase is initiated whereby the Route Error packets are generated at a node. The incorrect hop will be detached from the node's route cache; all routes containing the hop are reduced at that point. Again, the Route Discovery Phase is initiated to determine the most viable route. The major dissimilarity between this and the other on-demand routing protocols is that it is beacon-less and hence it does not have need of periodic hello packet (beacon) transmissions, which are used by a node to inform its neighbours of its presence. The fundamental approach of this protocol during the route creation phase is to launch a route by flooding Route Request packets in the network. The destination node, on getting a Route Request packet, responds by transferring a RouteReply packet back to the source, which carries the route traversed by the RouteRequest packet received [8][9].

During route maintenance, S detects the link failures along the path. If it happens, it repairs the broken links. Otherwise, when the source route is completely broken, S will restart a new discovery (figure 2).



1. A----->B : (A) ID=2
2. B---- > C: (A, B) ID=2
3. C---->D :(A, B, C) ID=2
4. D----> E :(A, B, C, D) ID=2

Figure 2: Route Discovery process

To initiate the Route Discover in the above figure, the source transmits a ROUTE REQUEST (RREQ) message as a single local Broadcast packet, which is received by (approximately) all nodes currently within wireless transmission range of source [10]. When another node receives a RREQ, if it is the target of the Route Discovery, it returns a ROUTE REPLY (RREP) message to the initiator of the Route Discovery, giving a copy of the accumulated route record from the RREQ; when the initiator receives this ROUTE REPLY, it caches this route in its Route Cache for use in sending subsequent packets to this destination. Otherwise, if this node receiving the RREQ has recently seen another RREP message from this initiator bearing this same request id, or if it finds that its own address is already listed in the route record in the RREQ message, it discards the REQUEST. Otherwise, this node appends its own address to the route record in the ROUTE REQUEST message and propagates it by transmitting it as a local broadcast packet with the same request id. Route Maintenance is the mechanism by which source node is able to detect, while using a source route to destination node, if the network topology has changed such that it can no longer use its route to destination node because a link along the route no longer works.

When Route Maintenance indicates a source route is broken, source node can attempt to use any other route it happens to know to destination node, or can invoke Route Discovery again to find a new route. Route Discovery and Route Maintenance each operate entirely on demand. For example, DSR does not use any periodic routing advertisement, link status sensing, or neighbor detection packets, and does not rely on these functions from any underlying protocols in the network. This entirely on-demand behavior and lack of periodic activity allows the number of overhead packets caused by DSR to scale all the way down to zero, when all nodes are approximately stationary with respect to each other and all routes needed for current communication have already been discovered (figure 3).

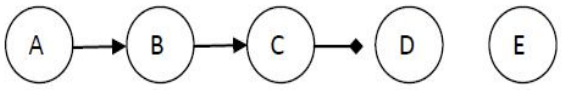


Figure 3: Route Maintenance Process

As nodes begin to move more or as communication patterns change, the routing packet overhead of DSR automatically scales to only that needed to track the routes currently in use. In response to a single Route Discovery (as well as through routing information from other packets Overheard), a node may learn and cache multiple routes to any destination. This allows the reaction to routing changes to be much more rapid, since a node with multiple routes to a destination can try another cached route if the one it has been using should fail. This caching of multiple routes also avoids the overhead of needing to perform a new Route Discovery each time a route in use breaks.

When originating or forwarding a packet using a source route, each node transmitting the packet is responsible for confirming that the packet has been received by the next hop along the source route; the packet is retransmitted (up to a maximum number of attempts) until this confirmation of receipt is received. For example, in the above figure, node A has originated a packet for E using a source route through intermediate nodes B, C and D. In this case, node A is responsible for receipt of the packet at B, node B is responsible for receipt at C, node C is responsible for receipt at D, and node D is responsible for receipt finally at the destination E. This confirmation of receipt in many cases may be provided at no cost to DSR, either as an existing standard part of the MAC protocol in use such as the link-level acknowledgement frame defined by IEEE 802.11 or by a *passive* acknowledgement.

If neither of these confirmation mechanisms are available, the node transmitting the packet may set a bit in the packet's header to request a DSR-specific software acknowledgement be returned by the next hop; this software acknowledgement will normally be transmitted directly to the sending node, but if the link between these two nodes is uni-directional, this software acknowledgement may travel over a different, multi-hop path. If the packet is retransmitted by some hop the maximum number of times and no receipt confirmation is received, this node returns a ROUTE ERROR message to the original sender of the packet, identifying the link over which the packet could not be forwarded.

he operation of Route Discovery and Route Maintenance in DSR are designed to allow uni-directional links and asymmetric routes to be easily supported. In particular, in wireless networks, it is possible that a link between two nodes may not work equally well in both directions, due to differing antenna or propagation patterns or sources of interference. DSR allows such uni-directional links to be used when necessary, improving overall performance and network connectivity in the system. DSR also supports internetworking between different types of wireless networks, allowing a source route to be composed of hops over a combination of any types of networks available. A node forwarding or overhearing any packet may add the routing information from that packet to its own

Route Cache. In particular, the source route used in a data packet, the accumulated route record in a ROUTE REQUEST, or the route being returned in a ROUTE REPLY may all be cached by any node.

