Opportunistic routing to forgo flooding attacks in MANET

[1]Elakkiya.M, [2]Dr.Edna Elizabeth.N,
[1]PG Student, [2]Professor
[1]Dept of ECE, SSN college of Engineering, Chennai, India [2]Dept of ECE, SSN college of Engineering, Chennai, India
[1]elakkiya90.ece@gmail.com, [2] ednaelizabethn@ece.ssn.edu.in

***Abstract*— Adhoc Networks (MANETs) are an emerging area of mobile computing. There are various challenges that are faced in adhoc environment. These are mostly due to the resource poorness of these networks. They are usually set up in situations of emergency, for temporary operations or simply if there are no resources to set up elaborate networks. Adhoc networks therefore throw up new requirements and problems in all areas of networking. The solutions for conventional networks are usually not sufficient to provide efficient adhoc operations. The wireless nature of communication and lack of any security infrastructure raise several security problems. With little protection against tampering, nodes are susceptible to compromise. Thus the networks are vulnerable to DOS attacks through compromised nodes or intruders. Many denial of service type of attacks are possible in the MANET and one of these type attacks is flooding attack in which malicious node sends the useless packets to consume the valuable network resources. Flooding attack is possible in all most all on demand routing protocol. Thus the paper introduces an opportunistic routing technique to forgo this instant attack. The opportunistic routing takes into account the relative velocity rather than the distance between nodes.**

***Index Terms*—Trust Management; Opportunistic Routing; MANETs; Selfish Nodes; Malicious Node, flooding attack.**

I. INTRODUCTION

Mobile Ad-hoc networks have been gaining popularity because of availability of low cost mobile devices and its ability to provide instant wireless networking. These are temporary networks with no pre-defined infrastructure and each node controls its own activities. There is no central authority to decide what is to be done unlike sensor networks. The other major concern that makes the design of MANET complex is security. Being infrastructure less network and heterogeneous the communication range is not limited to any boundary. To extend the reach ability of the node, other nodes in the network assist as routers. Thus have the probability of being attacked by both internal and external factors. The current design and intended use of MANETs are such that the nodes are susceptible to attacks of hackers. Malicious nodes may become part of active routes and cause network operation disruptions.

The traditional routing algorithms are obsolete in these cases as these algorithms establish a route before forwarding data. But the network is so volatile that the route once established might not last until the data is transmitted completely and this would cause loss of data. Instead if a path is established as the data packet moves along a network then the data packet would be able to traverse across the network by avoiding those nodes which might not be able to forward it. This is called opportunistic routing where a node do not simply forward data to any node but forwards only if the other node is the most competent among the available nodes [1]. This proves higher probability of packet delivery. Many such routing algorithms are proposed in [2-4]. They all propose a common metric to select the next forwarder which is the ability to deliver the data to the destination. This probability is influenced by both its trust value and its velocity vector in the proposed model.

This paper presents one of the most predominant DOS attacks namely flooding attack. The attack results in denial of service when used against all previously defined on-demand ad hoc networks routing protocols. In this attack, the attacker either broadcasts a lot of Route Request packets for node ID who is not in networks, or sends a lot of DATA packets to consume the bandwidth so as to congest in links. These attacks are rarely identified as malicious nodes behaves normally in all aspects except that they initiate frequent control packet floods. To defend routing protocols against the flooding attack, a trust model based opportunistic routing [1] is proposed. The constraint is placed over TTL field based on the trust model. The results are simulated in NS2 and are analyzed to check the performance.

The scenario of the paper is a network with highly mobile nodes and data is transmitted in store and forward method. We adopt a multicast method instead of broadcasting to reduce the overhead due to the presence of redundant data in the network. Though broadcasting improves data delivery probability it might not be suitable for networks with low bandwidth availability. Figure (1) explains the scenario better and the arrow in the circle indicates the direction of motion of node. The malicious nodes are differentiated from benign nodes by color. Further each node is assumed to contain a reliable GPS system to detect the current location, the direction of motion of the node and also its velocity.

