ISSN (ONLINE): 2454-9762
ISSN (PRINT): 2454-9762
Available online at www.ijarmate.com
International Journal of Advanced Research in Management, Architecture, Technology and Engineering (IJARMATE) Vol. 3, Issue 5, May 2017

A Recovery Based Minimal Rerouting Scheme For MANETs

H Prabavathi[1], A Archana[2]
1. Assistant Professor, Department of CSE, A.V.C.College of Engineering
2. PG Student, Department of CSE, A.V.C.College of Engineering

ABSTRACT — Mobile Ad hoc networks are autonomous collection of devices that enables communication in an on-demand manner. Due to its decentralized nature, the network is exposed to external security issues due to which the performance of the network is retarded to a greater extent. To avoid inbound network misbehavior and node elimination here we propose markov based prediction, rank based node selection and secure transmission methods. To further optimize neighbor selection and to improve network performance by minimizing backtracking process, an integrated approach of Recovery Path Routing (RPR) and ranking were proposed. Rank method selects a node by its behavior wherein recovery routing initiates rerouting from the discontinued node and also prevents backtracking issues. As a result, the network has less impact towards re-transmission and detection by avoiding multiple flood issue. The simulation proves the effectiveness of the proposed system by improving detection rate and minimizing drop and delay.

Keywords - **Hyper-geometric distribution; Markov process; Rank process; Recovery Path Routing.**

I INTRODUCTION

Mobile Ad hoc Networks (MANETs) consisting of a collection of wireless mobile nodes that communicate with each other without having any centralized monitoring system. MANETs can be deployed efficiently and there arise a number of issues in routing. Routing is very much difficult in MANETs because of no centralized monitoring network terminal, mobility may cause radio links to breakup frequently. When any link of a path is break, this path needs to be either repaired through finding another link or replaced by a newly found path. Such rerouting operation wastes the scarce radio resource and battery power whereas rerouting delay may affect the quality of service (QoS) and de-grade network performance. To reduce rerouting operation, path reliability may be more important in selecting optimal paths in MANETs than other metrics such as path cost and QoS that are frequently used in wired networks. Link availability is used to find the link available by measuring the probability or degree. Prediction-based link availability gives estimation to quantify the link reliability. This quantity uses some instantly available information and also considers the dynamic nature of link status in order to properly reflect the link reliability **[1]**.

Other issues is to cope up with the selfish behavior of the neighboring node whereas routing and forwarding it is mandatory to study and analyze the behavior of selfish neighbors in the network so we introduce a probabilistic model that observes the behavior of the intermediate node whereas forwarding packets from source to destination. For this, they use a markov process to represent a cluster of one-hop neighbors as one collaboration point. As a result they able to regulate the collaboration based on residual energy, the number of neighbors in the cluster and other network parameters **[2].** Another thing is network topology of MANETs changes rapidly hence there occurs a routing attack. Security is a major issues in this infrastructure, here three attacks namely selfish node attack, shared root node attack and control packet attack are consider out of this the shared root node has more vulnerable issues, using Multicast Ad hoc On Demand Distance Vector (MAODV) protocol these attacks are evaluated using three parameters namely packet delivery ratio, control overhead and total overhead to overcome this attack **[3].** Hence this protocol is insufficient due to multiple link failure and state transition increase a pause time of the communication. To cope up with those types of issues proficiently we introduce a rank based secure scheme with recovery path routing that reduces the backtracking of data packet. .

