IJCTA, 9(27), 2016, pp. 275-282
ISSN: 0974-5572

FFFS-Functional Framework for Flooding Scheme in MANETs to reduce Uncertainty

R. Sheik Abdullah* and S. Hari Ganesh**

ABSTRACT

A mobility-assisted scheme known as effective flooding mechanism is provided to accomplish a great chance of trust convergence. Trust is known as the opinion in the ability of a node to carryon securely, reliably and dependably within a specific context. It designates a MANET participant's hope of other nodes' behavior while approaching the risk engaged in future interactions. Here, the participant, known as the trustor, and other nodes are known to be trustee. The trust relationship commonly builds on the part of others' recommendations associated with the trustee and the trustor's past direct interaction experiences. The abstracted value of preceding experiences and from recommendations is known as the trustee's reputation. The proposed functional framework for flooding scheme which is based on node's mobility. The effective flooding scheme is based on one-hop neighbor that guides to minimization of number of forwarding nodes. This scheme provides a handy tradeoff among delay, cost, packet delivery and trust ratio which provides an uncertainty reduction.

Keywords: Flood, FFF, MANETs, forwarding, Trust Convergence, Uncertainty reduction.

1. INTRODUCTION

Mobile Ad Hoc Networks capable of communicating in a wireless medium without having to choose an existing network infrastructure. An essential property of ad hoc networks is that they are able to configure themselves on-the-fly without the presence of a centralized administrator. As MANET is a self configuring and independent communication system that employs node to node hops for transmission of data from one node to another. In a MANET, traffic which is not mitigated by a node is forwarded by that node to other nodes within the range and a node which involves in forwarding will therefore represent as simple router.

Uncertainty is the degree to which a node that cannot accurately foretell the behavior of its communal rival [1]. Uncertainty emerges from opportunism and information asymmetry. For the effective uncertainty reduction is to accomplish the key aspect of mobility of MANETs. The node's movement can increase the aim of recommendation transmission and direction and so pace up trust convergence. The proposed scheme called effective flooding mechanism helps in exploiting mobility.

Flooding is the most primary function in mobile ad hoc networks (MANET). The key routing protocols such as Dynamic Source Routing, ZRP and AODV rely on flooding for route discovery transmission, topology update and route upholding. Flooding is a very repeatedly invoked efficient function in MANETs. Hence, an effective play of flooding mechanism is necessary in order to minimize the overhead of routing protocols and to magnify the throughput of networks. Flooding mechanism needs that every node should keep only 1-hop neighbor information. An effective implementation flooding mechanism leads to overhead reduction of routing protocols and enhancing the throughput of the network. The effective flooding mechanism varies from the broadcast mechanisms.

* M.C.A.,M.Phil., (Ph.D)., Assistant Professor, CS Alagappa University College of Arts and Science Paramakudi, India, *Email: sheik.es1914@gmail.com*

** M.Sc.,M.Phil., Ph.D., Assistant Professor, CS The Rajahs College Pudukottai, India, *Email: hariganesh17@gmail.com*

1.1. MANETs and Floods

MANET can be damaged by different kinds of attacks, as it has different mobile nodes that are decentralized and requires cooperation to transfer traffic. Any node can be malicious and can participate to produce flood attacks. MANETs are framework less networks, and has group of de-centralized nodes, which can be randomly moved. This basic characteristic of MANETs makes it susceptible to various attacks such as flooding, black hole, warm hole, etc. Request flooding- Here malicious nodes send Route Request (RREQ) packet to the destination that does not prevail, and for MANET to build a route source sent a RREQ message and any intermediate node will flood it more till it reaches the destination. But in flood attack if RREQ destination does not exist, so node will continuously flood such packets and occupy the bandwidth. Data Flood Attack: In this it floods fake data to the destination once the path is preserved. Hello flood- In routing protocols they are used to preserve neighbor entry. When they are flooded with greater frequency rate, the nearby nodes are not able to proceed other packets. Other kinds of attacks [3] that exist in MANET such as black holes, sinkhole, wormhole, selfish nodes, etc. Any node with this type of behavior can create drastic harm to networks