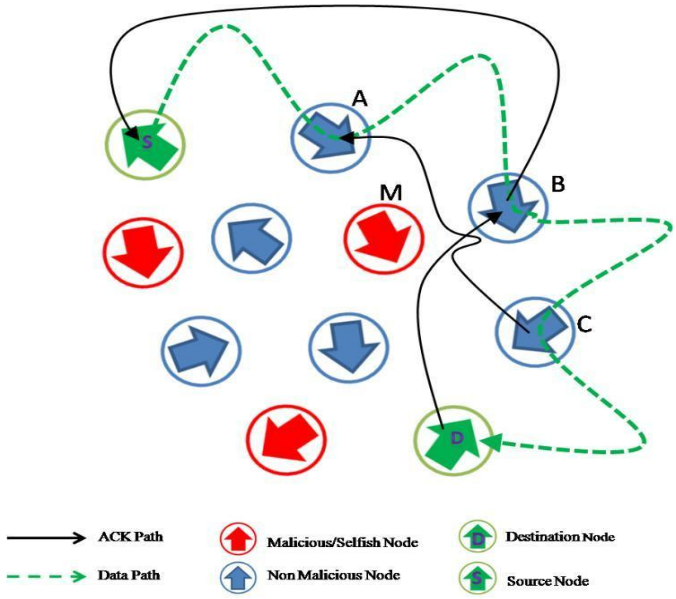


FIGURE 1 NETWORK SCENARIO

II. RELATED WORK

In the previous work [1] a trust model was proposed based on relative velocity. The model was incorporated into AODV for routing process and it followed an opportunistic routing. The results proved the model optimum for packet delivery ratio against black hole, gray hole and DOS attacks. Now the model is extended to overcome flooding attack so as to reduce the overhead. When this is done the model is complete mitigating multiple attacks.

The first flooding attack prevention (FAP) method was proposed in [2]. In their paper, first they described RREQ flooding and data flooding. This was the first paper that addressed the prevention of flooding attack in ad hoc network. The authors proposed the separate approach for RREQ flooding and data flooding. To resist the RREQ flooding, they defined the neighbour suppression method which prioritizes the node based on the number of RREQ received. A node gets higher priority if it sends less numbers of RREQ packets and defined the threshold value. To deal with data flooding they used path cut off method. In this method when node identifies that sender is originating data flooding then it cutoff the path and sends the route error message. In this way attack is prevented up to some extent but the disadvantage of this method is flooding packet still exists in the network. This limitation of FAP is eliminated by [3] presented threshold prevention. In this method they defined the fixed threshold value for every node in the network. If any node receives the RREQ flooding packet more than the threshold value then the sender is assumed as a attacker and all the packets from attacker is discarded by the receiver node. This method eliminates the flooding packet but if the intruder has the idea about the threshold value then it can bypass the TP mechanism. Normal node with high mobility is treated as the malicious node.

The author proposed the distributive approach to resist the flooding attack [4]. In this method they have used the two threshold value; RATE_LIMIT and BLACKLIST_LIMIT. If RREQ count of any node is less then RATE_LIMIT then the request is processed otherwise check whether it is less then BLACKLIST_LIMIT, if yes then black list the node but if the count is greater than RREQ_LIMIT and less than the BLACKLIST_LIMIT then put the RREQ in the delay queue and process after queue time out occurs. This method cannot handle the network with high mobility.

In [5], the author analyzed the flooding attack in anonymous communication. They used the threshold tuple which consist of three components: transmission threshold, blacklist threshold and white listing threshold. If any node generates RREQ packet more than transmission threshold then its neighbour discards the packet if it crosses the transmission threshold more than blacklist threshold then it black list the node. But to deal with accidental blacklisting they defined white listing threshold. If any node performs good for number of intervals equal to white listing threshold then it again start treating as a normal node.

