Volume 3, Issue 1, January 2016 ISSN: 2348-8565 (Online)

International Journal of Modern Engineering and Research Technology

Website: http://www.ijmert.org Email: editor.ijmert@gmail.com

# Effect of Selfish Behavior of Misbehaving Nodes on DSR in Mobile Ad-hoc Network

**Rohan Rajoriya**
*Lecturer-Information Technology*
*Printing Technology Department*
*Govt. Kalaniketan Polytechnic College*
*Jabalpur (M.P.), [INDIA]*
*Email: rohan.rajoriya@rediffmail.com*

## ABSTRACT

*With the recent technological advancements in the field of Mobile AdHoc Networks[7], their utility has increased by leaps and bounds. MANETs find their use particularly in the field where infrastructured network are not possible without having any centralized administration. Where this feature helps in rapidly Deploying and establishing the AdHoc networks, it makes it highly susceptible for attacks by the malicious and the selfish nodes present in and around the network.*

***Keywords:—****Mobile computing, Protocols, Wireless, DSR, Protocol design and analysis.*

## I. INTRODUCTION

In the recent years, wireless technology has enjoyed a tremendous rise in popularity and usage, thus opening new fields of applications in the domain of networking. One of the most recent advancements has been in the field of mobile ad hoc networks (MANETs), where the participating nodes do not rely on any existing network infrastructure. A mobile ad hoc network is a collection of wireless nodes that can be rapidly deployed as a multi-hop packet radio network without the aid of any existing network infrastructure or centralized administration. Nodes within each other's radio range communicate directly via wireless links, while those that are further apart use other nodes as relays.

Generally there are two distinct approaches for enabling wireless mobile units to communicate with each other as described below and shown in **figure 1**:

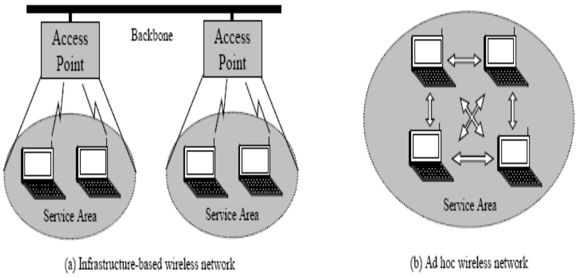
Access Point
Backbone
Access Point
Service Area
Service Area
Service Area
(a) Infrastructure-based wireless network
(b) Ad hoc wireless network

**Figure 1:** Infrastructure-based and infrastructure less wireless networks

1. ***Infrastructured.*** Wireless mobile networks have traditionally been based on the cellular concept and relied on good infrastructure support, in which mobile devices communicate with access points like base stations connected to the fixed network infrastructure. Typical examples of this kind of wireless networks are GSM, UMTS, WLL, WLAN, etc.

2. ***Infrastructureless.*** As to infrastructureless approach, the mobile wireless network is commonly known as a mobile ad hoc network (MANET). A MANET is a collection of wireless

nodes that can dynamically form a network to exchange information without using any pre-existing fixed network infrastructure. This is a very important part of communication technology that supports truly pervasive computing, because in many contexts information exchange between mobile units cannot rely on any fixed network infrastructure, but on rapid configuration of a wireless connections on-the-fly. A mobile ad hoc network is a collection of wireless nodes that can dynamically be set up anywhere and anytime without using any pre -existing network infrastructure. It is an autonomous system in which mobile hosts connected by wireless links are free to move randomly and often act as routers at the same time. The traffic types in ad hoc networks are quite different from those in an infrastructure-based wireless network.

## II. Related Work

**Sonja Buchegger and Jean-Yves Le Boudec**, proposed **CONFIDANT[1][2]**,for making misbehavior unattractive; based on selective altruism and utilitarianism. It aims at detecting and isolating misbehaving nodes, thus making it unattractive to deny cooperation. Trust relationships and routing decisions are based on experienced, observed, or reported routing and forwarding behavior of other nodes. The implementation of CONFIDANT, assumes that the network layer is based on the Dynamic Source Routing (DSR) protocol. It shows that a network with CONFIDANT and up to 60% of misbehaving nodes behaves almost as well as a benign network, in sharp contrast to a defenseless network.