2. LITERATURE SURVEY

2.1. Trust Evaluation System

Uncertainty is estimated in terms of high authentication probability and trust convergence. Various mobility mechanisms like metropolis, hierarchical are resolved. Existing reputation systems provide space for liberate attackers for propelling false accusation attacks considering there is no stipulation on update frequency. This way has also cannot desperate newcomers from misbehavers. Josang [7] proposed an algebra for identifying trust relations, where a triplet allocating uncertainty, belief and disbelief are fixed to each trust declaration. However, the primary weakness is that the reputation of every entity is based on own slanted policy and the system cannot certify that users will have persistent values. It's also difficult to integrate various recommendations. Carbone et al. mentioned a formal trust structure in [14].

2.2. Reputation System

(RTMS) Reputation and Trust-based Monitoring Systems have given an ideal architecture for Wireless Sensor Network (WSN) security. In the existing RTMSs, specifically each node has a *watchdog* which functions in a promiscuous mode for obtaining information about neighboring node's behavior. Sensors are very much resource (energy) -constrained and its independent operation in unreceptive territories provides them revealed to physical node capture attacks. So the sensors that are resource-constrained must be used only for challenging services, hence the lifetime of the network can be extended.

2.3. Flooding Mechanism

Flooding is one of the most essential and important functions in mobile ad hoc networks. Classic methods of flooding suffer from the troubles of massive message redundancy, signal collision and resource contention. This causes a high protocol overhead and interference of traffic in the networks. Various flooding mechanisms were designed to avoid these complications. Anyway, those mechanisms perform poorly in transmission redundancy reduction and maintain 2-hop neighbor information of every node. Hence, an effective application of flooding mechanism is in demand for the routing protocol overhead reduction and increasing the throughput of networks. The existing flooding mechanisms are differentiated based on the information that each node keeps: i) nil neighbor information ii) one-hop neighbor information iii) two-hop/more neighbor information. Methods that are under first one does not require information on neighbors. A pure flooding mechanism is a typical example in this section.

3. PROPOSED WORK

3.1. FFF-Functional Framework for flooding scheme

The functional framework of the proposed scheme is shown in figure 1. A completely distributed reputation system that can cope up with false transmitted information where the haphazard mobility models are to be used that can