The trust based security scheme developed for RREQ flooding attack [6], describes the route request flooding and data flooding attack. The paper follows the DSR routing protocol. The protocol maintains route cache to store route to mobile nodes. The process consists of two phases. Route discovery phase is to find the route to destination when node don't have unexpired route. The second phase is route maintenance to detect whether the path to the destination exist. Further route error message and ACK route error message is to recognize any transmission error in data link layer. The protocol proved efficient as packet overhead scale down to zero when nodes are stationery. But the major limitation is that the packet overhead will increase significantly for networks with larger hop diameters as more routing information will need to be maintained in packet headers. Thus they are suited only for small to medium sized networks and not for larger networks.

III. Trust Management System

The objective of the trust model is to numerically quantize the trustworthiness of a node to deliver data. This is achieved in the proposed trust model [1] in two parts: direct and indirect trust observation values. Indirect observation values are necessary as all nodes may not encounter every other node in the network.

Every node in the network contains a table of TVM of every other node in the network. Initially all nodes in the network are assigned a Base trust Rating (BR). This rating would then increase or decrease depending on the behavior of the node as time progresses. Hence whenever node A forwards data to node B the TVM of node B stored in the routing table of node A is varied which is called direct observation and the TVMs of other nodes stored in A is varied according to the TVMs stored in the node B which is called indirect observation.

Now when a node starts behaving maliciously or selfishly the TVM of the respective node would reduce with each interaction the node has with other nodes. But if it is not interacting with any other node for some time it would still retain its TVM. Also a selfish node avoiding other nodes for forwarding purposes would also retain its TVM. To avoid this we use the

Aging factor (α (t)). The TVM is periodically reduced by the aging factor which means that the trust of any node decays with time. Hence to maintain the trust level in the network the nodes are now forced to continuously work collaboratively to forward data.

Consider that a node X meets node Y. The following formula represents the change in TVM value of Y present in X. The formulae used for updating the trust value and the explanations of the same are obtained from the previous work of trust model [1].

A. Direct observation:

$$TVM_{Xy}^{(new)} = TVM_{xy}^{(old)} + \frac{BR}{\beta * PDR} * (T_{TH} - T_D) \qquad (1)$$

T_{TH} is the threshold time below which the ACK from the node is expected to be received. If not then the value of T_D is set to a value greater than T_{TH} making the second part of the expression negative and hence reducing the value of TVM. The factor ~~provid~~es the multiplication factor which decides the factor by which the delivery time would impact the TVM. β is

the time scaling factor which influences delivery time impact on TVM and its introduced so that we could change it depending on the network configuration.

B. Indirect observation:

$$TVM_{xk}^{(new)} = \frac{TVM_{xk}^{(old)} + TVM_{yk} * \frac{TVM_{xy}}{BR}}{1 + \frac{TVM_{xy}}{BR}} \qquad (2)$$

$$TFM = \frac{TVM_{xy}}{BR} \qquad (3)$$

If the TFM is greater than 1 it means TVM of the node Y is greater than its Base Trust Rating (BR). And the TVM is greater than BR only when it is trustworthy and has successfully forwarded many data. So TFM is greater than 1 if the node is trustworthy. If the TFM is less than 1 when substituted in the equation the final result would be closer to the value present in X and hence reducing the effect of the value provided by the malicious node.

C. Aging of TVM:

$$TVM_{xk}^{(new)} = TVM_{xk}^{(old)} * (1 - \alpha(t)) \qquad (4)$$

It is evident that as α(t) increases with time TVM value of the set of all nodes in X decreases. The aging factor range is 0<α(t)<1.

Table1 Notations

Symbol	Explanation
TVM_{AB}	Trust Value Metric of node B stored in node A
BR	Base Trust Rating
T_D	Packet delivery time
T_{TH}	Threshold Time
PDR	Packet Delivery Ratio
α(t)	Aging factor
TFM	Trust Factor Multiplier

IV. Flooding Attack Mitigation

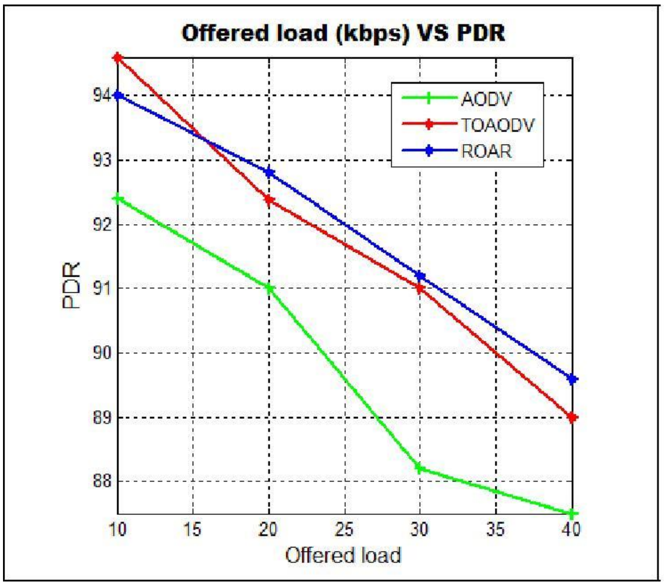
The proposed trust model [1] integrated into AODV was named as Trusted Opportunistic AODV (TOAODV) routing protocol. The protocol mitigates black hole attack, gray hole attack, DOS attack effectively. But the major limitation was the overhead and delay for the packet to transmit from one node to another. Thus the work is extended to have some constrained on overhead and forgo flooding attack. Thus the new protocol is named as Reputation based Opportunistic Adhoc Routing (ROAR). As the nodes are selected based on the trust value and the relative velocity, a node with too low TVM are isolated. Thus the black hole, gray hole attacks are mitigated. Further as the aging factor is introduced, every node has to cooperate with each other to be rated normal and thus DOS attack is mitigated.

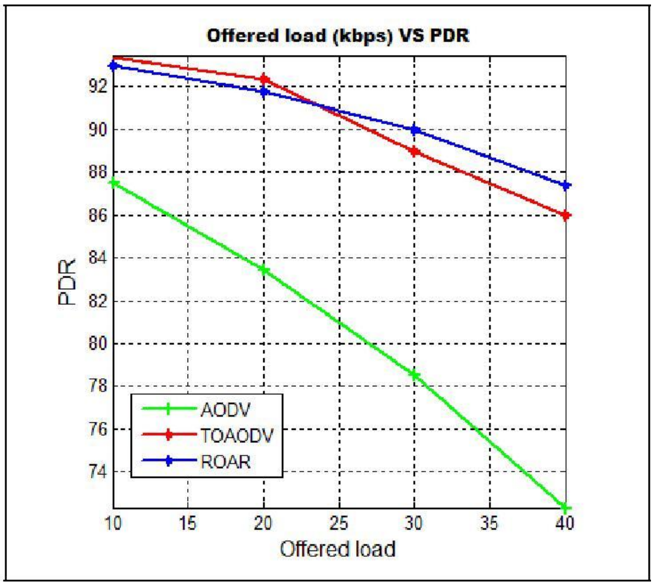
Now, the most prominent type of DOS attack namely flooding attack is to be focused. Flooding the whole network with bogus RREQ and data consumes all the resources of the network. To reduce congestion in the network, AODV adopts some methods. A node cannot generate RREQ more than a rate limit. After broadcasting a RREQ, a node waits for a RREP.If a route is not received within round-trip milliseconds, the node may try again to discover a route by broadcasting another RREQ, up to a maximum of retry times at the maximum TTL value. Repeated attempts by a source node at route discovery for a single destination must utilize a binary exponential back off. Hence, the waiting time for the RREP corresponding to the second RREQ is 2 * round-trip time. The RREQ packets are broadcast in an incrementing ring to reduce the overhead caused by flooding the whole network. The packets are flooded in a small area (a ring) first defined by a starting TTL (time-to-live) in the IP headers. After RING TRAVERSAL TIME, if no RREP has been received, the flooded area is enlarged by increasing the TTL by a fixed value. The procedure is repeated until an RREP is received by the originator of the RREQ, i.e., the route has been found. Thus some constraint on TTL would reduce flooding of packets.

