Power Aware and Secure Routing in MANET using a Hybrid and Novel Approach

Pratyush Yadav and Mrs. Shaheen Naaz
[1]M.Tech Student, [2]Assistance Professor
Department of Electrical, Electronics and Communication Engineering
Sharda University, Greater NOIDA

Abstract: In order to make routing in MANETs secure, number of security based routing protocols have been proposed in the literature but none of them is compliant with the MANETs environment. The monitoring operation is distributed among a few set of nodes called monitor nodes. The set of monitor nodes is selected sporadically which makes the proposed method adaptable to the two focal concerns of MANETs: dynamic network topology and energy constraint devices. The method detects malicious packet dropping and packet modification attacks.

This algorithm has also been developed to reduce the packet dropping attack in MANET which has been simulated on MATLAB and demonstrated an increase in packet delivery ratio, throughput while decrease in average.

I. INTRODUCTION:

Recent advances in wireless technology have equipped portable computers, such as notebook computers and personal digital assistants with wireless interfaces that allow networked communication even while a user is mobile. A particular kind of wireless network called mobile ad hoc networks is presently under development. A mobile ad hoc network is a selforganizing and rapidly deployable network in which neither a wired backbone nor a centralized control exists. The network nodes communicate with one another over scarce wireless channels in a multi-hop fashion. The ad hoc network is adaptable to the highly dynamic topology resulted from the mobility of network nodes and the changing propagation conditions. These networks are used in emergency disaster rescue operation, tactical military communication and law enforcement. In these applications, where a fixed backbone is not available, a readily deployable wireless network is needed. Mobile ad hoc networks are additionally a decent option in provincial regions or underdeveloped nations where essential correspondence foundation isn't entrenched. Another intriguing utilization of mobile ad hoc networks is omnipresent processing. Wise gadgets are associated with each other by means of remote connections and are self-sorted out such that a recently joined hub can ask for benefit from nearby servers with no human intercession. With the advancement of the up and coming age of wireless correspondence frameworks, there will be a requirement for the fast organization of free mobile clients. A few cases of conceivable uses incorporate understudies utilizing PCs to take an interest in an intuitive address, business partners sharing data amid a gathering, and crisis calamity alleviation work force planning endeavors after a tropical storm or seismic tremor. Such system situations can't depend on unified and sorted out availability, and can be considered as uses of Mobile Ad Hoc Networks. A MANET is a self-ruling accumulation of mobile clients that convey over generally data transfer capacity compelled wireless connections. In view of the portability of the nodes, the system topology may change quickly and unusually. Because of versatility requirement of nodes the system operational trademark is capricious. Consequently a course chose would not be ideal after a correspondence period. To build up a directing plan most solid in adhoc organize, secure routing are need.

Security Model

In MANET the main security treat is the packet dropping attack. In packet dropping attack some malicious nodes in the network try to capture some packets and then drop them. This diminishes the Packet Delivery Ratio (PDR) and Throughput of the system. In MANET most generally utilized steering convention is AODV which does not has any methodology to find the malevolent hub in the system. Subsequently, to execute security in AODV a distributive recognition calculation is proposed here. In this calculation each hub sets itself in the wanton mode and after that checks the conduct of the neighboring hub to choose about the noxious conduct of the hub based on some flag esteems related with every hub. Amid the steering procedure every one of the nodes keep up their flag esteems which might be utilized to check the conduct of some other hub in the system. The insights about calculation of flag esteems are given beneath in Algorithm 1:

Algorithm 1: Computation of Flag values

1) $F(AB) = F(B) + F(\sum Bi)$ Where $F(AB)$= In this flag value node A checks the behavior of node B and this flag

value set to false by node A if the behavior of node B is unexpected.

F(B)= Node A set this flag value on the basis of its own monitoring and calculations.
F(∑Bi) = This flag value is the sum of the flags of other nodes which monitors node B directly.

2) F(B)+F(B1)+F(Bn2)+----------F(B) > N=2

3) F(AB) is turned false if F(B) is turned false and F(∑B) > N=2 So by the help of these steps we can detects the malicious nodes in the network and after detection we can block them for the further communication.

II. RESULT EXPLANATION

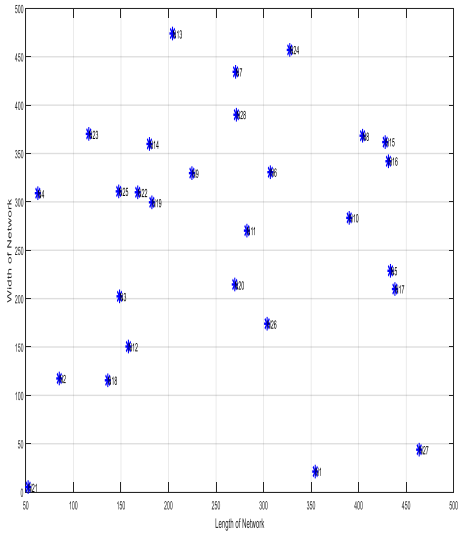

Fig 1: Network Creation

The fig 1 shows the network creation in which the nodes are deployed in the network having length of 500 meters in length and 500 meters in width and shows the total area of 1000 meters. The simulation is achieved using MATLAB programming

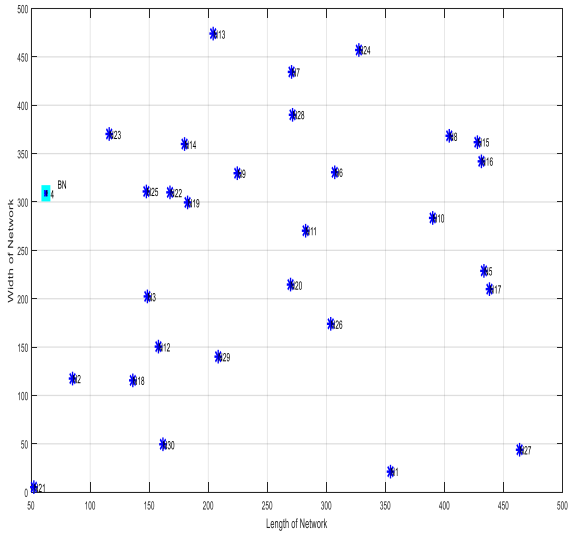

Fig 2: Identification of black hole node

The fig 2 shows the black hole node in the cyan color and also it acts as a malicious node which will generate the fake route path

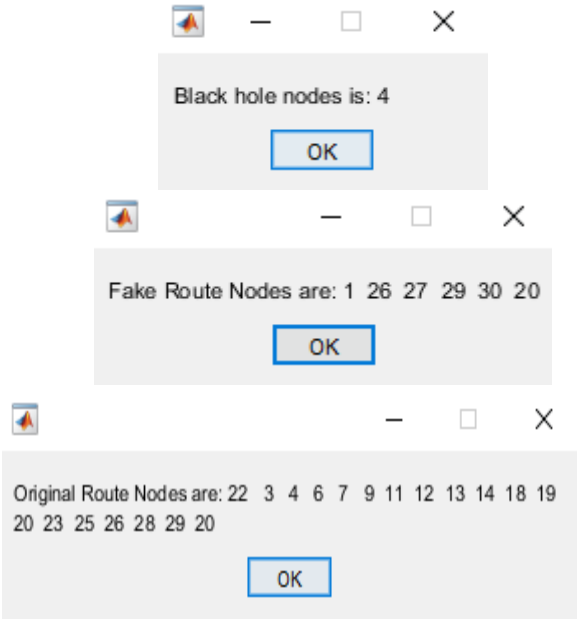

Fig 3: Node ids (Black Hole node, Fake Rout, Original Route after Mitigating)

The fig 3 shows the node ids for the black hole node and also the fake route node ids which is done by the malicious node in the presence of attack and also the original node ids which is achieved after mitigating the effect of attack in the sensor network

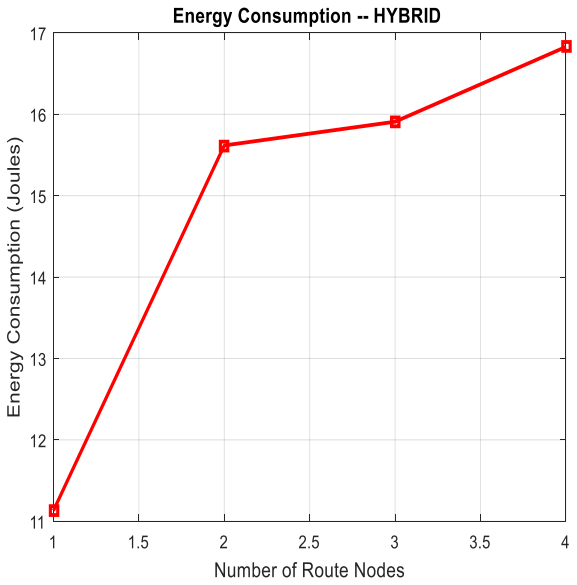

Fig 4: Energy consumption

The fig 4 shows the energy consumption with respect to the total number of nodes which are performing or participating in the route and shows that the hybrid approach is able to achieve less energy consumption which will increase the lifespan of the nodes

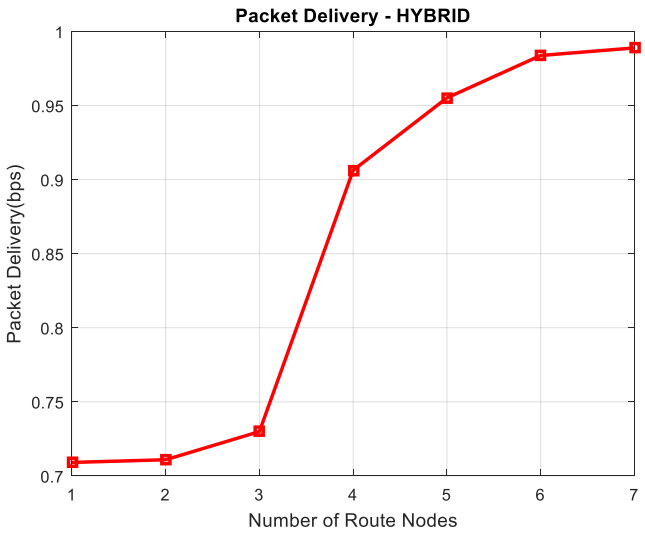

Fig 5: Packet Delivery

The fig 5 shows the packet delivery of the network in terms of probability which shows that the proposed approach is able to achieve high packet delivery in terms of successful packet deliveries and it is showing closest to the 1 which shows that the proposed system is able to achieve high packet deliveries

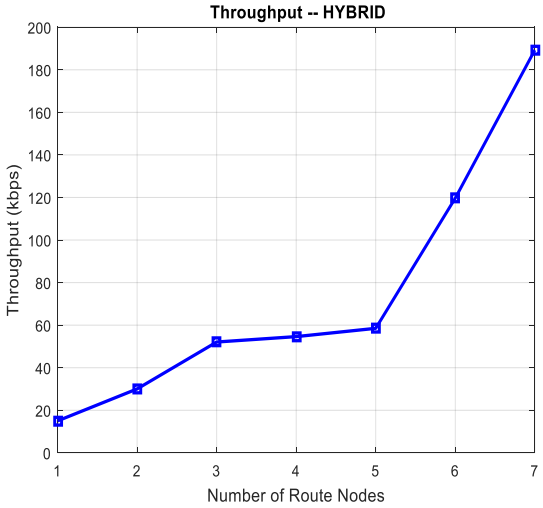

Fig 6: Throughput

The fig 6 shows the throughput in kilobits per second and shows the proposed approach is able to achieve high throughput of the network which shows the network is delivering packets from source to the destination in attack free environment which is done in the efficient manner by our proposed approach

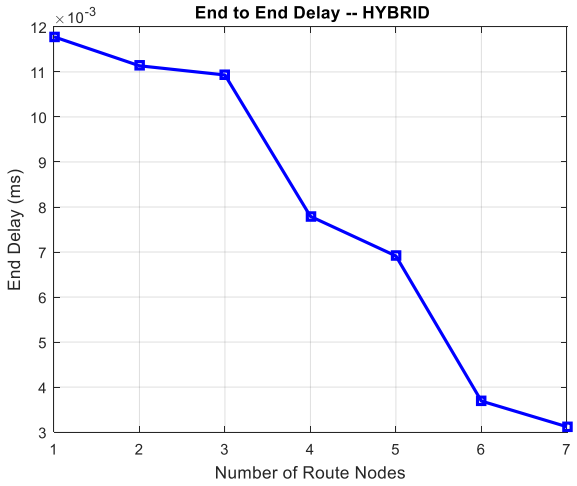

Fig 7: End Delay

The fig 7 shows the end delay of the network which must be low for high packet deliveries and less packet losses which shows that the proposed system is able to achieve less end delay from the source to the destination