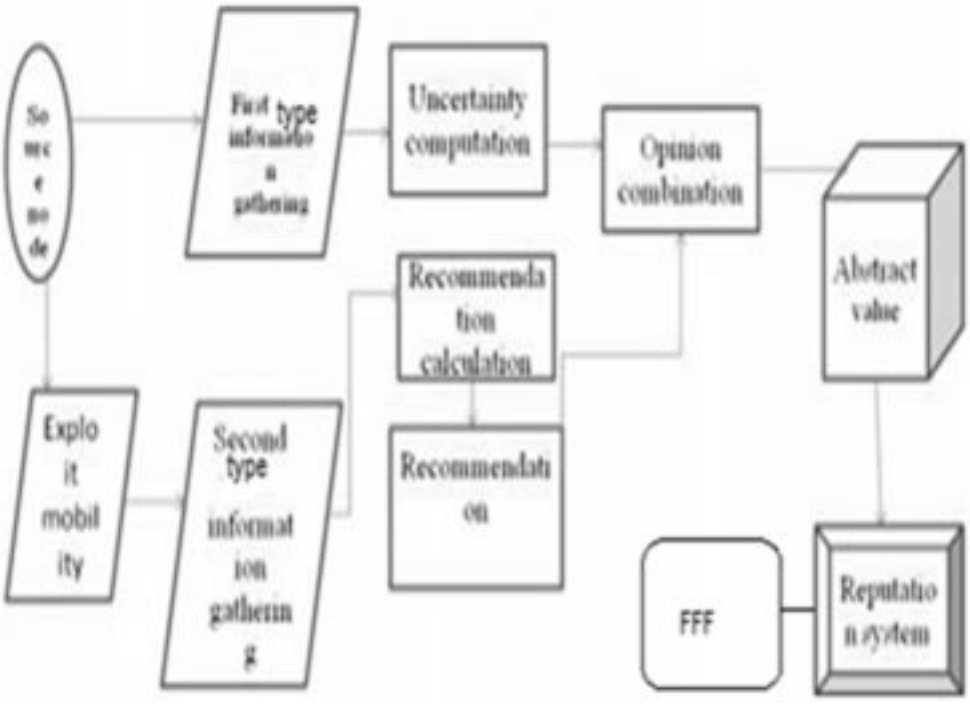

Figure1: Functional Architecture of proposed system

identify the ideal path in terms of route stability and route availability. The effective flooding mechanism is going to be used which heads speedup *high authentication* probability and *trust convergence* respectively for uncertainty reduction.

3.2. Functionalities

The trust, reputation has to be collected from first level information and second level information. The second level information heads recommendation calculation from different nodes. All these recommendations should be combined. While combining, the dales praise and false accusation should be removed. An opinion incorporation has to be produced from synthesized recommendation and uncertainty computation. This heads abstract value of the opinion system.

3.3. Effective Flooding Mechanism

Flooding is one of the most essential and important functions in mobile ad hoc networks. Classic methods of flooding suffer from the troubles of massive message redundancy, signal collision and resource contention. This causes a high protocol overhead and interference of traffic in the networks. Various flooding mechanisms were designed to avoid these complications. Anyway, those mechanisms perform poorly in transmission redundancy reduction and maintain 2-hop neighbor information of every node. The important and basic condition of deliverability of 100% for flooding mechanisms is based on only one-hop neighbor's information. The working of an effective flooding mechanism shown in Figure 2 that can accomplish the optimality in two wits: i) the number of forwarding nodes in every step must be reduced, ii) the time complexity computation for forwarding nodes must be less, which is $O(nlogn)$, n represents the number of neighbors of a node.

The main aim of the effective flooding mechanism is to reduction of number of forwarding nodes as much as achievable, hence minimizing the redundant packet transmission. The metric *ratio of forwarding nodes* to calculate the effect of flooding mechanisms is used. The ratio of forwarding nodes is known as the ratio of total number of nodes in the packet forwarding in a flooding function to the total number of nodes present in the network. Minimization of forwarding nodes is given in figure 3.