The proposed model [1] as explained earlier adopts multicast method instead of broadcast method. Two are three nodes are selected based on the trust factor that includes the relative velocity. The RREQ packets are sent only to those nodes that have higher probability of delivering packet to the node destined to. And these nodes in return send RREP packet with the number of hops it actually requires to reach the destination. Considering the number of hops and the time taken to reply, the most competent node is selected. Thus the overhead is reduces in each node. Further to avoid bogus requests, nodes are set with threshold based on the relative velocity. Thus the requests are minimized and a node also accepts requests from highly mobile nodes even if the threshold is exceeded. In this way flooding attack can be resisted, while also allowing large networks have continuous communication.

V. Performance Analysis

The simulation results were first obtained for a network with malicious nodes and then our proposed work was incorporated into the same network. For the performance analysis, the plots between the offered load (kbps) and other parameters such as PDR (Packet Delivery Ratio), Delay (m/s), Overhead (packets) are taken into account. Here the plots are analyzed for 1 RREQ / sec and 10 RREQ / sec.





A. PDR OF ROAR

The PDR of ROAR can be proved better than other trust models and also the traditional MANET protocol. Figure 2 and figure 3 explains the plot between PDR and offered load (kbps) with various numbers of RREQ /sec. The proposed trust framework ROAR has proved efficient than TOAODV [1] and traditional AODV. This is because, in the proposed framework, as the nodes transmit packets, detects the malicious nodes perfectly and isolates them. Thus the PDR is high and optimal in the proposed ROAR.

B. DELAY OF ROAR

The average delay is the time taken for each node to transfer the packet to the next competent node based on the TVM. In figure 4 and figure 5 delay parameter is plotted against the offered load. Initially the proposed trust frame seems to be inefficient. As the routing process is continued for certain timing and once the data are available for most of the nodes in the network, the malicious nodes are isolated and so ROAR proved better than AODV. The graph is evident that delay of ROAR proves better than AODV even at high mobility of nodes. This is mainly because the path is created dynamically based on relative velocity as the data packet traverses.

C. OVERHEAD OF ROAR

The overhead is the main parameter to analyze the flooding attack. The trust model proposed proves efficient when the TTL of nodes selected are based on the trust factor and relative velocity. The overhead when plotted against offered load with varying RREQ / sec proves that ROAR is much better than the traditional protocol and TOAODV. This is evident from the figure 6 and figure 7.

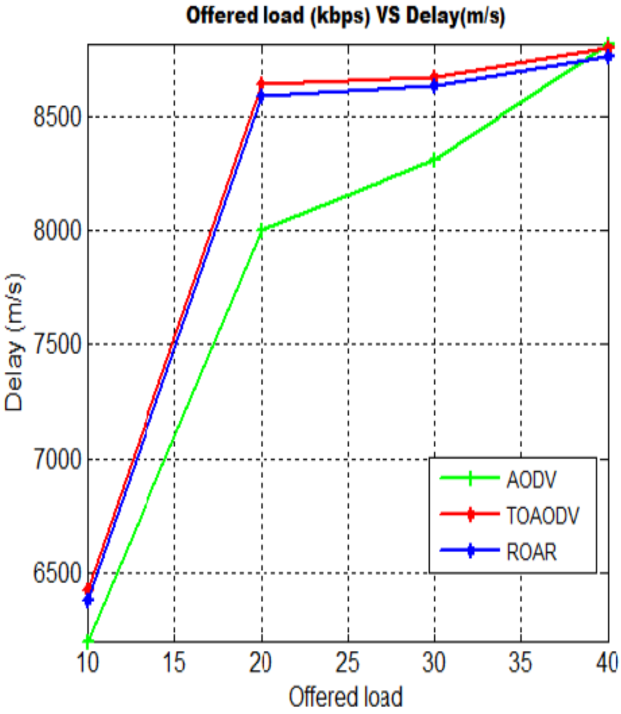


Figure 5 Offered load Vs Delay in m/s (1 RREQ / sec)

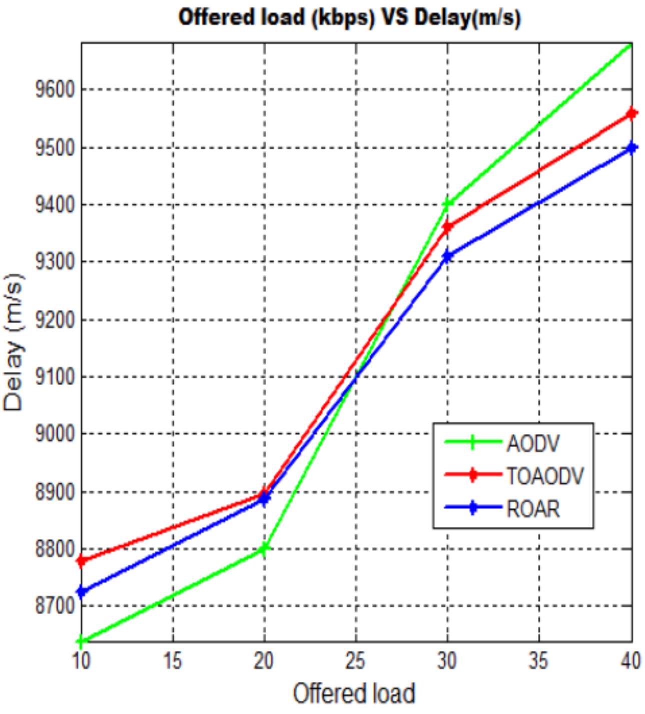


Figure 6 Offered load Vs Delay in m/s (10 RREQ / sec)

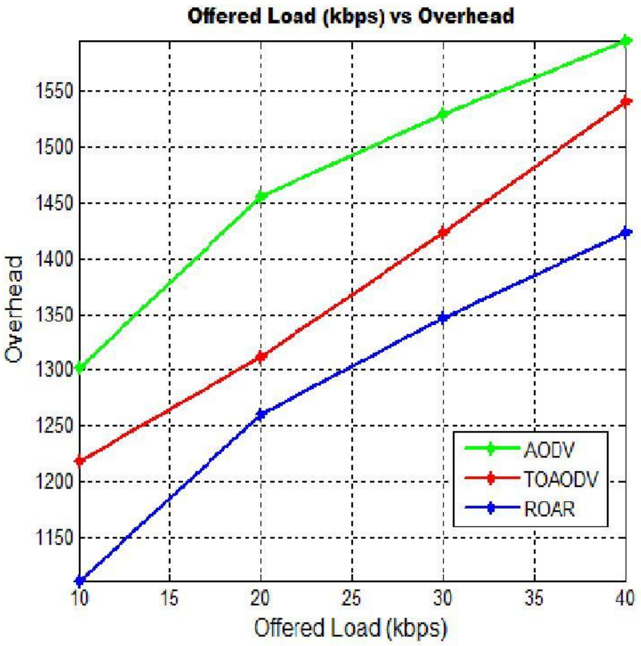


Figure 7 Offered load Vs Overhead (1 RREQ / sec)

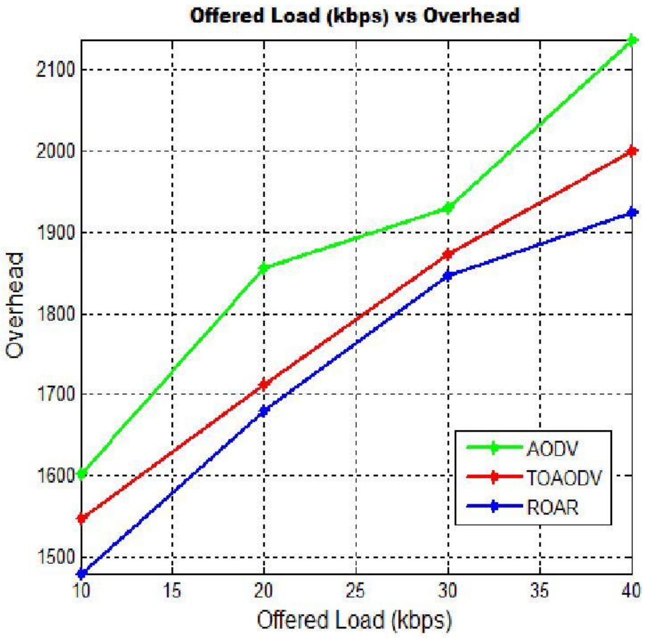


Figure 8 Offered load Vs Overhead (10 RREQ / sec)

VI. CONCLUSION

The paper have focused mainly on developing a trust model for opportunistic routing which is able to route data even in a highly unstable scenario consisting of frequent link breakage and presence of malicious and selfish node. Further the work is to be extended to overcome the most prominent type of Dos attack namely flooding attack. The idea is to have constrained control on TTL field to reduce the overhead and intentional flooding by malicious nodes. The other major attack namely Sybil attack is also to be dealt in near future by including some key management and biometric technique. When the secure opportunistic routing and a key management technique integrated would overcome the inter dependency cycle problem of the existing works. Thus the proposed trust model incorporated in traditional AODV combined with a key management and biometric identity scheme could efficiently mitigate multiple attacks in MANET. As on now the efficiency can be proved with the simulation results.

REFERENCES

[1] Kaushik.S, Elakkiya.M, Deepa.R, Edna Elizabeth.N, "Trust based opportunistic routing in MANETS",7th International conference on Advanced Computing & Communication Technologies (ICACCT-2013), ISBN:978-93-83083-38-1, pp-218-223.

[2] Ping Yi, Zhoulin Dai, Yiping Zhong, Shiyong Zhang "Resisting flooding attacks in Adhoc networks" Proceedings of the International
Conference on Information Technology: Coding and Computing (ITCC'05), IEEE, 2005.

[3] Bo-Cang Peng and Chiu-Kuo Liang"Prevention techniques for flooding attack in Ad Hoc Networks"

[4] Jian-Hua Song, Fan Hong, Yu Zhang, "Effective Filtering Scheme against RREQ Flooding Attack in Mobile Ad Hoc Networks "
Proceedings of the Seventh International Conference on Parallel and Distributed Computing,Applications and Technologies (PDCAT'06), 2006.

[5] Venkat Balakrishnan, Vijay Varadharajan, Uday Tupakula, 'Mitigating flooding attacks in mobile adhoc networks supporting anonymous communications" The 2nd International Conference on Wireless Broadband and Ultra Wideband Communications (AusWireless '07), 2007.

[6] J. Burgess, B. Gallagher, D. Jensen, B.N. Levine, Maxprop, "Routing for vehicle-based disruption-tolerant networking," Proceedings of INFOCOM'06, 2006, pp. 1–11.

[7] Lindgren, A. Doria, O. Schelen, "Probabilistic routing in intermittently connected networks," SIGMOBILE Mobile Computing Communications Review 7 (3), 2003, pp. 19–20.

[8] Boldrini, M. Conti, A. Passarella, "Exploiting users' social relations to forward data in opportunistic networks: the HiBOp solution,"
Elsevier Pervasive and Mobile Computing 4 (5), 2008, pp. 633–657.

[9] Wang Boa, Huang Chuanhea, Li Layuanb, Yang Wenzhonga, "Trust-based minimum cost opportunistic routing for Ad hoc networks," Elsiever Journal of Systems and Software HYPERLINK "http://www.sciencedirect.com/science/journal/01641212/84/12" Volume 84, Issue 12, December 2011, pp. 2107–2122.

[10] Na Li, Sajal K. Das,"A trust-based framework for data forwarding in opportunistic networks," Elsiever Ad Hoc Networks,Volume 11,
Issue 4, June 2013, pp. 1497–1509.

[11] Jason LeBrun, Chen-Nee Chuah, Dipak Ghosal, Michael Zhang, "Knowledge-Based Opportunistic Forwarding in Vehicular Wireless Ad Hoc Networks," Vehicular Technology Conference, IEEE, Vol.4, 2005, pp. 2289 – 2293.