**Zhiyong Shi, Shenquan Zhu, and Zhenyu Zhang [4]** introduced the Dynamic Source Routing (DSR) protocol, and proposed a scheme of building a mobile communication network which is based on the DSR protocol. And, the handover mechanism of the network is the soft handover mode with MS's assistance. Through an example and simulation, it is shown that the mobile communication network has the entire mobility after adopting the DSR protocol, while the requirement of the communication can be satisfied in such network.

**Rendong Bai and Mukesh Singhal [5]**, Fellow, IEEE, presented a lightweight hierarchical routing model, Way Point Routing (WPR), in which a number of intermediate nodes on a route are selected as waypoints and the route is divided into segments by the waypoints. One distinct advantage of this model is that when a node on the route moves out or fails, instead of discarding the whole original route and discovering a new route from the source to the destination, only the two waypoint nodes of the broken segment have to find a new segment. In addition, the model is lightweight because it maintains a hierarchy only for nodes on active routes.

**Asad Amir Pirzada and Chris McDonald [6]** presented a variant of the DSR protocol in which intermediary nodes act as Trust Gateways. These gateways take into account the contemporary trust levels of the network nodes and thus facilitate in detecting and evading malicious nodes. Extensive simulations, demonstrates that the proposed DSR protocol augments the performance of the standard DSR protocol by up to 30% in a network where 40% of the nodes act maliciously. The proposed scheme is also independent of cryptographic mechanisms and does not impose any superfluous conditions upon the network establishment and operation phase.

## III. Routing Concepts

Routing is the act of moving information from a source to a destination in an internetwork. During this process, at least one intermediate node within the internetwork is encountered. The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an internetwork. The later concept is called as packet switching which is straight forward, and the path determination could be very complex. Routing protocols use several metrics to calculate the best path for routing the packets to its destination. These metrics are a standard measurement that could be number of hops, which is used by the routing algorithm to determine the optimal path for the packet to its destination. The process of path determination is that, routing algorithms initialize and maintain routing tables, which contain the total route information for the packet. This route information varies from one routing algorithm to another. Routing tables are filled with a variety of information which is generated by the routing algorithms. Most common entries in the routing table are ip-address prefix and the next hop. Routing table's Destination/next hop associations tell the router that a particular destination can be reached optimally by sending the packet to a router representing the "next hop" on its way to the final destination and ip-address prefix specifies a set of destinations for which the routing entry is valid for.

- Routing protocols in MANET's are primarily classified depending on:
- Routing/Network structure.
- Routing strategy
- Routing information

***Depending on the network structure routing protocols are classified as:***

- Flat routing – no assumption for subnetting, no correlation in addressing
- Hierarchical routing- involves subnetting, cluster formation, hierarchical addressing
- Geographic position assisted routing. - routing based on geographic position of nodes.

***According to the routing strategy the routing protocols can be categorized as:***

Table-driven (Proactive)

On-Demand or source initiated (Reactive)

Hybrid (mix of proactive and reactive)

### *Dynamic Source Routing Protocol*

The Dynamic Source Routing Protocol is a source-routed on-demand routing protocol. A node maintains route caches containing the source routes that it is aware of. The node updates entries in the route cache as and when it learns about new routes. The two major phases of the protocol are: route discovery and route maintenance. When the source node wants to send a packet to a destination, it looks up its route cache to determine if it already contains a route to the destination. If it finds that an unexpired route to the destination exists, then it uses this route to send the packet. But if the node does not have such a route, then it initiates the route discovery process by broadcasting a route request packet. The route request packet contains the address of the source and the destination, and a unique identification number. Each intermediate node checks whether it knows of a route to the destination. If it does not, it appends its address to the route record of the packet and forwards the packet to its neighbors. To limit the number of route requests propagated, a node processes the route request packet only if it has not already seen the packet and it's address is not present in the route record of the packet. A route reply is generated when either the destination or an intermediate node with current information about the destination receives the route request packet. A route request packet reaching such a node already contains, in its route record, the sequence of hops taken from the source to this node.

### *Routing Attacks*

An act that leads to breach of security of information can be considered as a threat & the possible attack. Since routing is the backbone of the network layer functioning, thus any disrupting the routing mechanism – route discovery or route maintenance, will virtually lead to failure of the network layer functioning, required to provide & extend connectivity beyond the one hop nodes, across entire network. Thus the attacks over the network layer are centered in & around the routing mechanism.

Primarily attacks can be classified as: (i) Internal attacks – attacks due to one or more compromised nodes with the network to which the particular node belongs to. (ii) External attacks – attacks breaching the security of the network by the nodes not belonging to the same network, rather some external nodes outside the network.

## IV. Result Analysis

### Behavioral Analysis of Malicious and Selfish Nodes on DSR

### *Effect of Malicious Nodes*

### *I. Throughput of Sending Bits Vs End-to-End Delay*

Graphical representation of DSR for throughput of sending bits reveals the following points:

1. Their occurs an initial delay of 0.0152 seconds in DSR at $0.4*10^4$ throughput.
2. The maximal delay for the considered throughput range from $0.4 \times 10^4$ to $2.8 \times 10^4$ is 0.0242 secs and 0.0164 secs respectively for DSR.
3. In case of DSR the maximal delay of 0.0242 secs occurs at throughput $1.6 \times 10^4$ bits/TIL.
4. Careful analysis of DSR reveals that there occurs an increase in delay after $2.45 \times 10^4$ bits/TIL.
5. By varying percentage of Malicious Nodes in DSR following observations are made:
6. The End-to-End delay increases as the percentage of Malicious Nodes increases.

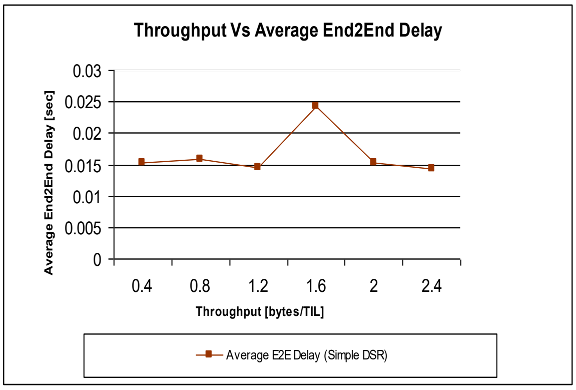

*Figure 2: Throughput of Sending Bits Vs End-to-End Delay with all normal nodes for DSR*

The misbehaving activity of the Malicious Nodes is seen to impact the performance of network even for 5% malicious nodes occurrences and increases successively for 10%, 25%, and 50% and so on. As for 5%, 10% and 50% malicious nodes, End-to-End delays for the transmission of data packets at 0.4 throughput is 0.0143, 0.0143 and 0.017 respectively as depicted in **Figure 3**.

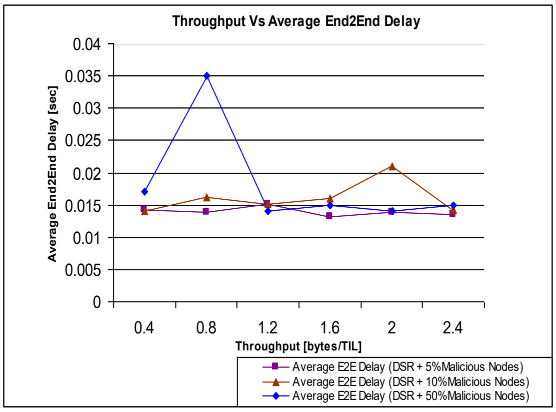

*Figure 3: Throughput of Sending Bits Vs End-to-End Delay with 15%, 25% and 50% Malicious nodes for DSR*

Conventionally with the increase in the transmitted data packets the throughput also increases irrespective of the presence or absence of malicious nodes, but the increase in the throughput in case of the malicious nodes occurs at the cost of increasing End-to-End delay.

The initial rise of [0.018 / 0.4 x $10^4$] for 50% malicious nodes is much steeper as compared to DSR without any malicious nodes, DSR with 10%, 25%, etc malicious nodes indicating the increase in the time required for each data packet to be transmitted at the transmitting site. This increase in the time required with increasing data packets under the influence of malicious nodes can be explained as follows:

Since the malicious nodes responds positively to all the route requests from the sender, thus it may happen that these malicious nodes might be operating in a cooperative manner resulting in wormhole, black hole or gray hole attacks.

By the very nature of these attacks it happens that the transmitted data packets are either completely dropped due to black hole phenomenon or even if these packets are transmitted, its occurs with increasing time delay as compared to network with all the normal nodes due to wormhole phenomenon.

Looking at the given network condition the 50% malicious node activity results in a peak delay of 0.035 secs at just 0.8 x $10^4$ throughput as compared to 0.0167 secs at throughput of 2.45 x $10^4$ and 0.0195 secs at throughput of 2.45 x $10^4$ for 15% and 25% malicious nodes indicating lesser amount of data packets transmitted under the similar simulation conditions but varying percentage of malicious nodes as shown in **Figure 4**.

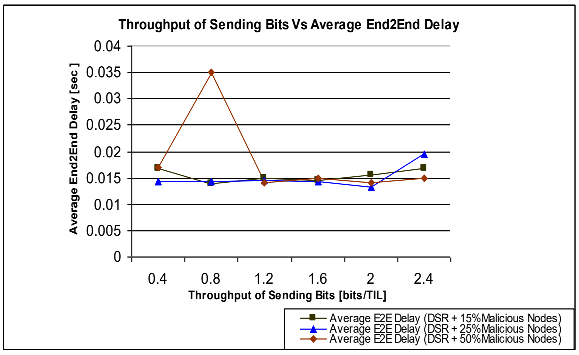

*Figure 4: Throughput of Sending Bits Vs End-to-End Delay with 15%, 25% and 50% malicious nodes for DSR*

## II. Throughput of Receiving Bits Vs End-to-End Delay

The analysis has been based considering the same packet size.

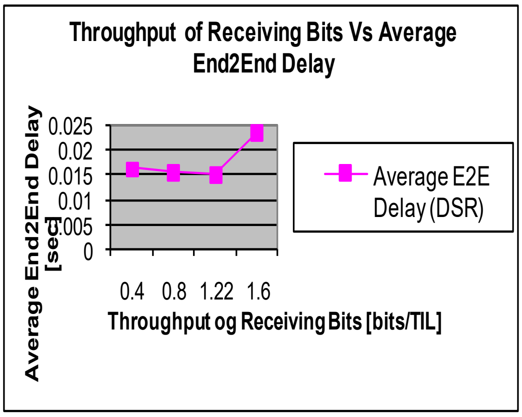

*Figure 5: Throughput of Receiving Bits Vs End-to-End Delay with all normal nodes for DSR*

Analyzing the **Figure 5** of “throughput of receiving bits vs. average End-to-End delay” without any abnormal behaving node following points are observed: Initially for DSR there occurs a fall in E2E delay with the increasing throughput in DSR as more data packets are received with reducing delays. **Figure 6** reveals the effect of just 10% malicious nodes as:

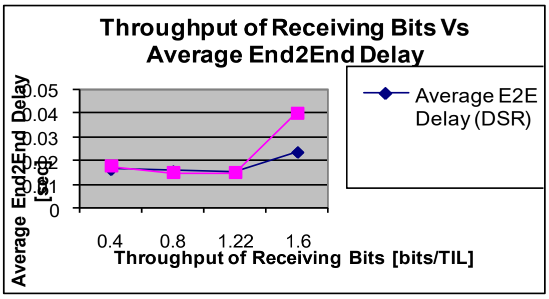

*Figure 6: Throughput of Receiving Bits Vs End-to-End Delay with all normal nodes and 10% malicious nodes for DSR.*

Due to the malicious node attack, its being observed that in case of DSR where the initial/first breakpoint occurs at 0.8 throughput in case of DSR + Malicious first breakpoint occurs at the same level but the initial delay is higher in case of DSR + Malicious as compared to DSR, moreover as the protocol demands that average delay should be minimum or at least should reduce with the time and throughput to use the specified route efficiently, but in case of DSR + Malicious, at 0.8 throughput the average delay is on rising side till 1.22 throughput as compared to DSR where its falling, indicating the rise in the dropping packets in the way from sender to receiver.