V. PROPOSED WORK

In the previous research there are multiple schemes provided to find the truth values of individual nodes that describe the reliability, trustworthiness and availability of the node. One of the main issues related to MANET is secure routing. A black hole attack [11] degrades the performance of wireless networks such as MANET. In order to attain security in routing it is compulsory to compute trust value of nodes without any centre authority.

A common solution provided by the researchers is as follows: when a node initiating route discovery determines the required minimal trust level for nodes participating in the query and reply propagation. Since only nodes at each trust level share symmetric encryption keys, intermediate nodes of different trust levels cannot decrypt in-transit routing packets or determine whether the required security attributes can be satisfied. Only the nodes with the correct key can read the header and forward the packet. So if a packet has reached the destination, then it must have been propagated by nodes at the same trust level. Therefore Routes discovered by trust aware routing comes with "quality of protection" guarantees.

In this research, we propose a new approach based on relationship among the mobile nodes which makes them to cooperate in an infrastructure-less environment. The faith unit is used to calculate the faith values of each node in the network. The calculated faith values are being used by the relationship estimator to determine the relationship status of mobile nodes. The proposed enhanced protocol was compared with the standard DSR protocol and the results are analyzed using the MATLAB [12].

Here we are proposing a secure routing technique to deliver the data packets from source to destination.

VI. PROPOSED WORK

We have 10 nodes for simulation and traffic type is random waypoint, where percentage of malicious node is 10% i.e. one node will act as blackhole in this simulation. The area for simulation is 50 m X 50 m.

The assumptions are node 1 will act as source and node 10 will act as destination, whereas node 9 will act as blackhole.

Figure 4 below shows the routing in secure DSR protocol. The black node is represented by red circle.

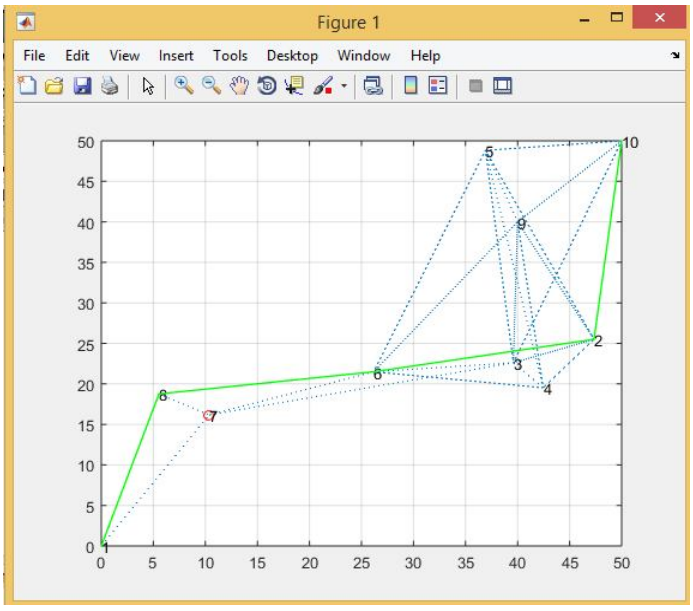


Figure 4: Routing in secure DSR protocol.

Figure 5 below shows the distance taken from source to destination by secure DSR and Normal DSR. It is clear that secure DSR covers less distance.