II RELATED WORK

In case of shared root node attack, the attacker node disguises a tree node and sends a MACT packets i.e., a tree prune control packet to all the nodes' present in the multicast tree. If a downstream node has one and only downstream link and if it is a non member, it prunes itself and sends a prune message to its entire downstream node. This may cause multicast tree to be pruned. So the multicast pruning may disturb the group communication by not relaying the packets to the multicast members as well as the non members. Here, we propose a detecting shared root node algorithm to identify the mobile nodes which tries to exhibit shared root node behavior. The identified attacker nodes are removed and new zone leader is elected by means of the secure zone leader election algorithm. The newly elected zone leader will update its entries in the multicast table. The zone is reconstructed with the help of newly elected zone leader. The Mitigating mechanisms for rendezvous point attack has (i) A Markov process based prediction model that detects a attack node futuristically has not been much explored to the best of our knowledge. (ii) A forecasting model that incorporates a Hyper-geometric trust factor for mitigating rendezvous point attack for enhancing packet delivery rate is not examined. Hence, these limitation may result in introducing Hyper-geometric Trust Factor based Markov Prediction Mechanism (HTFMPM) for extenuating rendezvous point attack that quantifies the pressure of rendezvous point attack. In this model a rank based scheme has been introduced to quantify the node transmission rate by using the behavior model.

III PROPOSED WORK

In a new rank based self initiated routing method is proposed to select/identify active transmission neighbor based on distributed trust by the neighbors self initiated forwarding avoids back tracking of packets and thus minimizes source drop. The integrated approach provides secure transmission for a MANET. This process is performed by the following task as,

o Neighborship based detection. o
Ranking process.
o Recovery node
identification and rerouting.

- *A. Neighborship based detection*:

Each node shares its position at the maximum displacement. Displacement update is used to find the accurate neighbor for propagation. (it minimizes link failures).

From large ranked to minimum ranked condition makes specific for selection that is lesser transmission overhead. Supports multi path node selection.

B. Ranking Process:

- Based on the trust gain, each node broadcasts its rank to the communication requesting node.
- Rank is given to those that are in range at the time of broadcast.

Trust Factors:

Packet delivery factor and response time are the trust factors considered here. In this, packet delivery factor is increases with response time or decreases otherwise, Drop decreases if response time decreases.

Packet Transaction rate:

$$P_{Tr} = \Sigma d(i)t(i)_{ni=0}$$

Packet drop:

$$d_p=\Sigma[dr(i)\sim`ds(i)t(i)-t(i\sim t)ni=0+ dr(i+1)\sim ds(i+1)t(i+1)-t(i+1\sim t)+\cdots+dr(i+n)\sim ds(i+n)t(i+n)-t(i+n \sim t)]$$

Response time:

$$r_t=\Sigma[TRreq(i)-TRrep(i)Kki=1$$

Where, Ksequence of 1,2,3.., K t(n)

Probability of rt:

$r_t \rightarrow$ *S to D when* $\{d_p(t)>0 \text{ or } d_p(t)\neq 0\}$

Trust Computation:

To compute the trust factors using the following formulae,

$T_N(i)=\pi_{PTr-dpPTr}=: r_t$ Where t≠0 {for all $_{mk}\in T_N$}

if, $dp=0$;

$T_N(i)=\pi_{PTr\,PTr}: r_t$

$TN(i)= \pi\, rt$

Node selection:
To select the node for routing we are using the following formula,
Node selection = Max$\{TT_N(i),T_N(i+1),..T_N(i+x)\}$
Ranking Process:

- Rank lies between one and number of nodes in range.
- If all the trust values are satisfied, rank=1
- If almost one condition is not satisfied, rank=2
- If more than one condition is not satisfied, rank=number of nodes – 1
- If number of condition is satisfied, rank = number of nodes in range + 1.

A neighbor is discarded based on:

- Larger rank.
- If it denies to share previous history of rank.
- If it is out of range.
- If miscommunicated.

C. Recovery Node Identification and Rerouting:

Identify the recovery node to initiate the transmission. It prevents backtracking (i.e) avoids data to be transmitted back to the source from the point of drop. The recovery node is selected based on the broadcast a node receives (at the time of source routing) from its forwarding node. Recovery node initiates re-transmission rather than broadcasting. Further node selection is based on weighted node selection/ shortest path from the recovery node.