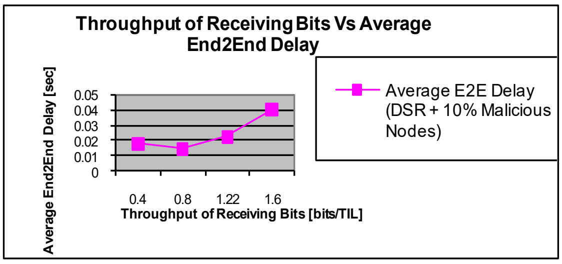

*Figure 7: Throughput of Receiving Bits Vs End-to End Delay with 10% malicious nodes for DSR.*

Due to the malicious node attack, its being observed that in case of DSR where the initial/first breakpoint occurs at 0.8 throughput in case of DSR + Malicious first breakpoint occurs at the same level but the initial delay is higher in case of DSR + Malicious as compared to DSR, moreover as the protocol demands that average delay should be minimum or at least should reduce with the time and throughput to use the specified route efficiently, but in case of DSR + Malicious, as 0.8 throughput the average delay is on rising side till 1.22 throughput as compared to DSR where its falling, indicating the rise in the dropping packets in the way from sender to receiver.

Due to the malicious behavior of the node, there occurs a considerable increase in the amount of delay with increasing malicious activity. This is fact is further strengthen by the simulation results as by increasing the malicious node from 0 % to 10%, there is an increase in delay for the throughput of 1.6 x $10^4$ by nearly 37% and even suggested Figure 1 and Figure 4 has 25% DSR + Malicious case.

But however this strictly analysis is particularly seen at higher T.P it can be seen that after the T.P of nearly 0.8 x $10^4$ there occurs a sharp increase in delay in all the cases mentioned above. This is due to the fact that initially delays of higher malicious nodes will be higher, due to all verifying scheme, thus higher the malicious node greater the delays, thus lesser packet received with higher delays. After this delay decreases with higher malicious node activities due to above mentioned scenario where as in 10% it remains fairly constant.

## *Effect of Selfish Nodes*

### *I. Throughput of Sending Bits Vs End-to-End Delay*

The effect of selfish nodes, which purposely drops the request packets, can be analyzed with the help of **Figure 8**.

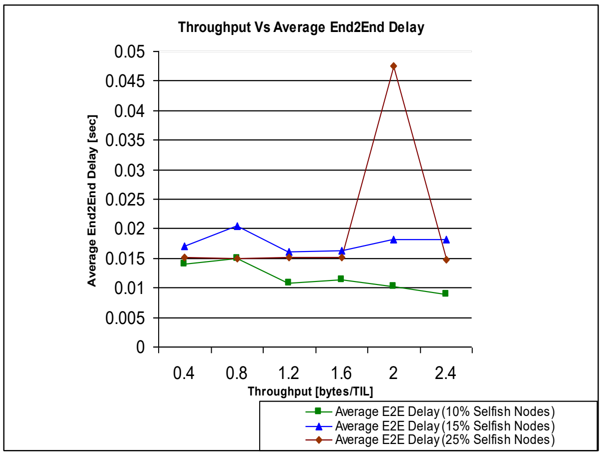

*Figure 8: Throughput of Sending Bits Vs Average End-to-End Delay with 10%, 15% and 25% Selfish nodes for DSR*

As expected, with the increasing number of selfish node the route request which fails to reach the destination from the sender source also increases, unlike malicious nodes, which in order to gather the data information drops the packets after the route request have sailed through them. Thus in DSR + Selfish 10% case where the maximum delay reaches 0.015 sec at 0.82 throughput, at the same throughput for DSR + 15% Selfish the delay is 0.0205 sec and 0.0475 sec for 25% DSR + Selfish behavior at 2.2x 10 $^{4}$ throughput value. This increased delay is not due to the increased RREQ, but also due to the detection and correction measures incorporated for selfish nodes identification, as the delay would also increase while transmitting the data because with the increasing number of selfish nodes, the time required to verify also increases.

The second hand information suggests that although the increased throughput indicates the increased amount of data transmitted but still with this transmitted data minimum delay also increases with percentage of the selfish nodes. Both these selfish nodes effects can be seen even due to the other behavior of selfish nodes which performs the route request of their own in order to use other nodes to send there own traffic throughout the network, causing congestion and thus increased delays.

### *II. Throughput of Receiving Bits Vs End-to-End Delay*

Observing the graphs for the above cases it is observed that like all the previous cases the initial delay increases in DSR + Selfish receiving bits with end to end delay also with for increasing amount of throughput.

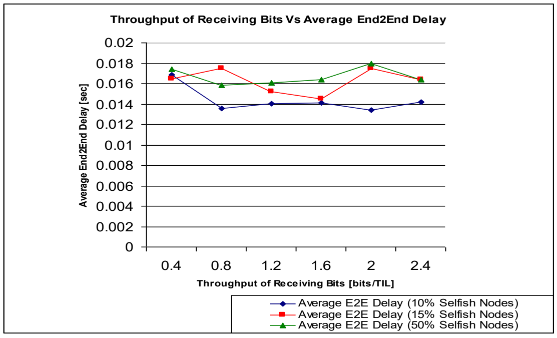

*Figure 9: Throughput of Receiving Bits Vs Average End-to-End Delay with 10%, 15% and 50% Selfish nodes for DSR.*

Throughput of Receiving Bits Vs End-to -End Delay can be analyzed with the help of **Figure 8** as: Although with the increasing number of bits received the throughput also increases irrespective of the number of selfish nodes, but the delay range for the entire duration of the receiving bits increases as for 10% selfish nodes from throughput value of 0.82 x $10^{4}$ to 2.43 x $10^{4}$ it lies between (0.0136 to 0.0142) sec i.e. the width of 0.0006 sec is observed. Whereas in case of 15% the delay is abruptly high as compared to 10% selfish node case and its minimum delay is at 0.016 sec at 1.63 x $10^{4}$ throughput and initially only the delay nearly at 0.0175 sec having a delay width of nearly 0.0029 sec with respect to 0.0006 sec of 10%. As can be thought of with 50% selfish nodes the maximum delay is quite high even higher than the 15% selfish nodes and at no point of time is the delay lesser than the 0.0158 sec. All the results in accordance with the Sending Bits + End to End delay analysis indicates that even while receiving the bits, this increasing delay is due to the fact that the selfish nodes which in a sense have impersonated the normal nodes and thus transmitting their impersonated data as the same path as that would have been for the normal nodes and now at the end all the detection and correction mechanism are coming firstly to get their received bits that are originally meant for them and are not from the selfish nodes and more over the nodes which are at the receiving bits side might even take the word of caution regarding these selfish node occurrences to their neighbors. And both these activities will ask for higher delay for receiving bits at the receiving end, with the increase in the selfish node.

## IV. Conclusion

After carefully analyzing the behavior of Malicious and Selfish Nodes present in the DSR protocol, it is observed that the End-to-End delay increases as the percentage of Malicious Nodes increases. The misbehaving activity of the Malicious Nodes is seen to impact the performance of network. Since the malicious nodes responds positively to all the route requests from the sender, thus it may happen that these malicious nodes might be operating in a cooperative manner resulting in wormhole, black hole or gray hole attacks.

By the very nature of these attacks it happens that the transmitted data packets are either completely dropped due to black hole phenomenon or even if these packets are transmitted, its occurs with increasing time delay as compared to network with all the normal nodes due to wormhole phenomenon.