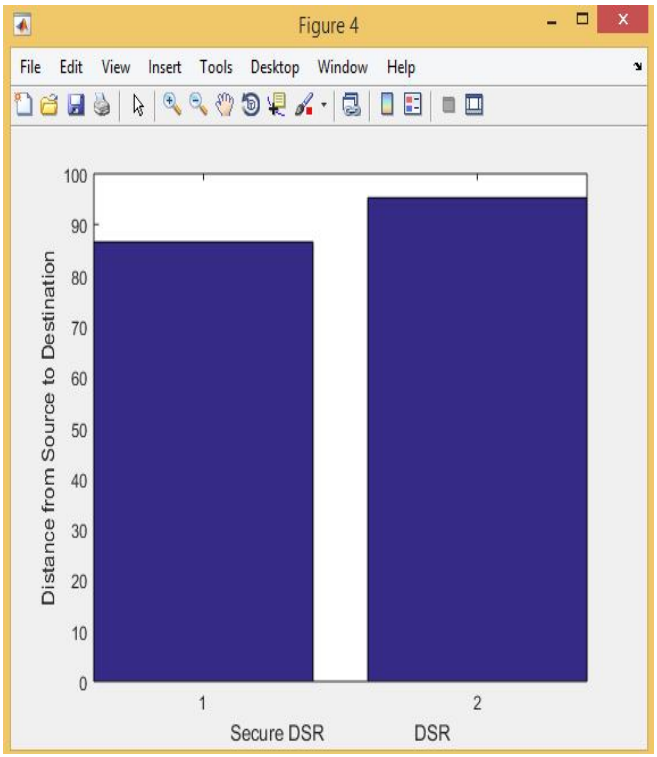


Figure 5: Distance taken from source to destination

Figure 6 below shows the computation time taken by secure DSR and normal DSR. The secure DSR takes less time as compared to normal DSR.