IV Architecture

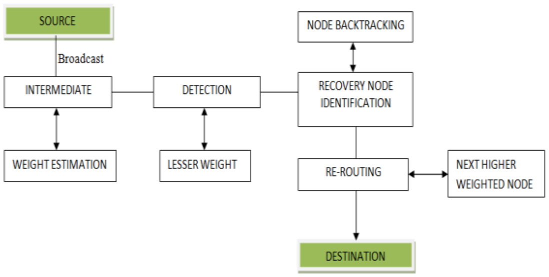

Fig. 1 shows the flow of how the packet transfer from source to destination via intermediate node using the Ranking based secure routing scheme in MANETs with recovery path routing.

V Experimental Result

In this experiment, the performance of the proposed rank based approach assessed by varying the number of root node attacker and recovery path routing that reduces the source node queue in the simulation environment. These experiments shows the Packet Delivery Ratio (PDR), throughput, average packet latency, packet drop rate and detection rate derived from various mitigation mechanisms. In Ad hoc network, the PDR value decreases as number of root node attackers increases, the proposed system increase the PDR when compared with other existing system and also it reduces the backtracking of packets.

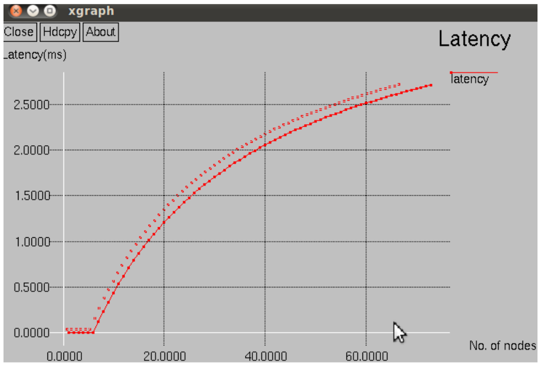

Fig.2 represents the comparison graph between the no. of nodes and latency.

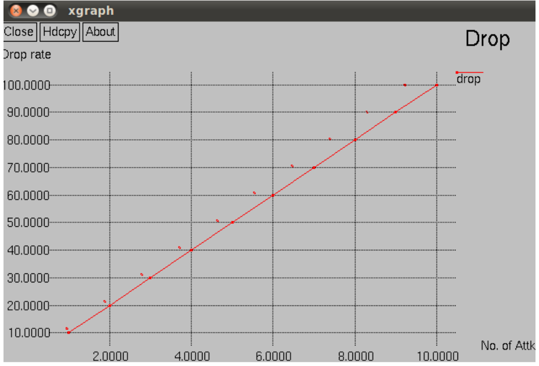

Fig. 3
Fig.3 shows the comparison graph between the no. of attackers and drop rate.

VI Conclusion

We have studied the problem of transmission overhead due to backtracking of packets. A new rank based self initiated routing method is proposed to select active transmission neighbor based on distribution by the neighbors. Self initiated forwarding nodes avoid backtracking of packets and thus minimizes source drop. This integrated approach provides secure transmission for a MANET. As a result, the network has less impact towards re-transmission and detection by avoiding multiple flood issue.

VII Reference

[1] Jiang, S.; He, D.; Rao, J.: "A prediction-based link availability estimation for routing metrics in MANETs." *IEEE ACM Trans. Netw*. **13**(6), 1302–1312 (2005)

[2] Komathy, K.; Narayanasamy, P.: "A probabilistic behavioral model for selfish neighbors in a wireless ad hoc network." *Int. J. Comput. Sci. Netw. Secur.* **7**(7), 77–82 (2007)

[3] Sengathir, J.; Manoharan, R.: "Security algorithms for mitigating selfish and shared root node attack in MANETs." *Int. J. Comput. Netw. Inf. Secur*. **5**(10), 1–10 (2013)

[4] Parthiban, S.; Rodrigues, P.: "Swarm based energy aware mitigation mechanism for root node attacks in MANETs." *In: 13th WSEAS International Conference on Recent. Advances in Telecommuni-cations, Informatics and Educational Technologies, Turkey*, ISBN: 978-1-61804-262-0, pp. 199–207 5–17 (2014)

[5] De Rango, F.; Guerriero, F.; Fazio, P.: "Link-stability and energy aware routing protocol in distributed wireless networks." *IEEE Trans. Parallel Distrib. Syst.* **23**(4), 713–726 (2012)

[6] Buchegger, S.; Le Boudec, J.Y.: "A robust Reputation system for mobile ad-hoc networks." *EPFL IC Technical Report IC*/2003/05

[7] Michiardi, P.; Molva, R.: CORE:" A collborative repudiation mech-anism to enforce node cooperating in mobile ad hoc networks*." In: Proceeding of the 6th Joint Working Conference on Communica-tions and Multimedia Security*, pp. 107–121

[8] Mei, A.; Stefa, J.: Give 2Get: "Forwarding in social mobile wireless networks of selfish individual." *IEEE Trans. Dependable Secure Comput.* **9**(4), 569–581 (2012)

[9] Md. Akhtar, A.K.; Sahoo, G.: "Mathematical model for the detection of selfish nodes in MANETs." *Int. J. Comput. Sci. Inform*. **1**(3), 25– 28 (2008)

[10] Marti, S.; Giuli, T.J.; Lai, K.; Baker, M.: "Mitigating rout-ing misbehavior in mobile ad hoc networks." *Mobile Comput. Netw.* **1**(1), 255–265 (2000)

[11] Hernandez-Orallo, E.; Serraty, M.D.; Cano, J-C.; Calafate, T.; Man-zoni, P.: "Improving selfish node detection in MANETs using a collaborative watchdog." *IEEE Lett*. **16**(5), 642–645 (2012)

[12] Xing, F.; Wang, W.: "Modeling and analysis of connectivity in mo-bile ad hoc networks with misbehaving nodes." *In: Processing of IEEE International Conference on Communications*, vol. 4, No.3, pp. 1879–1884 (2006)

[13] Cárdenas, A.A.; Radosavac, S.; Baras, J.S.: "Evaluation of detec-tion algorithms for MAC layer misbehavior: theory and experi-ments." *IEEE Trans. Netw*. **17**(2), 605–617 (2009)

[14] Xing, F.; Wang, W.: "On the survivability of wireless ad hoc networks with node misbehaviors and failures." *IEEE Trans. Dependable Secure Comput.* **7**(3), 284–299 (2010)

[15] Roy, S.; Addada, V.G.K.; Setia, S.; & Jajodia, S.: "Securing MAODV: attacks and countermeasures" *In: 2nd IEEE International Conferences SECON* (2005)

[16] Xia, H.; Xia, S.; Yu, J.; Jia, Z.; Sha, E.H.-M.: "Applying link stability estimation mechanism to multicast routing in MANET's*." J. Syst. Archit*. 467–480 (2014)

[17] Hua, E.Y.; Haas, Z.J.: "An algorithm for prediction of link lifetime in MANET based on unscented Kalman Filter." *IEEE Commun. Lett.* **13**(10), 782–784 (2009)

[18] Namuduri, K.; Pendse, R.:" Analytical estimation of path duration in mobile ad hoc networks." *IEEE Sens.* J. **12**(6), 1828–1835 (2012)

[19] Shandilya, V.; Simmons, C.B.; Shiva, S.: "Use of attack graphs in security systems." *J. Comput. Netw. Commun.* **7**(7), 77–82 (2014)

[20] Buchegger, S.; Boudec, J-Y.: "Nodes bearing grudges: towards rout-ing security, fairness and robustness in mobile ad-hoc network." *In: Presented at Tenth Eurominicro*
workshop on Parallel, Distributed and Network based Processing, Canary Islands, Spain (2002)

.