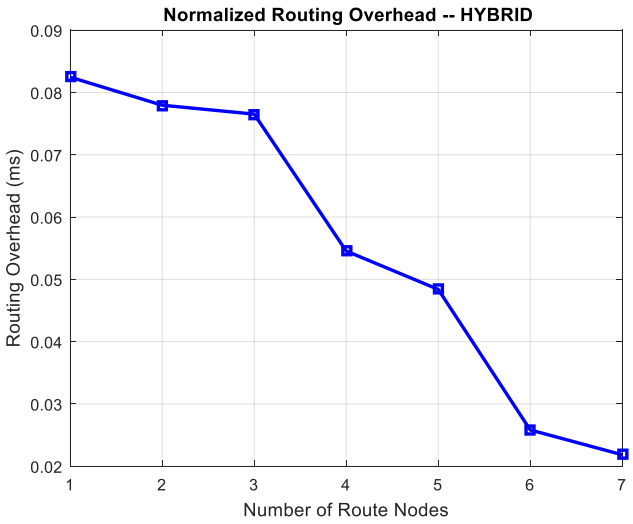

Fig 8: Routing Overhead

The fig 8 shows the routing overhead of the network which is one of the important parameter in the sensor network which must be less for the low efficient overhead for the less collisions of the packets between the nodes in the sensor networks. This parameters must be less as the number of routing nodes increases

III. CONCLUSION:

In this paper two calculations are proposed to enhance the vitality utilization and security of MANET. The proposed calculations use the dynamic course shortening and nearby course repair plan to enhance the dependable parcel conveyance and upgrade the course support if course breaks happen due to less residual vitality in the nodes. The proposed plans can be consolidated into any Ad-hoc on request directing convention.

REFERENCES:

[1]. J. Wang, Y. Liu, and Y. Jiao, "Building a trusted route in a mobile ad hoc network considering communication reliability and path length," Journal of Network and Computer Applications, vol. 34, no. 4, pp. 1138–1149, 2011.

[2]. G. Varaprasad and R. Wahidabanu, "New power-aware multicast algorithm for mobile ad hoc networks," IEEE Potentials, vol. 32, no. 2, pp. 32– 35, 2013.

[3]. J. Von Mulert, I. Welch, and W. K. Seah, "Security threats and solutions in manets: A case study using aodv and saodv," Journal of Network and Computer Applications, vol. 35, no. 4, pp. 1249–1259, 2012.

[4]. N.-C. Wang, Y.-F. Huang, and J.-C. Chen, "A stable weight-based ondemand routing protocol for mobile ad hoc networks," Information Sciences, vol. 177, no. 24, pp. 5522–5537, 2007.

[5]. A. Mahimkar and R. K. Shyamasundar, "S-MECRA: a secure energyefficient routing protocol for wireless ad hoc networks," in Proceedings IEEE 60th Vehicular Technology Conference (VTC2004), vol. 4, pp. 2739–2743 Vol. 4, 2004.

[6]. J. Furthm¨uller and O. P. Waldhorst, "Energy-aware resource sharing with mobile devices," Computer Networks, vol. 56, no. 7, pp. 1920–1934, 2012.

[7]. J. Gomez, A. T. Campbell, M. Naghshineh, and C. Bisdikian, "Conserving transmission power in wireless ad hoc networks," in Proceedings of the 9 IEEE International Conference on Network Protocols., pp. 24–34, 2001.

[8]. J. S. Yang, K. Kang, Y.-J. Cho, and S. Y. Chae, "PAMP: Power-aware multi-path routing protocol for a wireless ad hoc network," in Proceedings IEEE Wireless Communications and Networking Conference (WCNC'08), pp. 2247–2252, 2008.

[9]. R. Vadivel and V. M. Bhaskaran, "Energy efficient with secured reliable routing protocol (eesrrp) for mobile ad-hoc networks," Procedia Technology, vol. 4, pp. 703–707, 2012.

[10]. M. Pan, S.-Y. Chuang, and S.-D. Wang, "Local repair mechanisms for on-demand routing in mobile ad hoc networks," in Proceedings 11 IEEE Pacific Rim International Symposium on Dependable Computing, pp. 8–13pp, 2005.

[11]. P. M. John and P. Vivekanandan, "A framework for secure routing in mobile ad hoc networks," in Proceedings IEEE International Conference on Advances in Engineering Science and Management (ICAESM), pp. 453–458, 2012.

[12]. H. Kopka and P. W. Daly, A Guide to L Addison-Wesley, 1999. TEX, 3rd ed. Harlow, England: