International Journal of Engineering Research & Management Technology

ISSN: 2348-4039

May-June-2019 Volume 6, Issue-3

Email: editor@ijermt.org www.ijermt.org

CONSIDERED PLAN AND DEVELOPMENT OF ANONYMOUS LOCATION BASED ROUTING FOR MOBILE AD-HOC NETWORK

Vikram Singh,
Research Scholar, Dept. of Computer Application,
Himalayan Garhwal University

Dr. Poornima Tyagi,
Associate Professor, Dept. of Computer Application,
Himalayan Garhwal University

Abstract

Mobile ad-hoc network (MANET) is a decentralized radio communication involving several small sensors communicating spontaneously through the air. The topology of the network keeps on varying due to the changing nature of its sensors. The Security and safety issue starts because of self-configuration and self-supporting features. In MANET the basic routing technique is through a pair of nodes that behaves like an isolated node of channel for a specific route with different zones/sectors to manage network activity. Military and rescue operations are one of the highly sensitive applications of MANET wherein identifying the secure node and secure routing for data transmission is one of the important task, so coming up with a secure location-based routing with optimization is one of the major challenge. This paper gives a detailed case study of Anonymous Location Based Routing for MANET and compares with the exiting methods, which proves proposed method provides better performance

Key words : *Mobile ad-hoc network, routing technique, activity*

Introduction

The first generation of ad-hoc network began in 1972 wherein it was called as PRNET- (Packet Radio Network) and were used in Military application. The second generation began around 1980 where the ad-hoc network systems were further improved and developed into Survivable Adaptive Radio Networks (SURAN) program. After few decades particularly in 1990's where mobility and wireless network achieved popularity. As the mobile devices (MDs) and wireless networks became increasingly popular, wireless ad-hoc networks became highly usable and important fields of network infrastructure. Two types of MANETs are there like infrastructure networks and mobile wireless network. MANET can also be called as infrastructure less mobile network.

New strategy and advancement in anonymous location-based routing for MANET represent the protocol's technical capabilities to prospective implementation and influence expectations according to node's capabilities and constraints. It is required to determine routing requirements and provide designs for complex routing algorithms. The algorithm is used to resolve technical blockers for anonymous location-based routing. The work involves hands-on NS2 simulation to demonstrate and simulate targeted MANET environments including nodes and the coordination of additional technical resources. The outcome of the research is to recommend anonymous location-enabled route strategies, sectors, platforms, and application infrastructure required to successfully implement the proposed solution using MANETs best practices. The experimental process and outcome of the simulation are detailed in this paper.

Method

The proposed Strong Secure Anonymous Location Based Routing (S^{2}ALBR) method is focused mainly on the optimizing the uses of resource and getting the good performance. In any MANET applications having the good performance with less use of resource one of mail task which directly effects to lifetime process. So the proposed method is focuses on optimization technique.

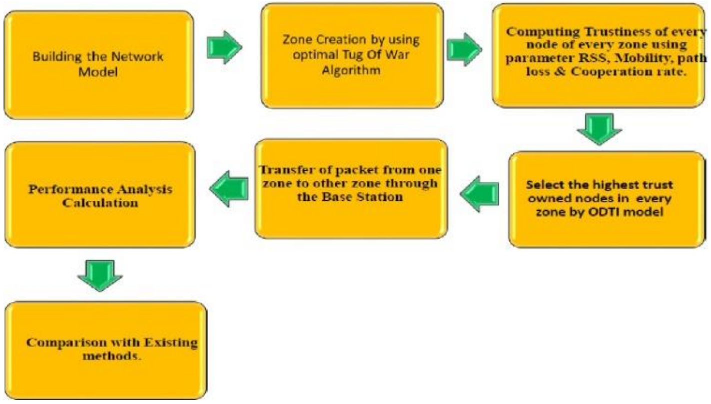

Building the Network Model
Zone Creation by using optimal Tug Of War Algorithm
Computing Trustiness of every node of every zone using parameter RSS, Mobility, path loss & Cooperation rate.
Select the highest trust owned nodes in every zone by ODTI model
Transfer of packet from one zone to other zone through the Base Station
Performance Analysis Calculation
Comparison with Existing methods.

Fig.-1 : Flow Diagram of S^{2}ALBR

Figure 1 shows Flow Diagram of S^{2}ALBR. The proposed method is using optimal partitioning and trust inference model. S^{2}ALBR method involves following steps:

Building of network model

The network model is created for 50,100,150,200 & 250 nodes. Nodes are deployed randomly in a network area of 1000m × 1000m.

Creation of Cluster

Partitioning a network into the cluster with the help of OTW algorithm, after partitioning into cluster it will calculate the trustiness of each node with the help of Optimal trust inference model (ODTI).The trustiness is considered based on strong network parameters such as RSS, mobility, path loss, and cooperation rate

Selection of Cluster head node in each zone

Once after getting the trust of every node, the maximum trusted owned node is selected as cluster head in each zone.

Transmission of packets

The packet will be transmitted from one cluster to other clusters through the help of a cluster header; Nodes will communicate to each other with Intra and intercommunication.

Performance Analysis

Network performance is measured by its network parameters. In the evolution of the network performance majorly considered parameters are energy, delay, network lifetime, and throughput.

Comparison of performance with existing method

The proposed method is compared with existing method to prove that the proposed method is having a better performance.

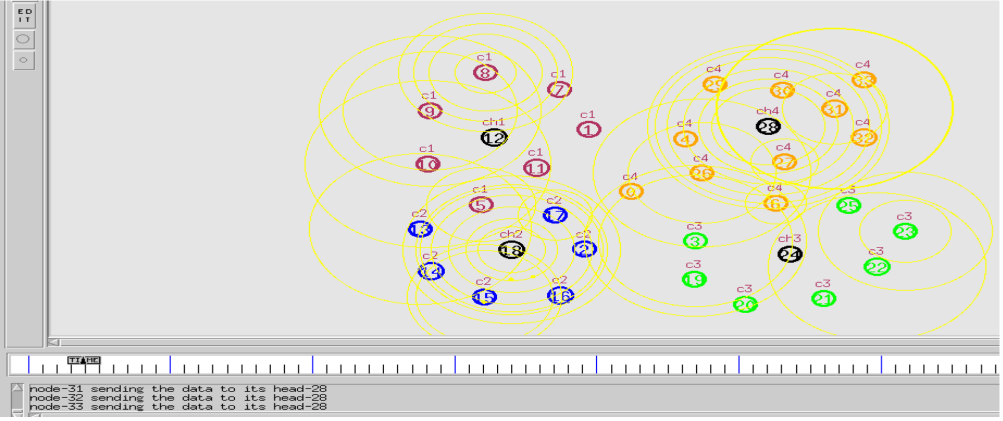
Objective of proposed method:

- To provide secure communication between mobile nodes.
- To reduce or minimize parameters namely delay and power utilization of nodes.
- To progress or maximize the throughput and MANET lifetime compared to available protocols.
- Comparing the performance with the popular methods like ALERT, ALARM, and AASR.

Experimental Setup

The routing network has been established by selecting a secure trustable node with a high trust degree known as cluster head and this selected cluster head was responsible to transmit data in each sector.

Figure 1.2 shows the routing model in the NS2 simulation environment. Each color of the node represents a different cluster. Nodes circled in black color represent the Cluster header (CH), the routing will take place between the clusters for transmission of the packet.



```
node-31 sending the data to its head-28
node-32 sending the data to its head-28
node-33 sending the data to its head-28
```

Fig.-2: Routing in Proposed model

Figure 2 shows the routing model in the NS2 simulation environment. Each color of nodes represents different sectors. Black nodes represent the CH.

