Enhancement of Security in MANET using Optimized Reactive Protocol

Pooja Rani[1] Er. Ramandeep Singh[2]
[1,2]Department of Computer Science & Engineering
[1,2]AIET Faridkot & Faridkot, India

Abstract— The investigations of energy-efficient communication in wireless networks provide many future research directions. The performance of any routing protocol mainly depends on the energy consumed while travelling from source to destination. We seek to optimize the energy in wireless network through routing. Essentially, energy optimization is used to enhance the lifetime so that less energy can be consumed, additional packets should be distributed with less Bit Error Ratio and less routing overhead.In this research, the performance analysis of reactive protocol is evaluated. MANETs are the dynamic network where topology can change with respect to time. So, the network topology becomes unstructured and node enters or leaves the network according to their need. As per Mobile Ad-hoc Network (MANET) is a collection of communication devices or nodes that wish to communicate without any fixed infrastructure and predetermined organization of available links. Security is a major challenge for these networks owing to their features of open medium, dynamically changing topologies.

Keywords: MANETs, Reactive Protocol

I. INTRODUCTION

MANET is a type of infrastructure-less wireless network which is dynamic in nature and nodes are mobile. A routing protocol for MANETs is a convention that governs all the nodes within the network to decide how to find a route to the destination in a Mobile Ad hoc Network. Routing between two nodes in an ad-hoc network is not an easy or trivial task because of the mobile nature of nodes. Moreover, a node can quit or switch the network suddenly. Due to increase in popularity of wireless mobile devices, researchers have proposed many routing protocol designs [1] to let the nodes connect with each other to communicate in an efficient and timely manner which are divided in many categories but three main categories are Proactive, Reactive and Hybrid routing protocol.

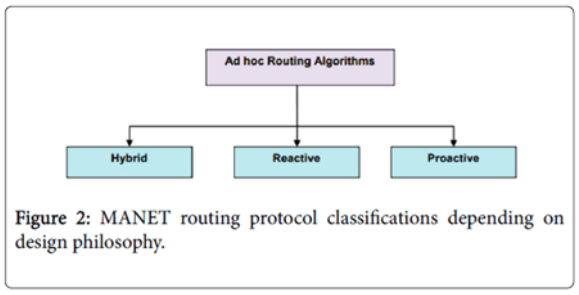
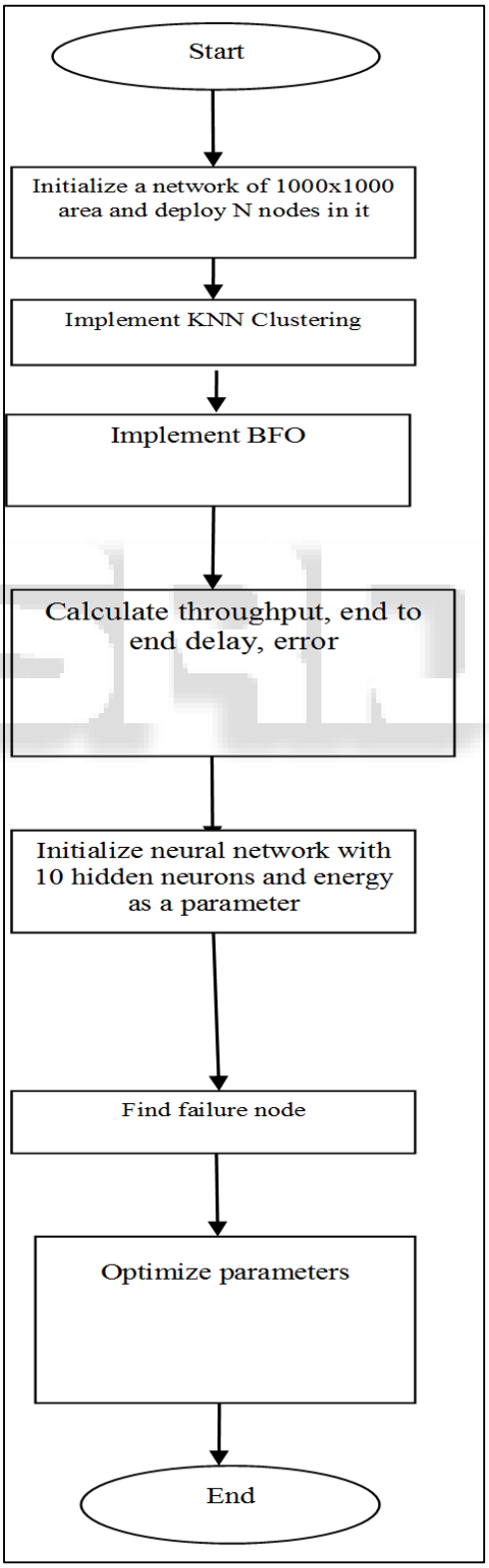


Figure 2: MANET routing protocol classifications depending on design philosophy.

reactive routing protocol is calculated on the basis of different parameter such as packet delivery ratio, end to end delay and throughput. Various challenges related to routing and security has been discussed and a new optimized authenticated (Adhoc On demand Distance Vector) is proposed. This secure optimized protocol uses KNN clustering to handle different network areas and generates a path based on BFO mechanism. For more security, shared key mechanism is also added to this proposed protocol. Results show the performance improvement in terms of both routing and security.

II. METHODOLOGY



III. SYSTEM MODELLING DESCRIPTION

The Following Development Tools has been used in the development of this work. There may also be other tools which can be used in this project as it depends person to person and his interest. Therefore the used tools are Minimum of 3 GB of RAM, Intel Pentium III Processor or Above, The tool used for the simulation of results is NS-2. It is discrete event simulator for networking research and works at packet level. The parameters considered in the simulation are Packet delivery Ratio, Average DelayFor comparison of the traffic type NS2 simulator with different simulation settings are being used.

The Following Development Tools has been used in the development of this work. There may also be other tools which can be used in this project as it depends person to person and his interest. Therefore the used tools are—

- Minimum of 3 GB of RAM
- Intel Pentium III Processor or Above
- MATLAB Software
- Window 7
- The tool used for the simulation of results is NS-2. It is discrete event simulator for networking research and works at packet level. The parameters considered in the simulation are Packet delivery Ratio, Average Delay.

For comparison of the traffic type NS2 as simulator with different simulation settings are in table no.1

IV. RESULT ANALYSIS

A. *End to End Delay:*

It is total delay that has been produced while packet is sent from source to destination.
End to End Delay=received time-sent time

B. *Throughput:*

Total packet sent in total communication time.
Throughput=(total packet sent-Packets received)/total time

TIME(s)	0	4	8	12	16	20	24	28
BASE AVG DELAY	0	0	0	0	0.058	0.041	0.041	0.31
NEW AVG DELAY	0	0	0	0	0.028	0.021	0.011	0.01

Table 4.1: PDR

C. *Packet Delivery:*

It means how many packets have been forwarded or successfully sent from source to the destination. It is received= (send-dropped).

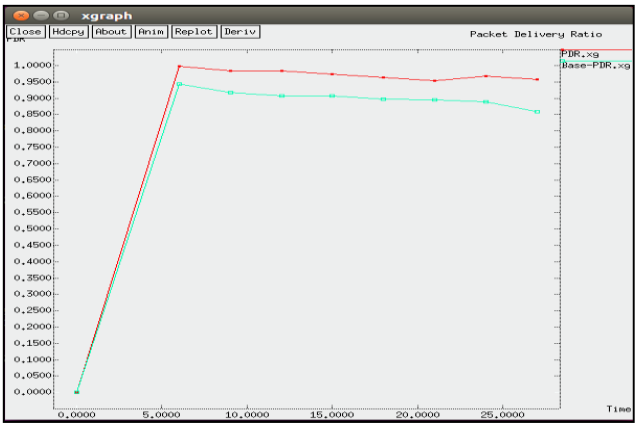


Fig. 3.1: Packet delivery Ratio with 170 nodes.

TIME	0	4	8	12	16	20
BASE PDR	0	0	0.95	0.91	0.90	0.89
NEW PDR	0	0	0.99	0.98	0.98	0.97

Table 4.2: Delay

Shown in figure and table no.3.1 packet deliver ratio with 170 nodes and table no.3.1 define reading of nodes

1) *End to End delay:*

It includes the average delay that is caused by buffering during route discovery, latency, and retransmission by intermediate nodes etc. for receiving the packet

Fig. 3.2: Delay with 170 nodes

Shown in figure and table no.3.2 delay with 170 nodes and table no.3.2 define new average delay

2) *Throughput:*

It is the amount of data packets that are transferred successfully from source to destination in a particular time instance.

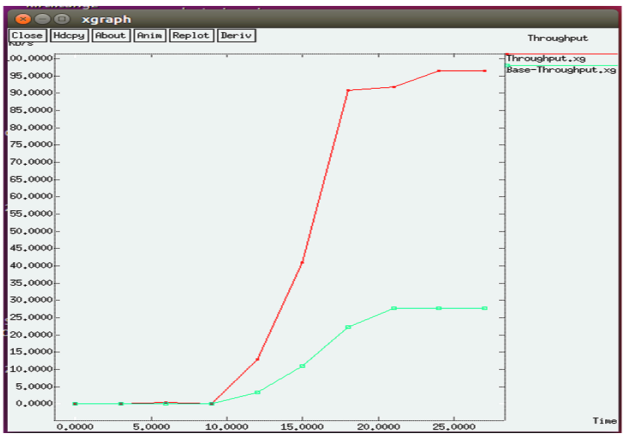


Fig. 4.3: Throughput with 170 nodes.

TIME(s)	0	4	8	12	16	20	24	81
BASE THROUGHPUT(kb/s)	0	0	0	0	4.4	12.9	24.18	37.64
NEW THROUGHPUT	0	0	0.3	0	15	45.9	92.92	90.88

Table 4.3: Throughput

The performance of the proposed work is evaluated by conducting the simulations for 170 nodes and on the basis of this simulation the parameters i.e. the packet delivery ratio, average delay, and throughput is evaluated. As MANETs faces various security challenges like interference that increases delays and also reduces the throughput of the network. So to overcome this problem secure routing based Bacteria foraging optimization and secure shared key mechanism using KNN is proposed that helps in accommodating the high network traffic rate and makes the network more secure and reliable.

V. CONCLUSION

The investigations of energy-efficient communication in wireless networks provide many future research directions. Thus, as a second future step, we aim at implementing each of the proposed solution and even their fusion over a real network test bed. , the secure and optimized framework is proposed to evaluate the BFO based routing protocol with an enhanced security mechanism using shared key mechanism. This framework combines the features of the Ant-hoc Net protocol, shared keys and KNN clustering. The main components of this framework are the cluster heads and the Certification authority. So, focus of this proposed work is to provide a secure environment in mobile ad hoc networks. In order to accommodate the high traffic rate in network the Limited member node based clustering is used that limits the numbers of nodes present in the cluster according to total number of nodes in the area. Further this technique can be implemented in fusion with other optimizing techniques.

VI. FUTURE SCOPE

In future proposed work can be utilized in the following. In future the proposed work will be extended to perform in dynamic environments.

The proposed routing algorithm may be utilized to design various WSN's, where in reliability, efficient use of energy, enhanced lifetime of the network, minimum end to end transmission delay are the QOS metrics for a particular applications.

There are many ways to extend this work. One of the most important is an analysis of more efficient routing techniques for both static and dynamic environment.

In second direction of future, the plan is to implement every proposed technique along with bio-inspired optimization techniques in a real environment. Network health monitoring can become a reality application of MANET

Wireless Sensor Networks is quite a rising and hot idea in wireless communication that is a lot of research is undergoing and numbers of issues are subjected to be investigating in this area. While, there are a lot of extra routing protocols that are need to be examine yet. Number of design issues like node deployment, heterogeneity, localization and synchronization that require being evaluating further and the protocols security that need to be explored by means of attacks nature to which wireless communication is taken as an appealing target.

REFERENCES

[1] D. K. Sharm et al," A Priority Based Message Forwarding Scheme for Opportunistic Networks", IEEE 2016
[2] V. Erramilli and M. Crovella," Forwarding in Opportunistic Networks with Resource Constraints", 2012.
[3] S.KIM," Effective Forwarding Scheme for Opportunistic Networks Based on Refined Contact Probability and Betweenness Centrality", Journal of Information Science and Engineering, 2016
[4] S. Kashp and J. Singh," Survey on Latest Routing Algorithms in Opportunistic Networks", International Journal of Science and Research (IJSR), 2014
[5] O. A. Mohamad and P. A. Tijare, "Performance Comparison of AODV, DSDV, OLSR and DSR Routing Protocols in Mobile Ad Hoc Networks", International Journal of Information Technology and Knowledge Management, Vol 2(2), pp. 545-548, 2015.
[6] S. J. Soni and P. Kanungo "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2Simulator", Procedia Engineering, Vol. 23, pp.229–234, 2015.
[7] C. Perkins and E. B. Royer, "Ad-hoc On-Demand Distance Vector (AOVD) Routing", IETF RFC 3561, 2015
[8] S. Gowrishankar and T.G. Basavaraju, "Scenario Based Performance Analysis of AODV and OLSR in Mobile Ad Hoc Networks", Special Issue of the International Journal of the Computer, Vol. 15(4), pp 8.1-8.6, 2015
[9] T. Clausen and P. Jacquet, "Optimized Link State Routing Protocol (OLSR)", IETF RFC 3626, 2015.
[10] S. Mohapatraa, and P. Kanungo, "Performance analysis of AODV, DSR, OLSR and DSDV Routing Protocols using NS2 Simulator", Procedia Engineering, Vol. 23, pp. 229–234, 2011
[11] S. Kumari and S. Maakar, "Traffic Pattern Based Performance Comparison of AODV, DSDV & OLSR MANET Routing Protocols using Freeway Mobility Model", (IJCSIT) Vol. 2 (4), pp. 1606-11611, 2015
[12] Bojan, S. ; Inst. Mihajlo Pupin, Univ. of Belgrade, Belgrade, Serbia ; Nikola, Z., "Genetic algorithm as energy optimization method in WSN", IEEE, pp.97-100, 2013.
[13] C. Alippi and G. Vanini. "Application-based routing optimization in static/semi-staticWireless Sensor Networks", IEEE, pages 47-51, 2006.
[14] Chunyao FU, Zhifang JIANG1, Wei WEI2and Ang WEI, "An Energy Balanced Algorithm of LEACH Protocol in WSN", IJCSI, Vol.10, pp.354-359, 2013.
[15] C. Intanagonwiwat, R. Govindan, and D. Estrin, "Directed diffusion: a scalable and robust communication paradigm for sensor networks", Proceedings of MobiCom'00, pp. 56–67, Boston, MA, USA, August2000.