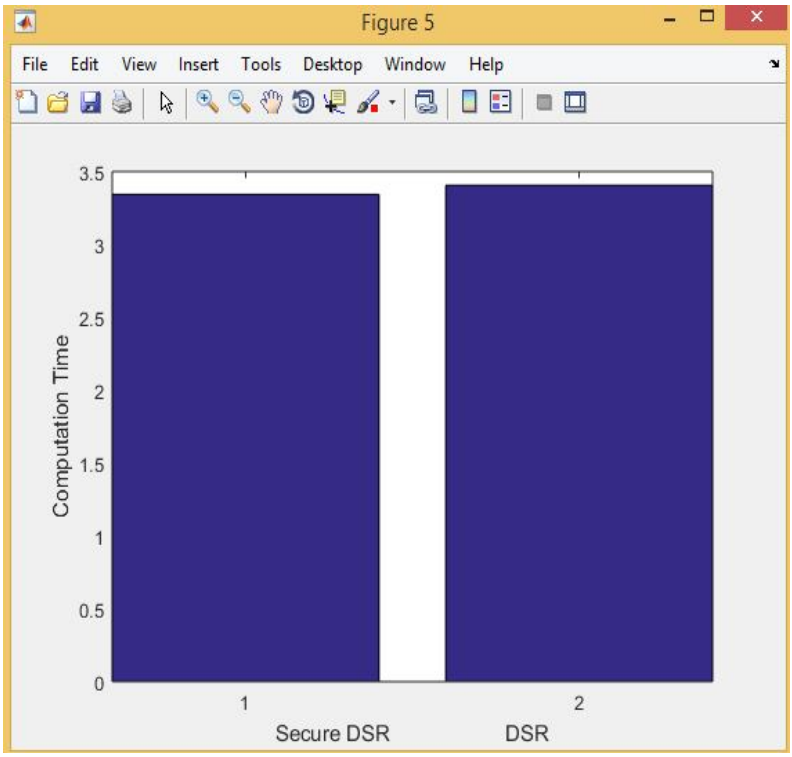


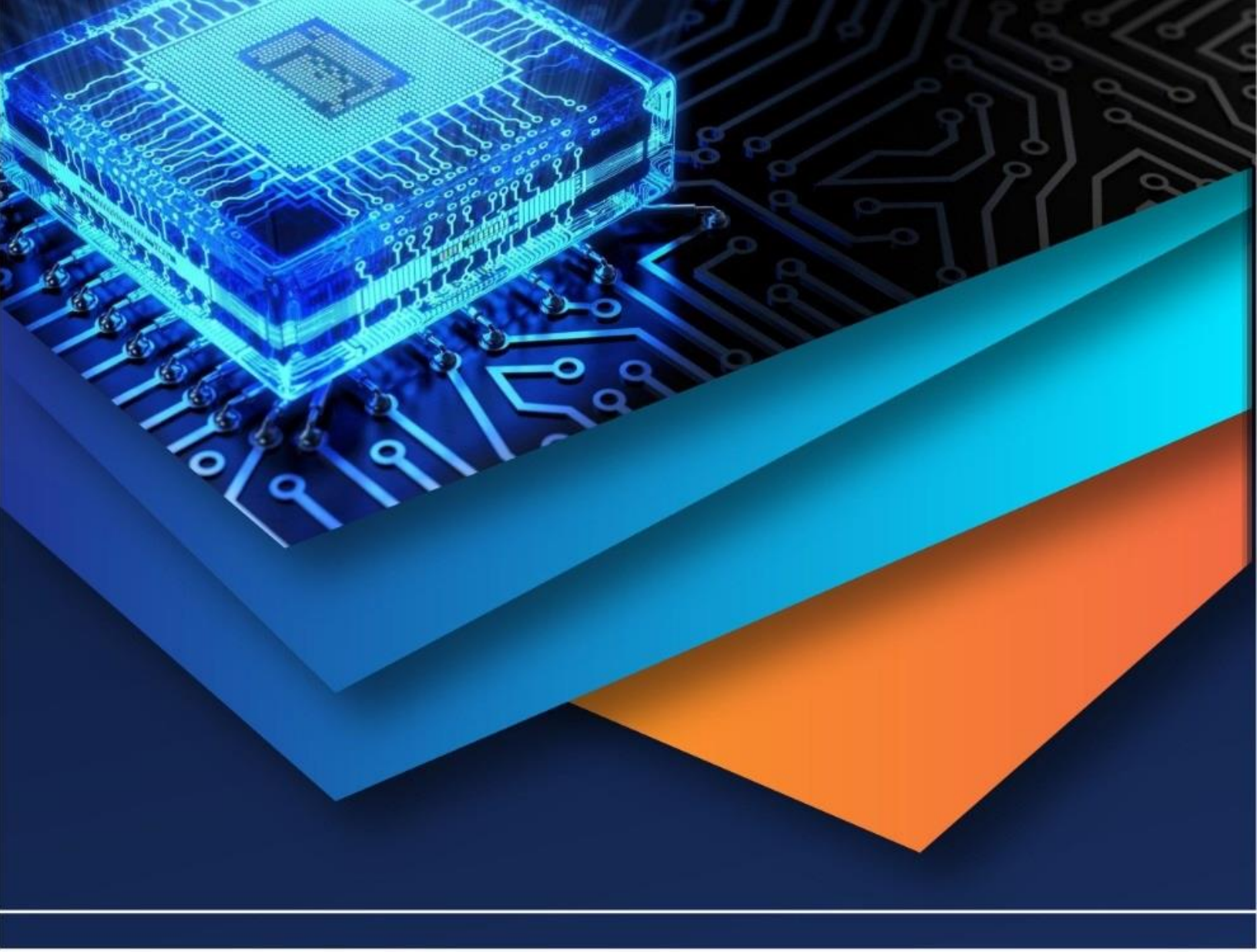
Figure 6 below shows the computation time taken by secure DSR and normal DSR

VII. CONCLUSION

Mobile Ad-hoc network is a set of wireless devices called wireless nodes, which dynamically connects and transfer information. In this paper, we have proposed a scheme to select secure route for data forwarding. This technique will avoid interception of messages through black hole nodes. We have compared our results with DSR routing protocol, the results showed that Secure DSR will avoid routing of packets through black hole nodes.

REFERENCES

[1] Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi, "A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)", International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013
[2] Kimaya Sanzgiri, Bridget Dahill, "A Secure Routing Protocol for Ad Hoc Networks", Proceedings of the 10th IEEE International Conference on Network Protocols (ICNP'02) 1092-1648/02 $17.00 © 2002 IEEE
[3] Anuj K. Gupta, Harsh Sadawarti, and Anil K. Verma, "Review of Various Routing Protocols for MANETs", International Journal of Information and Electronics Engineering, Vol. 1, No. 3, November 2011
[4] K. Selvavinayaki, K. K. Shyam Shankar, Dr. E. Karthikeyan "Security Enhanced DSR Protocol to Prevent Black Hole Attacks in MANETs" International Journal of Computer Applications (0975 – 8887) Volume 7– No.11, October 2010
[5] M. Guerrero Zapata and N. Asokan, "Securing Ad Hoc Routing Protocols," Proc. ACM Workshop on Wireless Security (WiSe), ACM Press, 2002, pp. 1–10.
[6] Neetendra Singh Dhakad, Anjana Goen, "Review on Routing Protocols of Mobile Ad-hoc Network MANET", International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering Vol. 5, Issue 4, April 201
[7] Mikita V. Talati, Sharada Valiveti, and K. Kotecha, "Trust Based Routing in Ad Hoc Network", FGCN 2010, Part II, CCIS 120, pp. 381–392, 2010.
[8] Rajesh Sharma Seema Sabharwal, "Dynamic Source Routing Protocol (DSR)", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013
[9] Ramandeep Singh, Farminder Singh, "Review Paper on Enhancement in DSR Protocol For Multicasting in Manet", International Research Journal of Engineering and Technology (IRJET) Volume: 03 Issue: 05 | May-2016
[10] S. Geetha Dr. G. Geetha Ramani, "Survey of Trust Based Routing Protocols in MANET", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 4, Issue 10, October 2014
[11] Jaspal Kumar, M. Kulkarni, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols", I. J. Computer Network and Information Security, 2013, 5, 64-7
[12] MATLAB Applications for the Practical Engineer by Kelly Bennett, InTech, 2014



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY