Novateur Publication's
International Journal of Innovation in Engineering, Research and Technology [IJIERT]
ICITDCEME'15 Conference Proceedings
ISSN No - 2394-3696

EFFICIENT REBROADCASTING USING TRUSTWORTHINESS OF NODE WITH NEIGHBOUR KNOWLEDGE IN MANET

Shailesh P. Patil
PG Scholar, Dept. of Computer Engineering, Flora Institute of Technology, Pune
shaileshpp19@gmail.com
Pankaj R. Chandre
Assistant Professor, Dept. of Computer Engineering, Flora Institute of Technology, Pune
pankajchandre30@gmail.com

ABSTRACT
Mobile Ad hoc network is an infrastructure less communication network with limited resources. To maintain virtual infrastructure for communication broadcasting mechanisms is used. Due to lack of energy efficiency in Mobile Ad hoc network, there is a need to develop an efficient broadcasting model which enhances energy efficiency. Also nodes with malicious behaviour cause an internal threat that disobeys the standard and degrades the performance of routing protocols. This paper introduced an enhanced rebroadcasting algorithm, where rebroadcasting decision for next hop is immediate or delayed on the basis of trust value and energy level of particular node. This approach helps to decrease number of rebroadcast, energy consumption and also enhances security. The decision is made with trust value associated with node, their remaining energy and total number of uncovered nodes.

KEYWORDS— Mobile Ad hoc network, Neighbor Coverage, Probabilistic Rebroadcast, Routing overhead

INTRODUCTION
Mobile Adhoc NET work (MANET) is capable of building a network without any fixed infrastructure. In MANET, nodes act as a router as well as host, which allow multi-hop transactions with rebroadcasting the received packets. This network has a wide range of applications in the fields like emergency situations, disaster rescue operations, collaborative group meetings and military. In wireless networks, the information packets can be transmitted by means of broadcasting or rebroadcasting. Broadcasting is a widely used dissemination technique in which packet transmitted by a node is simultaneously received by all its neighbors. This mechanism is effectively used for route discovery and network maintenance. Simplest way of broadcasting is flooding in which every node rebroadcasts the received packet in the network. In large mobile environments, flooding has the overhead of redundant retransmission, contention and collisions [5]. MANET is vulnerable to various types of attacks because of open infrastructure, dynamic network topology, lack of central administration. Due to this fact malicious nodes can compromise network with unreliable behavior. Along with this Mobile ad hoc network devices rely on exhaustive means of energy like batteries and it does not have central administration so some trust is to be calculated while forwarding RREQ packet to verify whether node is authenticate or is having sufficient energy to forward packet in network. An energy efficient rebroadcasting mechanism in the network demands for optimized approach which can achieve significant reduction in retransmissions of packets.

LITERATURE REVIEW
Due to quick movement of nodes there is problem of frequent link breakage in MANET, which causes frequent link failure. It increases routing overhead which cannot be ignored. Common technique for route discovery is broadcasting which increases number of rebroadcasts and leads to broadcast storm problem.
D. Johnson et al. [1] gives the Dynamic Source Routing protocol (DSR), which is particularly used in multi-hop infrastructure. "Route Discovery" and "Route Maintenance", allows route discovery and maintenance of arbitrary destinations. Advantages of the DSR protocol consist of assured loop-free routing in unidirectional link network, "soft state" routing and quick recovery when routes in the network vary.
N. Karthikeyanet al. [2] addressed schemes to reduce redundant rebroadcasts, implements separate timing of rebroadcasts to improve this problem, thus routing performance gets better.

A. Keshavarz-Haddadyet al. [3] proposes deterministic timer-based broadcast schemes: Dynamic Connector-Connector Broadcast (DCCB) and Dynamic Reflector Broadcast (DRB). A deterministic, timer-based broadcast scheme gives assurance of full reach ability over an optimistic lossless MAC layer; it provides strength against node failure.

J. Kim et al. [4] addressed a probabilistic broadcasting scheme based on coverage area and neighbour confirmation. To set rebroadcast probability neighbour confirmation and coverage area are used which guarantees reach ability.

F. Stan net al. [5] introduces Robust Broadcast Propagation (RBP) protocol which gives near great reliability for flooding in wireless networks with good efficiency. Due to change in network topology frequent path failures occurs, due to which there is increase in the routing control overhead.

Xin et al. [6] gives a neighbour coverage-based probabilistic rebroadcast protocol (NCPR) for reducing routing overhead in MANETs. Numbers of retransmission are minimized by considering neighbour knowledge, which decreases routing overhead and improves routing performance.

Along with these certain trust based protocols where implemented which gives enhanced calculation of trustworthiness of neighbours to avoid malicious nodes intercepting within communication.

U.Ramyaet al. [7] in this paper, To minimize energy consumption of node three factors like node mobility, malicious behaviour and unauthenticated node are considered. For this purpose Energy Based Routing Algorithm (EBRA) is given which ensures the minimum energy consumption rate.

Suchita Gupta and AshishChourey [8] explains "Performance evaluation of packet drop attack in MANET", which consists of detection and isolation of misbehaving nodes which in turn reduces the network traffic. Objective of this paper is to identify and isolate the malicious nodes, which deals with improvement of the AODV protocol under packet drop attack.

K. Sreenivasuluet al. [9] this paper gives an optimized routing protocol EQSRWQOS, that provides Energy efficiency, better QoS and Security against attacks in MANET. It comprises of two mechanisms Transmission Power Control Approach, Transmission Power Optimization. Also to avoid hashing at each node a trust model is maintained.

Pedro B. Vellosoet al. [10] proposes human based trust model which builds trustworthy relationship between nodes in MANET. A protocol named Recommendation exchange Protocol (REP) is introduced which allows nodes to share recommendation about neighbours. Paper evaluated impact of malicious nodes sending false recommendation.

Shilpa S. G. et al. [11] proposes a trust model, trustworthiness of each node is determined based on trust value and remaining energy of each node. On the basis of which route selection is done.

Aravindh S. et al. [12] gives concept of trust counter, if trust counter falls below certain threshold the particular node is marked as malicious and is isolated from network which increases performance of network. Also by this packet forwarding decision is taken. It works with Trust handler, Reputation accumulator.

PROPOSED WORK

To improve performance of MANET it is necessary to consider energy efficiency of node and trust. If node falls below certain energy level and that node is selected for route discovery then on failure of that node the discovery is useless. Also if route is established by untrusted node then its malicious behavior will cause the degraded performance. So here forwarding of RREQ packet on the basis of two concepts trust and energy is considered.

Each node is having certain battery life, also each node have set of neighbour it is associated with say, $N(n_i)$. When a node s forwards RREQ packet to its neighbours it forwards its neighbour set $N(s)$, along with trust values associated with each node, $NT(s,t)$.

After receiving RREQ packet from neighbour instead of rebroadcasting RREQ packet to further nodes, the rebroadcast Order (RBO) is found on the basic of following three factors:

- Uncovered neighbour ratio (UNR):It is ratio of neighbours covered by previous node and total number of neighbour of current node [6].
- Trust value of node: Each node is associated with trust value of every neighbour. The trust value represents trustiness of its neighbour. Based on experiences trust value is adjusted. On the basis of which whether that node is included or excluded is considered [11].
- Energy of particular note: Every node in the MANET calculates its power consumption and finds the remaining energy periodically.[21]

A. UNCOVERED NEIGHBOUR RATIO (UNR):

When n_i receives RREQ from its neighbour it first calculates its uncovered neighbour set (UNS) values,

$$\mathrm{UNS}(n_i) = N(n_i) - [N(n_i) \cap N(s)] \quad (1)$$

Where,
$N(n_i)$ = neighbours set of node n_i
$N(s)$ = neighbours set of node s

The node which has a lower Rebroadcast order (RBO) may listen to RREQ packets from the nodes having larger RBO. Thus, node could further adjust its UCN.

Then, the UNS (n_i) can be adjusted as follows:

$$\mathrm{UNS}(n_i) = N(n_i) - [N(n_i) \cap N(n_j)] \quad (2)$$

After adjusting the UNS, the RREQ packet received from n_j is discarded.

When the timer of the rebroadcast order of node n_i expires, final UNS is obtained. These are the nodes which need to receive and process the RREQ packet.

Uncovered neighbour ratio (UNR) is calculated as:

$$\mathrm{UNR}(n_i) = \frac{\mathrm{UNS}(n_i)}{N(n_i)} \quad (3)$$

This Uncovered Neighbor Ratio indicates number of nodes remained to be covered.

B. TRUST VALUE OF NODE:

A trust value of each neighbour is stored which represents trustiness of each neighbour. On the basis of experiences trust value will be adjusted [15].

The trust can be calculated by three parameters:

Malicious (m): The node is said to be malicious if node x never sends any message to or from node y. Here trust value between both of them is low and probability that node is malicious is very high.

Known (k): Here node x and node y has some message communication previously, the trust value between them is not low or high, malicious behaviour of node is need to be observed.

Friend (f): When there is huge message transfer between two nodes then trust value of both is very high. Having malicious behaviour is very low.

On the basis of m, k, f node decides trust value for particular neighbour and depending on this, trust values between neighbours is found.

Trust values of node $t(n_i)$ are also updated as,

$$t(n_i) = \frac{(t_{prev}(n_i) + t_{rec}(n_i))}{2} \quad (4)$$

$t_{prev}(n_i)$ = Trust previously calculated.
$t_{rec}(n_i)$ = Trust received from neighbour.

C. ENERGY OF PARTICULAR NODE:

Every node in the MANET calculates its power consumption and finds the remaining energy periodically.

The energy is calculated on the basic of remaining energy and consumed energy. Consumed energy may be energy consumed for transmission of packet or energy consumed for reception of packet. Therefore remaining energy $E_{rem}(n_i)$ of particular node is:

$$E_{rem}(n_i) = E_{curr}(n_i) - E_{cons}(n_i) \quad (5)$$

$E_{curr}(n_i)$ = Current energy of node n_i.
$E_{cons}(n_i)$ = Energy consumed by node n_i.

Finally rebroadcast Order (RBO) is considered with combination of all above parameters;

$$RBO\ (n_i) = UNR(n_i) * t(n_i) * E_{rem}(n_i) \qquad (6)$$

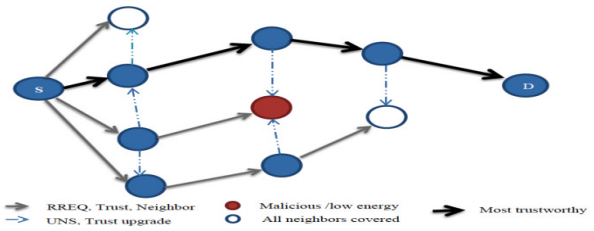

Fig. 1 A trustworthy boradcasting considering energy and trust constraint

By considering rebroadcast Order (RBO) the RREQ order is defined, the nodes having high RBO are considered to be most trustworthy node so broadcasting is to be done. Means if UNR becomes 0 means all neighbour covered so that node need not have to rebroadcast as already every neighbour is covered. Also when fewer neighbours covered nodes forward first, then remaining nodes with higher covered neighbours may automatically covered. If certain node falls below certain threshold of energy or trust then request is dropped.

PROPOSED ALGORITHM

{sis source node, RREQ is route request packet, UNS uncovered neighbour set }

1. Initialize nodes in MANET with initial trust values.
2. s Broadcasts RREQ packet along with Neighbour and Trust values of neighbour.
3. Calculate UNS and Trust of all neighbours.

{Calculation of battery life and trust values is done at intermediate nodes.}

4. If battery life or node trust is below threshold
    a. Drop packet. Remain silent
5. Else if all neighbours of node are covered
    a. Drop packet. Remain silent
6. Else
    a. Broadcast RREQ packet according to rebroadcast Order.

CONCLUSION

A new neighbour based broadcasting approach for mobile ad hoc network is introduced to reduce routing and maintenance overhead of the network, along with Energy consumption and security. A trust based authenticity of node is analyzed so untrusted nodes are avoided for further rebroadcasting of RREQ packets. Which in turn reduced retransmissions of packets and routing overhead, also avoids untrusted false route generation. This method includes neighbour coverage and timer based approach to identify the immediate rebroadcasting and wait state nodes. This proposed method will exploit the neighbour knowledge more efficiently to improve the performance of network by collaborative decision of neighbour trust value and energy level.

REFERENCES

[1] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol for Mobile Ad Hoc Networks (DSR) for IPv4", IETF RFC 4728, vol. 15, pp. 153-181, 2007.

[2] N. Karthikeyan, Dr. V. Palanisamy, and Dr. K. Duraiswamy, "Performance Comparison of Broadcasting methods in Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking Vol. 2, No. 2, June, 2009.

[3] A. Keshavarz-Haddady, V. Ribeirox, and R. Riedi, "DRB and DCCB: Efficient and Robust Dynamic Broadcast for Ad Hoc and Sensor Networks," Proc. IEEE Comm. Soc. Conf. Sensor, Mesh, and Ad-Hoc Comm. And Networks (SECON '07), pp. 253-262, 2007.

[4] J. Kim, Q. Zhang, and D.P. Agrawal, "Probabilistic Broadcasting Based on Coverage Area and Neighbour Confirmation in Mobile Ad Hoc Networks," Proc. IEEE GlobeCom, 2004.

[5] F. Stann, J. Heidemann, R. Shroff, and M.Z. Murtaza, "RBP: Robust Broadcast Propagation in Wireless Networks," Proc. Int'l Conf. Embedded Networked Sensor Systems (SenSys '06), pp. 85-98, 2006.

[6] Xin Ming Zhang, Member, IEEE, En Bo Wang, Jing Jing Xia, and Dan Keun Sung, Senior Member, IEEE, "A Neighbour Coverage-Based Probabilistic Rebroadcast for Reducing Routing Overhead in Mobile Ad-Hoc Networks", IEEE Transactions on Mobile Computing, vol. 12, no. 3, March 2013.

[7] U.Ramya, M.Arockiya Stalin Mary and R.Kayalvizh, "Reducing Energy Consumption in MANET under Different Scenarios,"IJAIST,Vol.4, Issue 1ISSN: 2319-2682August 2012.

[8] Suchita Gupta, and AshishChourey, "Performance evaluation of AODV protocol under packet drop attacks in manet," International Journal of Research in Computer Science, eISSN 2249-8265, Vol. 2, Issue 1, 2011.

[9] K Sreenivasulu, Dr.E V Prasad, and Dr. A. Subramanyam, "EOSRWQOS: An Energy Efficient Secured Routing for MANETs," International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3, Issue 2, ISSN 2278-6856, March – April 2014.

[10] Pedro B. Velloso, Rafael P. Laufer, Daniel de O. Cunha, Otto Carlos M. B. Duarte, and Guy Pujolle, "Trust Management in Mobile Ad Hoc Networks Using a Scalable Maturity-Based Model," 172 IEEE transactions on network and service management, vol. 7, no. 3, Sept. 2010.

[11] Shilpa S G, Mrs. N.R. Sunitha , and B.B. Amberker ,"A Trust Model for Secure and QoS Routing in MANETS," International journal of innovative technology & creative engineering (issn:2045-8711),Vol.1, No.5, May 2011.

[12] Aravindh S, Vinoth R S andVijayan R," A trust based approach for detection and isolation of malicious nodes in manet," International Journal of Engineering and Technology (IJET), vol. 5 no. 1, ISSN: 0975-4024, Feb-Mar 2013.

[13] Gurnam Singh, and Gursewak Singh," Improvement of Network Efficiency by Preventing Black Hole Attack in Manet," International Journal of Innovative Technology and Exploring Engineering (IJITEE), ISSN: 2278-3075, Vol. 4 Issue-2, July 2014.

[14] MeenaBharti , Manish Goyal and RajanGoyal," Detection of rushing attack by comparing energy, throughput and delay with AODV," IPASJ International Journal of Computer Science (IIJCS),ISSN 2321-5992, Volume 2, Issue 11, November 2014.

[15] SenthilkumarSubramaniyan, William Johnson and KarthikeyanSubramaniya, "A distributed framework for detecting selfish nodes in MANET uses Record- and Trust-Based Detection (RTBD) technique," eurasip journal 2014.

[16] Andrea Lupia, and Floriano De Rango, " Evaluation of the Energy Consumption Introduced by a Trust Management Scheme on Mobile Ad-hoc Networks," journal of networks, vol. 10, no. 4, April 2015

[17] M.Abinaya, and MrsK.Thamaraiselvi, " EffectiveNeighbour Identification with False Report Verification Using Manets," International Journal of Innovative Research in Computer and Communication Engineering,(IJIRCEE) , Vol.2, Special Issue 1, March 2014.

[18] S.NeelavathyPari, and D.Sridharan ," A Performance Comparison and Evaluation of Analysing Node Misbehaviour in MANET using Intrusion Detection System," IJCSET, Feb 2011, Vol 1, Issue 1,35-40

[19] Rajeev Raman, Narendra Pal, Singh Rathore," A Survey on "Energy Efficient and Secure Infrastructure for MANET Jamming Attack," International Journal of Engineering Trends and Technology (IJETT) Vol. 23,No. 8- May 2015.

[20] Gaurav Sharma, and Mehajabeen Fatima,"An Energy Efficient Approach for Wormhole Detection and Prevention," International Journal of Computer Applications (0975 – 8887) Volume 76– No.17, August 2013.

[21] RagulRavi.R, Jayanthi.V, "Energy Efficient Neighbour Coverage Protocol for Reducing Rebroadcast in MANET", Procedia Computer Science 47, 417 – 423, 2015.