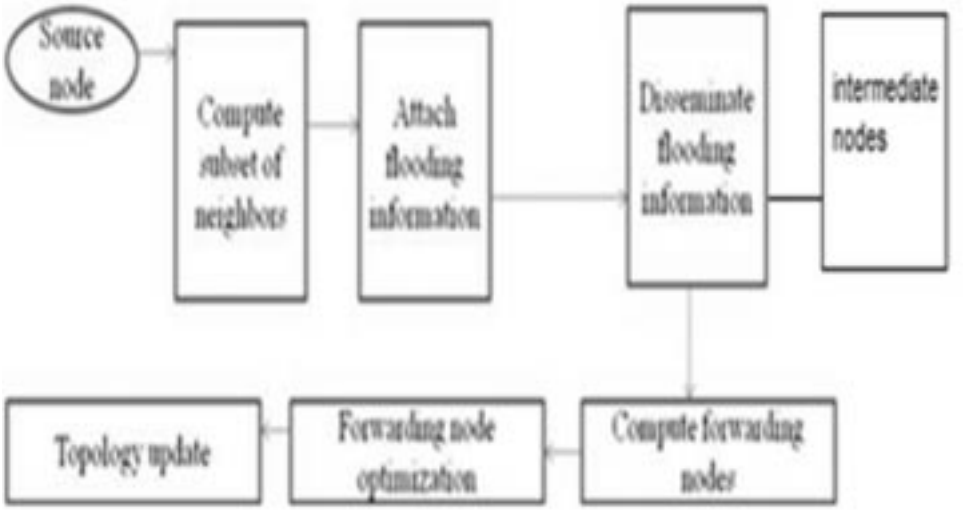

Figure 2: Working of Effective flooding Mechanism

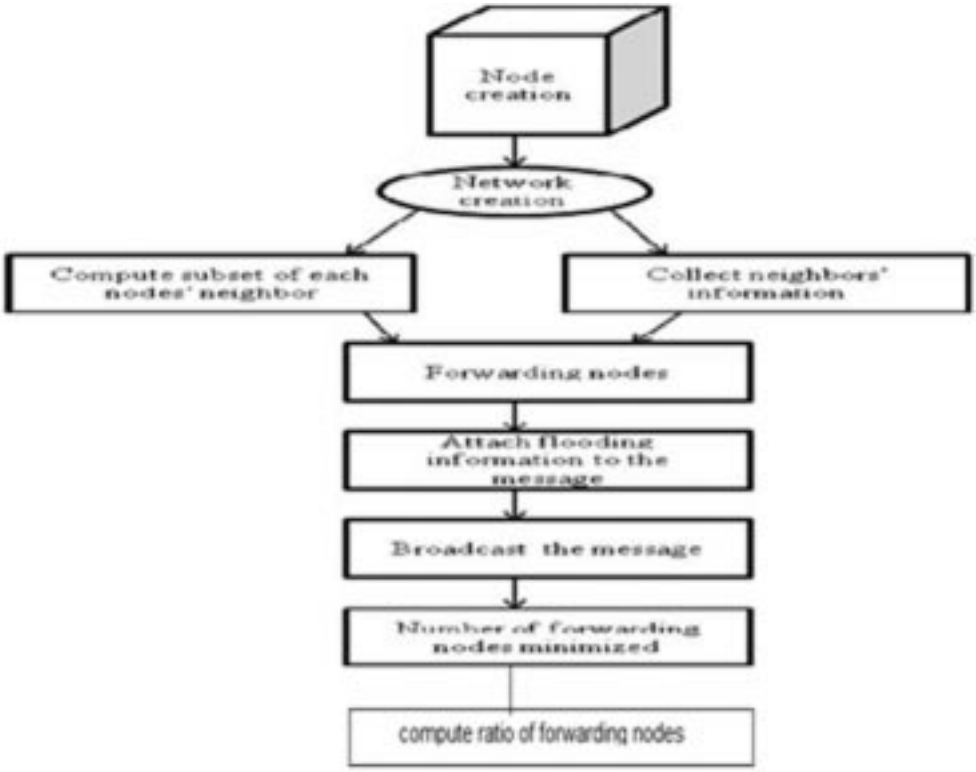

Figure 3: Minimization of forwarding nodes

3.4. Functional architecture of effective Flooding Mechanism

The source node will calculate the subset of neighbors. The flooding information will be hooked up to each of the neighbors and the neighbors will transmit the flooding information to other intermediate nodes. The calculation of forwarding nodes will be done. Node optimization will be done from the forwarding nodes. Based on the node's mobility the topology will be updated. Functional architecture is shown in figure 4.

3.5. Handling of Mobility

In MANETs, nodes are able to be mobile, which leads to aggressive changes of topology of the network. In the flooding mechanism, each node, say n, preserves its neighbor information and calculates F(n). To handle with the aggressive topology change, two scenarios are necessary in the flooding mechanism i) No update. Every node re-