The selfish nodes effects can be seen even due to the other behavior of selfish nodes which performs the route request of their own in order to use other nodes to send there own traffic throughout the network, causing congestion and thus increased delays.

As expected, with the increasing number of selfish node the route request which fails to reach the destination from the sender source also increases, unlike malicious nodes, which in order to gather the data information drops the packets after the route request have sailed through them.

Even while receiving the bits, this increasing delay is due to the fact that the selfish nodes which in a sense have impersonated the normal nodes and thus transmitting their impersonated data as the same path as that would have been for the normal nodes. The future course of work includes the detection of the malicious and selfish.

## REFERENCES:

[1] S. Buchegger and J. Y. Le Boudec – "Performance Analysis of the CONFIDANT Protocol (Cooperation of nodes: Fairness in dynamic ad-hoc networks)". In proceeding of The Third ACM International Symposium on Mobile Ad Hoc Networking and Computing, ACM Press, 2002.

[2] S. Buchegger and J. Y. Le Boudec. "A Robust Reputation System for P2P and Mobile Ad-Hoc Networks". In proceeding of P2PEcon 2004, Harvard University Cambridge MA, U.S.A, June 2004.

[3] Sorav Bansal, Mary Baker - Observation-based Cooperation Enforcement in Ad hoc Networks - Stanford University – IEEE - arXiv:cs.NI/0307012 Vol 2, 6 Jul 2003. 1 – 10.

[4] Zhiyong Shi, Shenquan Zhu, South China University of Technology and Zhenyu Zhang, Chongqing Communication Institution, China – Study on Application of DSR

Protocol to Mobile Communication System.

[5] Rendong Bai and Mukesh Singhal – DOA: DSR Over AODV Routing for Mobile AdHoc Networks – IEEE Transactions on Mobile Computing, Vol. 6, No. 10, October 2006 – 1403 – 1416.

[6] Asad Amir Pirzada and Chris McDonald - Deploying Trust Gateways to Reinforce Dynamic Source Routing - 2005 3rd IEEE Intemational Conference on Industrial Informatics (INDIN) – 779-784.

[7] Forouzan – "Data Communication".

[8] Jochen Schiller- Mobile Network Layer- Overview of AdHoc Routing Protocols – Mobile Communication, Second Edition, 2005 – 360-361.

[9] Charles E. Perkins and Pravin Bhagwat – DSDV Routing over a multi-hop wireless network of mobile computers – AdHoc Networking Concepts -53 – 69.

[10] Tsu-Wei Chen and Mario Gerlatobe - Global State Routing: A New Routing Scheme for Ad-hoc Wireless Networks – Computer Science Department, University of California, Los Angeles

[11] Guangyu Pei, Mario Gerla-Computer Science Department, University of California, Los Angeles and Tsu-Wei Chen-Bell Laboratories, Lucent Technologies-Fisheye State Routing in Mobile Ad Hoc Networks.

[12] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum, L. Viennot-Optimized Link State Routing Protocol for Ad Hoc Networks – Hipercon Project, INRIA Rocquencourt; BP 105, 78153 Le Chesnay Cedex, France.

[13] Josh Broch David, A Maltz David, B Johnson, Yih Chun Hu, Jorjeta Jetcheva – A proformance comparison of multi-hop wireless AdHoc Network Routing Protocols-Computer Science Department-Carnegie Mellon University–Pittsburgs, Pa 15213.

[14] Charles E. Perkins, Nokia Research Center and Elizabeth M Royer, University of California at Santa Barbara–AdHoc On Demand Distance Vector Protocol–AdHoc Networking Concepts.

[15] David B Johnson, A Maltz David, Josh Broch – DSR: The Dynamic Source Routing for Multi-hop Wireless AdHoc Networks – 139-154.

[16] Jochen Schiller- Dynamic Source Routing – Mobile Communication, Second Edition, 2005 – 356-357.

[17] Asad Amir Pirzada, Amitava Datta & Chris McDonald - Trustworthy Routing with the TORA Protocol - School of Computer Science & Software Engineering, The University of Western Australia.

* * * * *