Result and Discussion

Efficiency of suggested S^{2}ALBRmethod is accomplished with the following methods:

Performance-based on nodes quantity.

The performance has been considered by varying nodes in a network model; the network model is created for - 50, 100, 150, 200 & 250 nodes. In this research paper Performance analysis, Energy Consumption, Delay, Network lifetime, and through put parameter is considered.

Energy consumption indicates- how much energy the node is used for transmission of data. Figure 3 shows Energy consumption graph of S^{2}ALBR method for node of 50,100,150,200 & 250. The graph shows the energy consumption of nodes in joules(j)or new ton meter(nm).

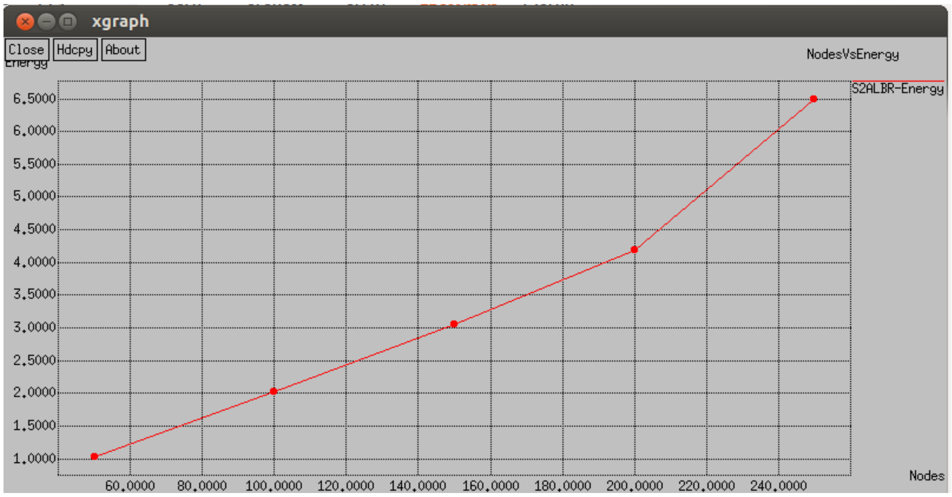


Fig.-3: Energy consumption graph of S^{2}ALBR method w.r.t nodes

Delay indicates the how long time node is interrupted to transferred the data from one node to another. Figure 4 represent Delay graphofS^2 ALBR method for nodes 50, 100, 150, 200 &
250.The graph shows a delay in communication between nodes in milliseconds (ms).

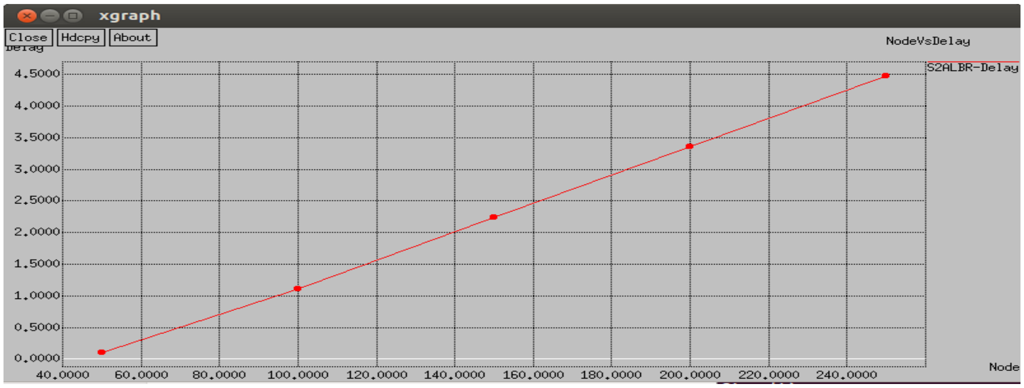


Fig.-4: Delay graph of S^{2}ALBR method w.r.t nodes

Network lifetime indicates how much nodes are alive in a network for the process. Figure 5 shows the Network lifetime graph of S^{2}ALBR method for the nodes 50,100,150, 200 & 250. The graph shows an increase in Network lifetime in comparison to node count. The network lifetime unit is represented in seconds.