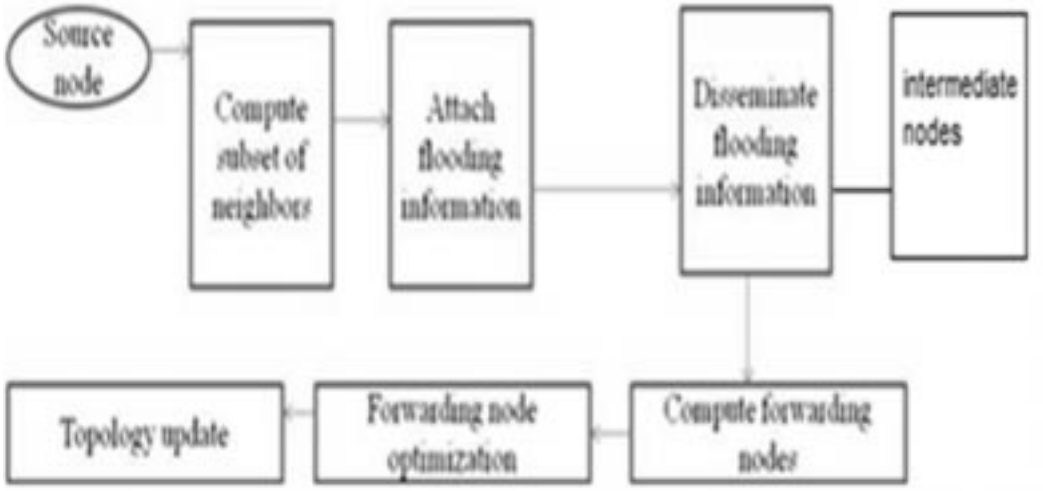

Figure 4: Functional Architecture

calculates its forwarding node set for the flooding request of that node or ii) update which must be incremented each and every time. Each node will incrementally update its forwarding node set upon change of topology. For scenario i), does not require anything.

4. EXPERIMENTAL RESULTS AND PERFORMANCE ANALYSIS

4.1. Effective Flooding Mechanism

The average delay, trust packets received, number of trust packets sent, and total number of uncertain packets for flooding mechanism is shown in Figure 5. The reduction of number of uncertain packets and the increment of packet delivery ratio is shown.

4.2. Analysis of Performance

The uncertainty reduction analysis has been done for two different mechanisms. The reduction of uncertainty is given in terms of delay, number of packets lost, number of packets sent and trust ratio. The data are taken from trace files for different simulation times.

4.2.1. Time Vs Delay

Delay is defined as the time taken to combine trust reputations since uncertain nodes are present in the reputation system. The x-axis is meant for time in ms and y-axis is taken for delay. By implementing the effective flooding mechanism the delay is reduced compared to hierarchical mechanism. Time vs delay is shown in figure 6.

Figure 5: Output terminal for Flooding Mechanism

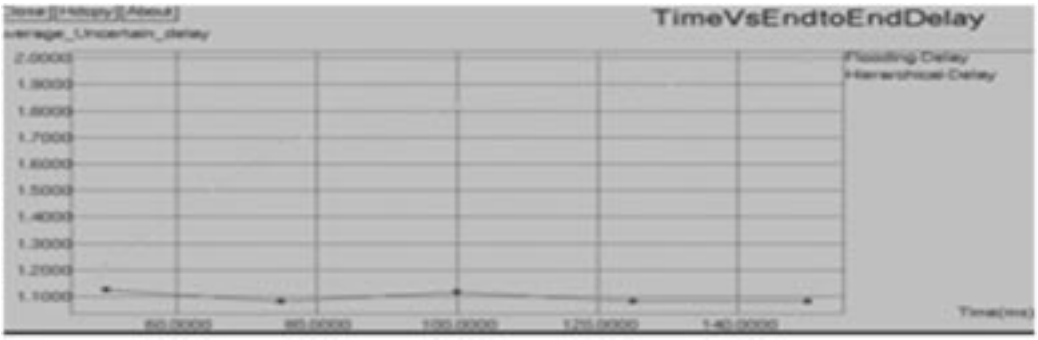

Figure 6: Time Vs Delay

Time Vs Packet loss

The Packet delivery ratio is defined as No. of packets received / total no. of packets sent. The x-axis is taken in time and the y-axis is meant for packets. The packet loss is reduced when compared to the existing mechanisms. Time vs packet loss is shown in figure 7.

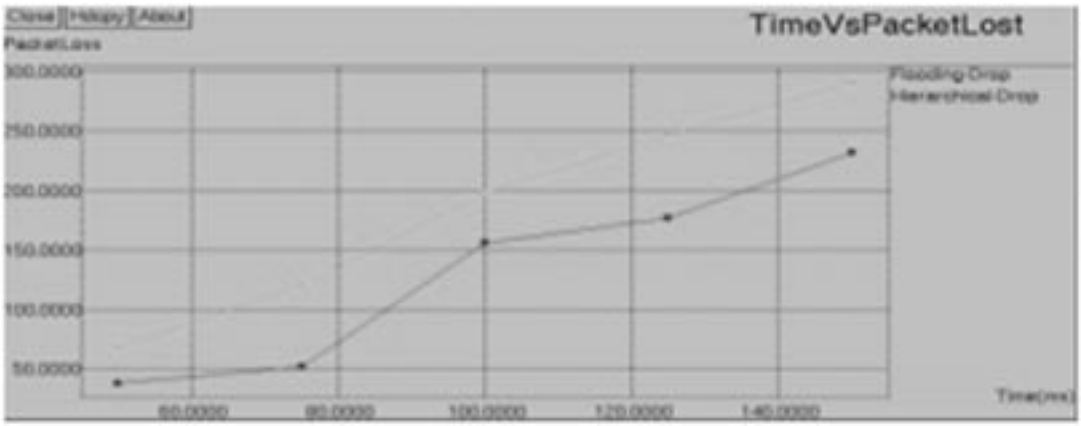

Figure 7: Time Vs Packet loss

Time Vs Trust Ratio

Trust is defined as the firm opinion on the competence of an entity to act independently, securely and reliably within a specified context shown in Figure 8. The x-axis is taken in time and the y-axis is meant for trust ratio.

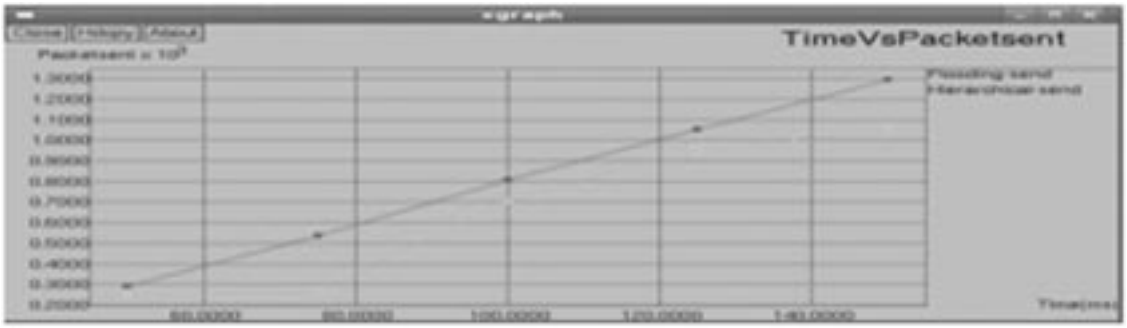

Figure 8: Time Vs Trust ratio

Time Vs Packet sent

The packet consists of trust reputations about different nodes. The x -axis is taken for time and the y-axis is meant for packets. The number of packets sent is huge compared to existing mechanisms. Time vs packet sent is shown in figure 9.

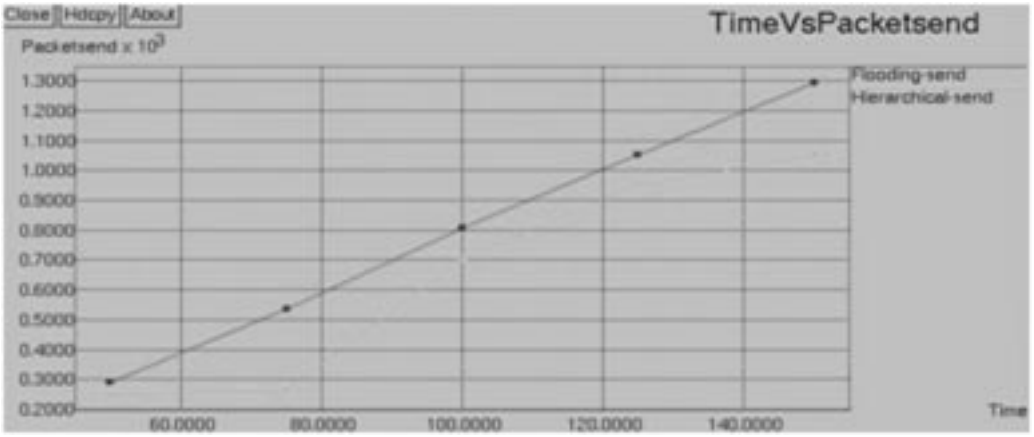

Figure 9: Time Vs Packet sent

Table I. summarizes the comparative analysis of the FFF scheme with the existing mechanisms.

Table 1
Comparative Analysis

	Metropolis	*RTMS*	*FFF*
Redundancy	High	High	Less
Resource contention	High	High	Low
Signal collision	More	More	Less
Protocol overhead	High	High	Less
Traffic interference	High	High	Less
Neighbors	2-hop	2-hop	1-hop
Throughput	Less	Less	High
Forwarding nodes	More	More	Less
Time complexity	High	High	Low
Packet drops	High	High	Low
Reliability	Less	Less	High
Lifetime	Less	Less	High
Deliverability	Low	Low	High
Uncertainty	High	High	Low

5. CONCLUSION

The Effective flooding mechanism uses only one-hop neighbor information and it is confirmed that effective flooding mechanism gains the optimality in terms i) minimization of number of forwarding nodes and ii) the time complexity $O(nlogn)$ must be less. The energy effective mechanism decreases packet drops and improves reliability. The life time of the each node and the network is increased by choosing more reliable node as a router. Simulations are done to compare my mechanism with hierarchical mechanism. Simulation results show that the proposed mechanism uses incurs forwarding node reduction, less collisions, and retrieves increased deliverability ratio compared with the existing mechanisms. Through the application of uncertainty reduction, forwarding node minimization, which leads to the enhancement of network lifetime.

REFERENCES

[1] Feng li, Jie Wu., "Uncertainty Modeling and Reduction MANETs" *IEEE Trans on Mobile Computing*, vol. 9, no. 7, July 2010.

[2] Feng Li, Jie Wu.,"Mobility Reduces Uncertainty in MANETs" *IEEE INFOCOM 26th IEEE International Conference on Computer Communications*, ISSN 0743-166X, 2007

[3] Hai Liu, Xiaohua Jia, Peng-Jun Wan, Xinxin Liu, Frances F. Yao., "A Distributed and Efficient Flooding Scheme Using 1-Hop Information in Mobile Ad Hoc Networks". *IEEE Trans on Parallel And Distributed Systems*, Vol 18, no. 5, May 2007.

[4] Nivedita N. Joshi, Radhika D. Joshi., "Variable Range Energy Efficient Location Aided Routing for MANET". D.C. Wyld, et al. (Eds): CCSEA, CS & IT 02, pp. 321–333, CS & IT-CSCP, 2011.

[5] Farukh Mahmudur Rahman, Mark A Gregory. "Quadrant Based Intelligent Energy Controlled MultiCast Algorithm for Mobile Ad Hoc Networks". *13th International Conference on Advanced Communication Technology (ICACT)*, ISSN: 1738-9445, 2011.

[6] M. Pushpalatha, Revathi Venkataraman, T. Ramarao., "Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks". *World Academy of Science, Engineering and Technology International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, Vol:3, No:8, 2009.

[7] A.Josang, "An Algebra for Assessing Trust in Certification Chains". *Proc. Network and Distributed Systems Security*. (NDSS '99), 1999.

[8] S. Buchegger, J. Boudec., "Performance Analysis of the Confidant Protocol". MOBIHOC'02, June 9-11, 2002, EPFL Lausanne, Switzerland. ACM 1-58113-501-7/02/0006, 2002.

[9] P. Michiardi, R. Molva. "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks". *Proc. IFIP TC6/TC11 Sixth Joint Working Conf. Comm. and Multimedia Security*, 2002.

[10] Vivekananda Bharathi, Rama Chaithanya Tanguturi, C Jayakumar, K Selvamani., "Node capture attack in Wireless Sensor Network: A survey". *IEEE Conference on Computational Intelligence & Computing Research (ICCIC)*, 978-1-4673-1342-1, 2012.

[11] A.Josan, S. Pope., "Normalizing the Consensus Operator for Belief Fusion". *Proc. Int'l Conf. Information Processing and Management of Uncertainty*, July 2006.

[12] K Priyadharshini, G Hemalatha, K Selvamani., "Securing Wireless Sensor Network using Intelligent Techniques". *International Journal of Computer Applications* (0975 – 8887) Volume 70– No.18, May 2013.