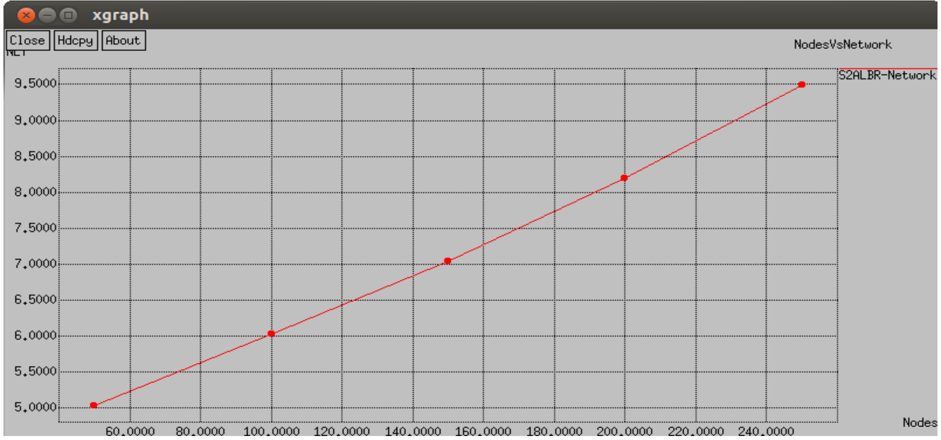


Fig.-5: Network life time graph of S^{2}ALBR method w.r.t nodes

Throughput is measured by number of packets transferred per second. Figure 6 shows throughput graph of S^{2}ALBR method for the node of 50,100,150,200 & 250. The graph shows an increase in throughput with respect to number of nodes;

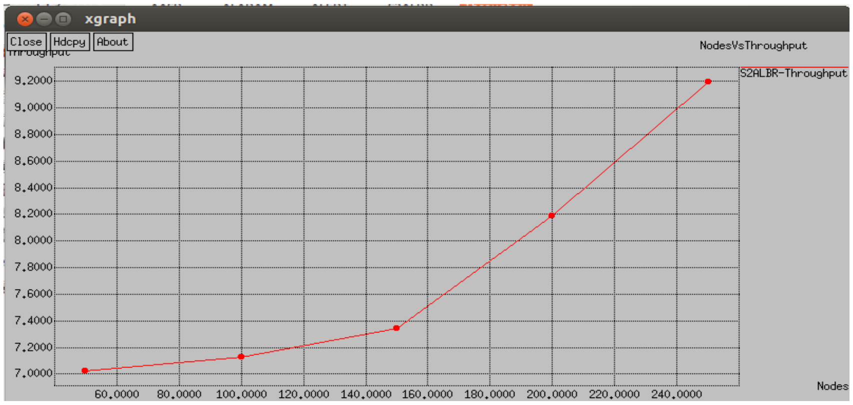


Fig.-6: Through put graph of S^{2}ALBR method w.r.t nodes

Performance-based on threat quantity.

The performance is considered by improving the count of attackers in the MANET model like- 5, 10, 15, 20 & 21. Figure 7 depicts the energy consumption graph of the S^{2}ALBR method compared to attackers. There are 1.10.15, 20 & 25 attackers with node of 50,100,150, 200 & 250. The graph shows the energy consumption of node w.r.t to attackers in joules (j) or newton meter (nm)

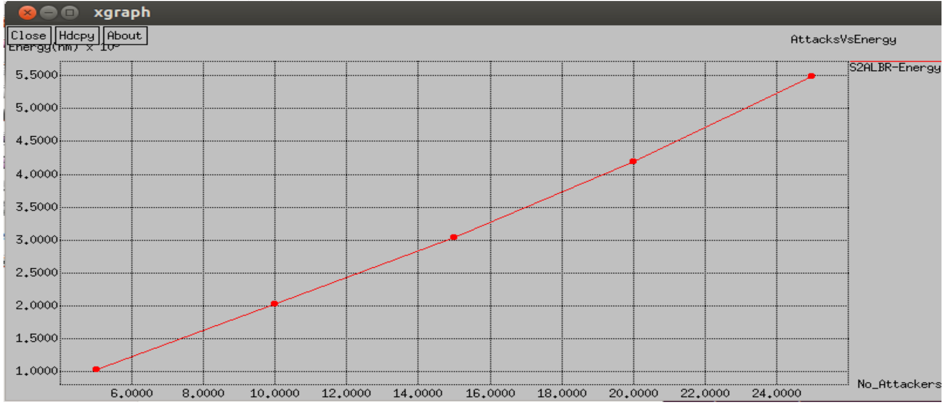


Fig.-7: Energy consumption graph of S^{2}ALBR method w.r.t attack

They are 1.10.15, 20 & 25 attackers with node of 50,100,150, 200 & 250. The graph shows a delay in communication between the node w.r.t to attackers in milliseconds (ms) as shown in figure 8 Delay graph of the S^{2}ALBR method w.r.t to attackers.

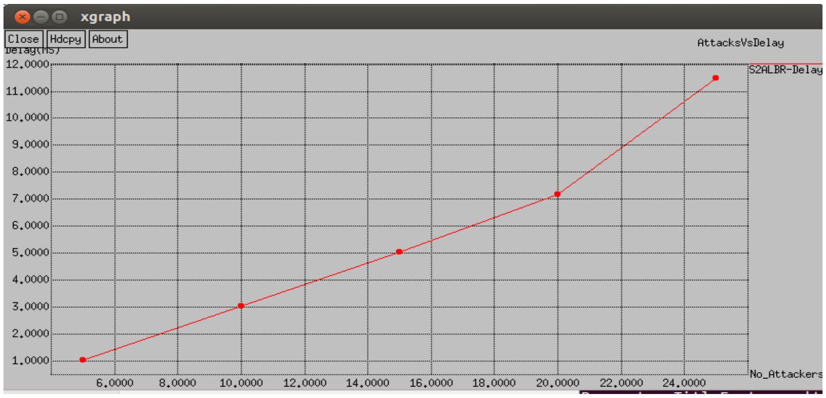


Fig.-8: Delay graph of S^{2}ALBR method w.r.t attack

There are 1.10.15, 20 & 25 attackers with node of 50,100,150, 200 & 250. The graph shows Network lifetime is increased with respect to attacker nodes as shown in figure 9 Network lifetime graph of the S^{2}ALBR method w.r.t to attackers.

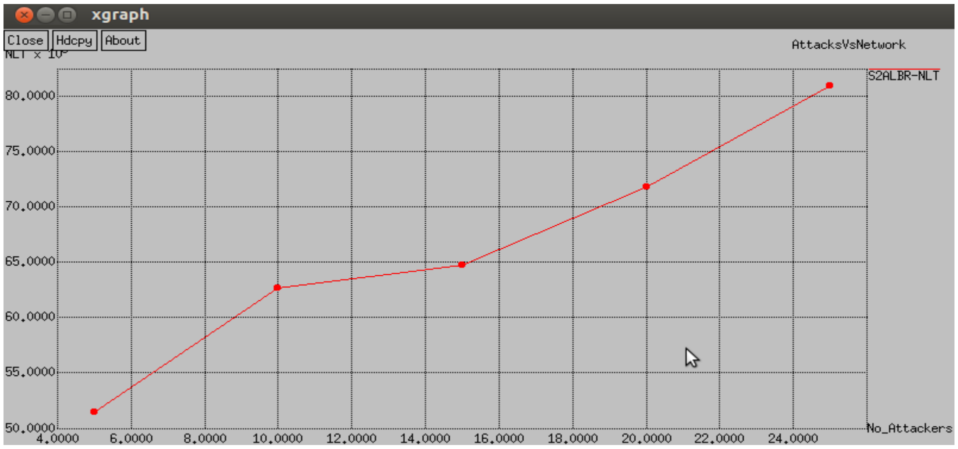


Fig.-9 : Network life time graph of S^{2}ALBR method w.r.t attack

There are 10, 15, 20 & 25 attackers with node of 50,100,150, 200 & 250. The graph shows throughput is increased with respect to the number of attackers also as shown in figure 10 Throughput graph of the S^{2}ALBR method w.r.t to attackers

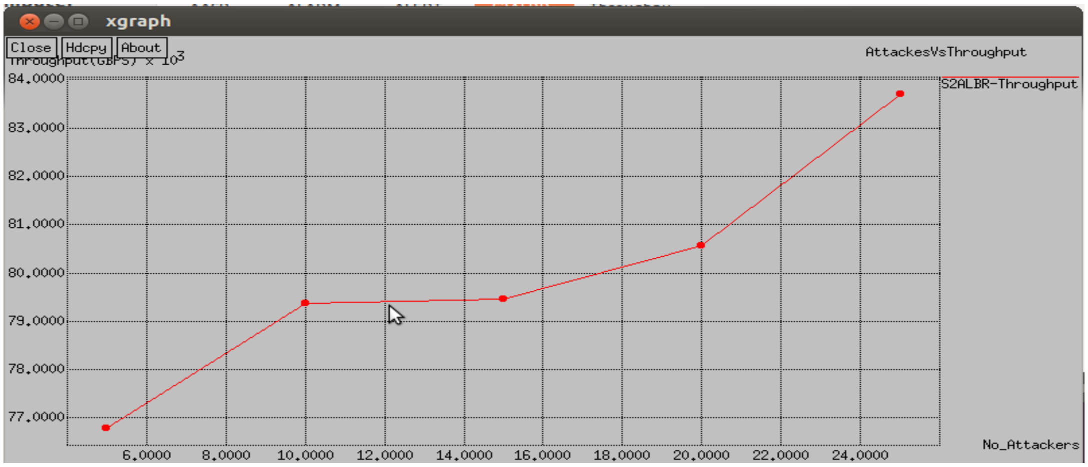


Fig.-10: Through put graph of S^{2}ALBR method w.r.t attack

Comparison

Comparison of S^{2}ALBR with ALERT, ALARM, and AASR is done again by nodes count and attackers count compared to the same parameters as considered above.

Comparison-Number of nodes

Energy consumption of the proposed S^{2}ALBR (Red color) method is 21.3% lower than ALERT (Green color), 29.42% lower than ALARM (Blue color), and 31.09% lower than AASR (Yellow color)as shown in figure 11 node count vs Energy for 50 to 250 nodes

p

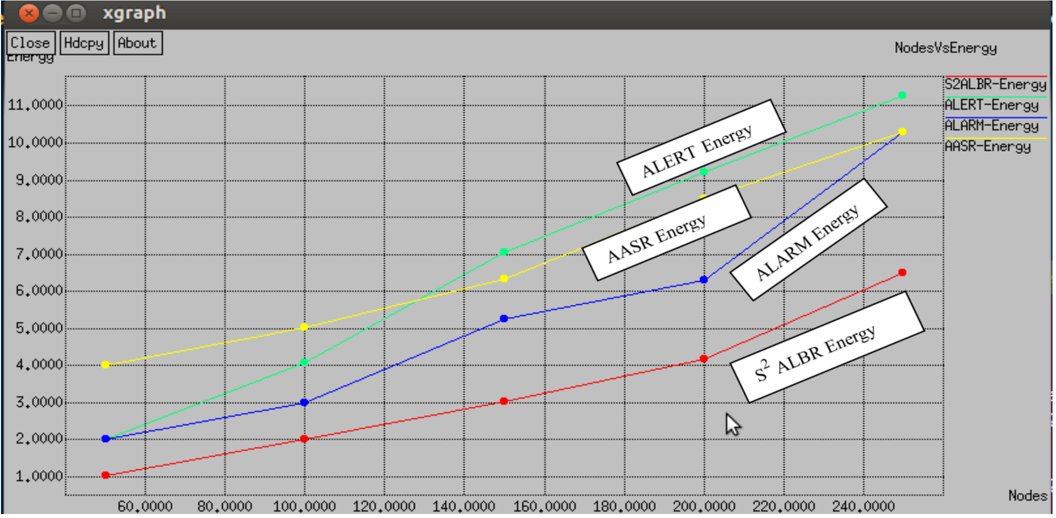


Fig.-11 : Nodes count vs Energy

Delay of proposed S^{2}ALBR method is 11.2% lower than ALERT, 7.1% lower than ALARM, and 14.5% lower than AASR as illustrates figure 12 number of nodes vs. delay for 50 to250 nodes.

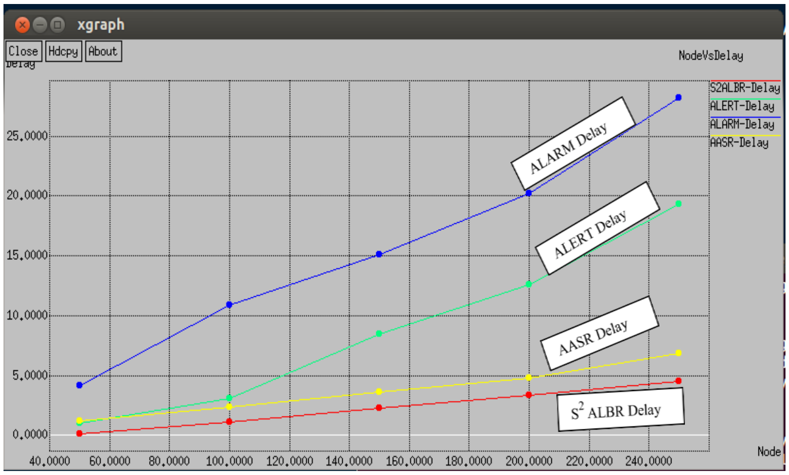


Fig.-12 : Node's count vs Delay

S2ALBR method is used for the selection of a strong secure trusted node in each sector and this trusted node is responsible for communication between the intermediate nodes. The main intention of proposal is reducing network parameters like delay, energy consumption, and maximize throughput, network lifetime in-network, and the said method S2ALBR is checked with the existing techniques ALERT, ALARM and AASR. By this clearly we can state proposed method is the better one. Current state of MANET demands parameter optimization and this investigation will be helpful in contributing in this direction

Conclusion

An innovative protocol for secured location-enabled routing for MANET using soft computing methods is the objective of the current dissertation. Key requirements of research are to identify issues like secured node, equal distribution of node in each cluster to manage the density of the network, secure transmission, communicating with nodes regarding coverage, routes, node relationships by managing CH with sinks and getting the good performance of the network. The Challenges will be technically complex and ethically threatening situations as requiring the highest level of optimal path selection.

The ideal approach is tousetheNS2 simulation environment effectively for resolving routing problems. It is difficult to do actual experiments Learning new algorithms such as OTW and collaborating to find solutions while demonstrating complex network models, continuously optimizing and improving the routing experience.

The aim of the current research is to show the capability of the proposed algorithms and compare them with popular methods. Prior experience with MANET, understanding of mobile networking concepts such as CH, Sink, node, and the packet have helped to propose the new S^{2}ALBR method. The proposed algorithm is found to be far more efficient than the published algorithms compared. S^{2}ALBR method for MANET using efficient partition for a zone and degree of trust model involves partitioning a MANET into zones using OTW algorithm. Subsequently computing the node's trustiness using the parameters such as transmission signal strength, mobility, path loss, and cooperation rate. Further, trust assessment is enhanced thru ODTI model to get trustiness of each mobile node.

Finally finding most trust-owned node for a zone considering the adjacent relay nodes for data transmission which represent anon-traceable anonymous route. S^{2}ALBR method is used for the selection of a strong secure trusted node. The objective is reducing network parameter energy, delay, and maximize throughput, network lifetime. In comparison to popular techniques such as ALERT, ALARM, and AASR the developed method has shown better-improved performance. This S^{2}ALBR method will pave the way for many innovative applications involving MANET.

The developed method is evaluated in two ways, first one by increasing number of nodes, the proposed method has minimized the delay by 11%, energy by 27%, maximized network lifetime by 27%, and throughput by 36%.

Secondly with an increasing number of attackers proposed method has minimized the delay by 36%, energy by 33% and maximized network lifetime by 42% and throughput by 33%. Thus, from above-mentioned results it clearly indicates proposed method has better performance.

With the published results and encouraging comparison parameters, the objective to develop "Novel Approach to Secure Location-Based Routing for MANET Using Soft Computing Methods" is successful. This is an innovative attempt towards making MANENT more self- reliant, less power-consuming, and easy to implement.

References

- Darren Hurley-Smith, Jodie Wetherell, Andrew Adekunle," SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad-hoc Networks" IEEE Transactions on Mobile Computing, Volume: 16, Issue: 10, 2014
- G. Pavani, and R. Tinini, "Distributed meta-scheduling in lambda grids by means of Ant Colony Optimization," Future Generation Computer Systems-The International Journal of Escience, vol. 63, no. 10, pp. 15-25, October 2015
- Kapur, R. K., & Khatri, S. K., "Analysis of attacks on routing protocols in MANETs", In Computer Engineering and Applications (ICACEA), 2015 International Conference on Advances in (pp. 791-798). IEEE, 2011.
- Lalar S, Yadav A. K. Comparative Study of Routing Protocols in MANET. Orient.J. Comp. Sci. and Technol;10(1) ISSN: 0974-6471, Vol. 10, No. (1): Pgs. 174-179, March 2014, http://dx.doi.org/10.13005/ojcst/10.01.23
- Mingchuan Zhang, Meiyi Yang, Qingtao Wu, Ruijuan Zheng, and Junlong Zhu, "Smart Perception and Autonomic Optimization: A Novel Bio-inspired Hybrid Routing Protocol for MANETs" Future Generation Computer Systems, Volume 81, Pages 505-513, 2014
- Remya S and Lakshmi K S, "SHARP: Secured Hierarchical Anonymous Routing Protocol for MANETs", Proc. Intl Conf. Computer Communication and Informatics (ICCCI), 2015
- Salwa Othmen, Faouzi Zarai, Aymen Belghith, Lotfi Kamoun, "Anonymous and Secure On-Demand Routing Protocol for Multihop Cellular Networks", Networks, Computers and Communications (ISNCC), 2015
- Swetha M S, Thungamani M and Pushpa S K (2012). "A Novel Approach To Secure Location Based Routing For Manet Using Soft Computing Methods", Ph.D., Computer Science and Engineering, VTU, Bengaluru.
- Tarunpreet Bhatia, A.K. Verma,"QoS Comparison of MANET Routing Protocols", IJCNIS, vol.7, no.9, pp. 64-73, 2011.DOI: 10.5815/ijcnis.2011.09.08
- Uma Rathore Bhatt ,NeeleshNema, RakshaUpadhyay," Enhanced DSR: An Efficient Routing Protocol for MANET", Issues and Challenges in Intelligent Computing Techniques (ICICT), 2014
- Vadhana Kumari, S., & Paramasivan, B. (2015). Defense against Sybil attacks and authentication for anonymous location-based routing in MANET. Wireless Networks, 23(3), 715–726. doi:10.1007/s11276-015-1178-7