OPEN ACCESS
Computer Science & IT Research Journal
Volume 1, Issue 1, P.7-14, March, 2020
Fair East Publishers
Journal Homepage: www.fepbl.com/index.php/csitrj

FEP

# PROPOSED CLUSTER BASED ALGORITHM FOR MOBILE AD HOC NETWORK

Chen Chao[1], Liang Jun[2], Sun Xin[3]
[1,2,3] Department of Computer Science and Technology, Tsinghua University, China

*Corresponding Author: Chen Chao

**Article Received:** 15-10-19 **Accepted:** 17-02-20 **Published:** 30-03-20

## ABSTRACT

Mobile ad hoc networks use the wireless network and have wider applications especially in emergency situation, military combat zones, and the mobility vehicles. The mobile ad hoc network especially poses the problem of security and efficiency as the network is often subject to internal and external attacks. To overcome such problems, different protocols are proposed. In this study, an improved protocol is proposed which makes use of hexacol cluster method and thus provide greater efficiency and security to the network. For validating the proposed method, a stimulation was performed and results were compared with other protocols. The results indicate that the proposed method showed improved performance compare to the other protocol.

**Keywords:** Mobile Networks, Cluster, Transmission, Protocol.

## INTRODUCTION

Mobile ad hoc network refers to the mobile devices which are connected to a single network and communicating with each other (Tseng, Ni, Chen, & Sheu, 2002). These networks are without wire and that’s why called mobile. Mobile ad hoc network (MANET) is a wireless network which is based on wireless infrastructure and thus have no fixed infrastructure. The application of the Mobile ad hoc network includes military settings, e-learning systems, road traffic information sent to other vehicles and so on (Singh, Woo, & Raghavendra, 1998). There are several other applications of these Mobile ad hoc network; however, because it does not base on any centralized control system, so the network is also subject to the security threats. Mostly, Mobile ad hoc network is more vulnerable to the security attacks. The attacks are occurred by malicious nodes in the system which can be external or internal (Taha, Alsaqour, Uddin, Abdelhaq, & Saba, 2017). An attacker can insert a malicious node in the network which can be used to monitor the communication between nodes or even withholding some information, changing data, stealing data, and blocking the performance of the entire network. For managing resources, in mobile ad hoc network, a cluster is developed which is a set of computers interlinked (Desai, Chong, Achilles, Daijavad, & La Porta, 2019). The clusters depend on the nodes radio range. Thus, cluster-based communication is common in Mobile ad hoc network. The cluster-based communication enables the Mobile ad hoc network to perform the work with less delays and efficient energy consumption.

If the Mobile ad hoc network is based on pure system, it creates problem of trust management for the central control. Calculations of trust for different levels is a main problem in Mobile ad hoc network (Singh, et al., 1998**).** A proposed method to overcome such problem is the Dempster-Shafer theory. The theory suggests making use of range of possibilities instead of single number of probabilities. By using the Bayesian theory, mass function can be achieved. The posterior probability gets changes because of the evidence obtained from the environment.

The Mobile ad hoc network can be used in situations such as emergency relief, battlefield, and even in normal civilian settings. In emergency situation in particular, the Mobile ad hoc network can be useful since the actual communication infrastructure is destroyed by the natural calamity. The battlefields also pose its own challenges of communication and Mobile ad hoc network can be used to overcome such challenges.

In Mobile ad hoc network, the trust means the nodes can have trust on neighboring nodes for sending the data packet. In Mobile ad hoc network, presence of such trust result in higher level of timeliness, reliability, and integrity of passing message to the next-hop node. The objective of higher security in Mobile ad hoc network can be achieved by using the continuous detection and authentication system (Nesargi & Prakash, 2002). Thus, trust management plays its role by creating a secure and reliable Mobile ad hoc network.

In Mobile ad hoc network, clustering mechanism is used which help in improving the network security and the energy consumption. Study by Raza, Aftab, Akbar, Ashraf, and Irfan (2016) proposed a hexagonal clustering where WSN are made up of hexagonal clusters. A cluster head is located in each cluster. The current study proposed that by making several sub-divisions, clusters energy consumption can be reduced. Accordingly, the trust can also be improved using the WSN energy efficiency. Tseng, et al., (2002) proposes a centralized competence and trust-based energy efficient routing scheme. The TRACE provide security against several type of attacks within the Mobile ad hoc network. The WSN contains sink or BS which are more powerful and knowledgeable for maintenance of trust and reliability. Topology control and routing is another perspective of energy efficiency in WSN. Desai, et al., 2019 provides a framework which ensure efficient energy consumption in terms of end-to-end data transmission delays, number of hops, and transmission delays.

Taha, et al., (2017) proposes another energy efficient routing protocol based on end-to-end localized routing and considered as highly efficient in terms of number of packets delivered.

One factor related to the transmission in the Mobile ad hoc network is the number of throughputs which can be increased to improve the network reliability but it also comes with the cost of higher energy consumption (Borkar & Mahajan, 2017). For efficient data transmission, bit error rate (BER) also plays important role as it can influence the throughput. The importance of energy efficient clustering techniques is that these techniques can be used to improve the system life and efficiency (Elhoseny & Shankar, 2019). Balancing the requirement of network energy efficiency and the reliability is a challenge. Sarkohaki, Fotohi, & Ashrafian (2020) proposed a framework which seems to be better balancing these two conflicting demands. For better energy consumption and improved reliability, an algorithm is proposed. Another proposed methodology aims to balance the conflicting demands of availability, scalability, reconfigurability, and reliability by Ahmed (2020).

For trust management, computation trust from different levels in the network become very cumbersome process (Rath, Pattanayak, & Pati, 2017). Thus, it is recommended that the trust management function should be less dependent on central authority. Use of some suitable protocol and encryption technique can help in achieving the desired level of trust and security in the Mobile ad hoc network. A decentralized trust management which makes use of nodes instead of central authority is proposed by (Marchang, Datta, & Das, 2016). In this study, the hexagonal clustering and trust management is combined for developing mechanism of efficient and trust-based network.

## PROPOSED SYSTEM ARCHITECTURE

The study proposes a trust-based algorithm which detect colluding nodes and thus defends against internal attacks made by the colluding nodes. The proposed algorithm is making use of the cluster technique and provide route detection and forward node selection process, and enable computation of trust. The cluster has routing protocol which perform trust computation, route selection, and forward node selection process. The trust computation is about calculating trust for each node; while, route detection performs the function of identifying the optimum route for packet delivery.

### Cluster Formation

The proposed application aims to improve the overall throughput of the network, and decrease energy consumption and transmission delays. Security wise, the proposed application also includes the colluding nodes detection and prevention of internal attacks. In Mobile ad hoc network, broadcast storm problem can occur. The cluster head is forwarded with the data packet by forward nodes. In situation, when there is no destination ID, the cluster head’s own covered nodes discard such message. By creating an efficient cluster, broadcasting problems can be avoided and become more energy efficient. The cluster formation procedure dictates other tasks such as trust computation, forward node selection and route detection. The hexagonal cluster makes the network more efficient and consumes less energy. The higher efficiency and reliability in hexagonal cluster is achieved since nodes are closer in the network which reduce the distance and required energy to convey the data.

### Computing Trust

For computing trust, common methods are Eigen method and the Bayesian method. The Bayesian model works on calculating trust based on collection of reputation. Because of local nature, the data storage requirement is also low in the Bayesian method. On the other hand, the Eigen method is used for computing the normalized local trust which is used for performing aggregation for obtaining global trust values. This Eigen method is more rigorous since it reduces the chances of presence of malicious nodes in the network. The limitations of the Eigen method can also be overcome by using the Dempster Rule which ignores the conflicting evidence by normalizing multiple sources. The success and failure of every node is done using the Dempster-Shafers combination rule which calculate the trust values which are stored in the nodes. The global trust value of a node which moved from other cluster can be obtained from its previous cluster head.

Forward node refers to a cluster head one hop neighbor node. The forward nodes are used in the cluster for routing purpose. Gateway nodes are utilized for routing between the clusters. Cluster heads perform the data broadcasting. The procedure is such that when a cluster head receives a packet, it forwards the packet to one hop forward node based on its destination. In case of data transmission by a node, the cluster is first receiving the packet which is broadcasted to forward nodes. If destination id is not found, the path is discarded. The neighbor set the forward set is used for obtaining the routing information from the forwarding nodes and the cluster head. Routing detection plays important role in performing certain important tasks such as efficiency management, trust value assessment, and the clustering mechanism. Computation of trust is made by the cluster head and the forwarding nodes.

## EXPERIMENT RESULTS

The proposed method is used for creating a stimulation which was used for comparing the results with RTSR and ADOV. The results are as follows;

### Throughput

The results of the throughput for the proposed method in comparison to the RTSR and AODV is as follows.

**Table 1: Throughput**

| Time (M) | Proposed Method | RTSR | AODV |
|---|---|---|---|
| 10 | 67 | 55 | 35 |
| 20 | 78 | 111 | 129 |
| 30 | 123 | 131 | 143 |
| 40 | 234 | 220 | 211 |
| 50 | 289 | 279 | 223 |
| 60 | 358 | 334 | 331 |
| 70 | 459 | 451 | 401 |
| 80 | 511 | 491 | 478 |
| 90 | 599 | 543 | 552 |
| 100 | 671 | 634 | 598 |

| | | | |
|---|---|---|---|
| 110 | 683 | 654 | 635 |
| 120 | 745 | 711 | 681 |

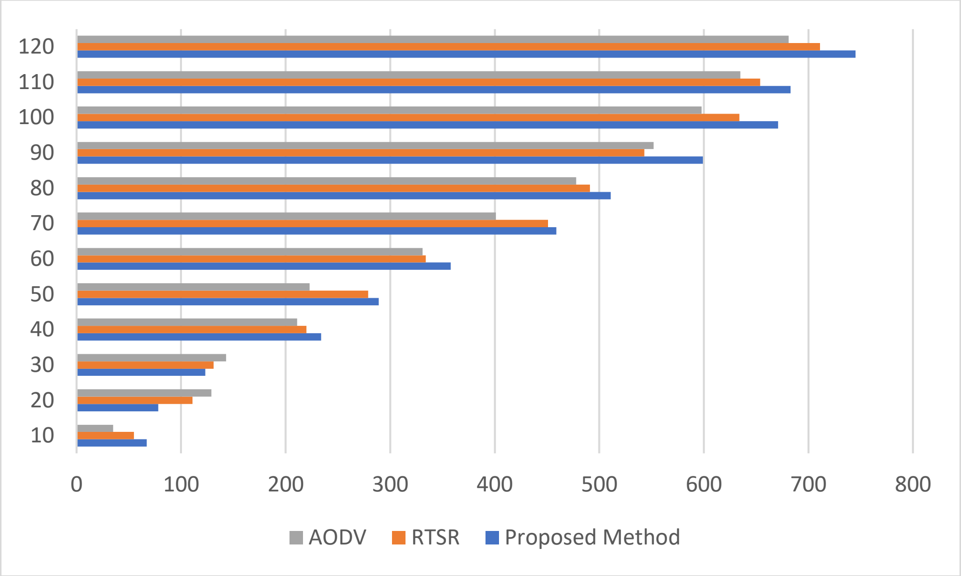

**Figure 1: Throughput Comparison**

The results show that at 10 minutes time interval, the throughput was 67 for proposed method; 55 for RTSR; and 35 for AODV. At 20 minutes time interval, the throughput was 78 for proposed method; 111 for RTSR; and 129 for AODV. At 30 minutes time interval, the throughput was 123 for proposed method; 131 for RTSR; and 143 for AODV. At 40 minutes time interval, the throughput was 234 for proposed method; 220 for RTSR; and 211 for AODV. At 50 minutes time interval, the throughput was 289 for proposed method; 279 for RTSR; and 223 for AODV. At 60 minutes time interval, the throughput was 358 for proposed method; 334 for RTSR; and 331 for AODV. At 70 minutes time interval, the throughput was 459 for proposed method; 451 for RTSR; and 401 for AODV. At 80 minutes time interval, the throughput was 511 for proposed method; 491 for RTSR; and 478 for AODV. At 90 minutes time interval, the throughput was 599 for proposed method; 543 for RTSR; and 552 for AODV. At 100 minutes time interval, the throughput was 671 for proposed method; 634 for RTSR; and 598 for AODV. At 110 minutes time interval, the throughput was 683 for proposed method; 654 for RTSR; and 635 for AODV. At 120 minutes time interval, the throughput was 745 for proposed method; 711for RTSR; and 681 for AODV.

**Table 2: Packet Delivery Rate**

| Time (M) | Proposed Method | RTSR | AODV |
|---|---|---|---|
| 10 | 0.1 | 0.2 | 0.2 |
| 20 | 0.3 | 0.3 | 0.3 |
| 30 | 0.4 | 0.4 | 0.4 |
| 40 | 0.5 | 0.4 | 0.4 |
| 50 | 0.7 | 0.6 | 0.5 |
| 60 | 0.9 | 0.8 | 0.8 |
| 70 | 1.2 | 1.2 | 1 |

| | | | |
|---|---|---|---|
| 80 | 1.9 | 1.7 | 1.3 |
| 90 | 2.3 | 2.1 | 1.6 |
| 100 | 2.4 | 2.3 | 1.7 |
| 110 | 2.6 | 2.5 | 1.9 |
| 120 | 3 | 2.8 | 2.1 |

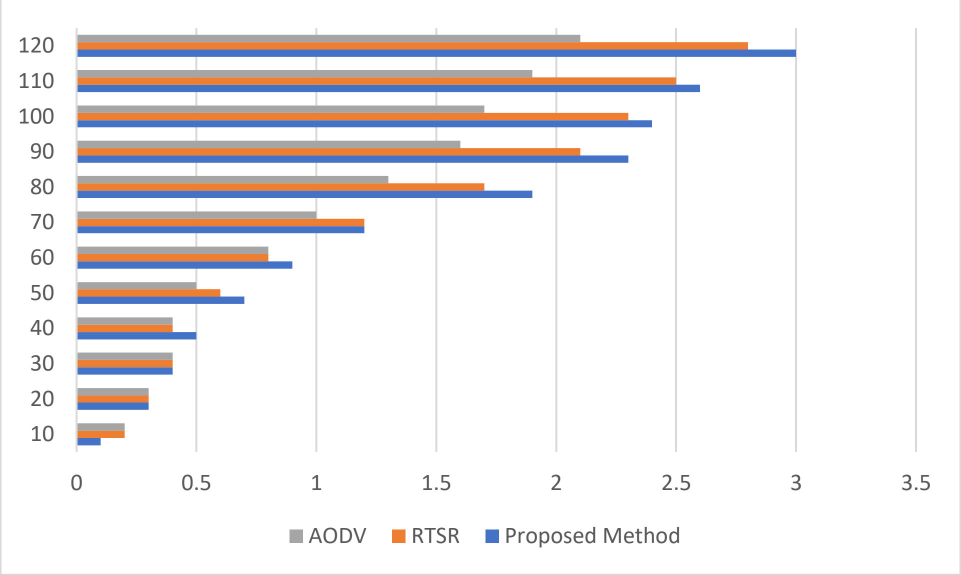

**Figure 2: Packet Delivery Comparison**

The results of packet delivery rate are provided above. At 10 m, the packet delivery rate is 0.1 for proposed method; 0.2 for RTSR; and 0.2 for AODV. At 20 m, the packet delivery rate is 0.3 for proposed method; 0.3 for RTSR; and 0.3 for AODV. At 30 m, the packet delivery rate is 0.4 for proposed method; 0.4 for RTSR; and 0.4 for AODV. At 40 m, the packet delivery rate is 0.5 for proposed method; 0.4 for RTSR; and 0.4 for AODV. At 50 m, the packet delivery rate is 0.7 for proposed method; 0.6 for RTSR; and 0.5 for AODV. At 60 m, the packet delivery rate is 0.9 for proposed method; 0.8 for RTSR; and 0.8 for AODV. At 70 m, the packet delivery rate is 1.2 for proposed method; 1.2 for RTSR; and 1 for AODV. At 80 m, the packet delivery rate is 1.9 for proposed method; 1.7 for RTSR; and 1.3 for AODV. At 90 m, the packet delivery rate is 2.3 for proposed method; 2.1 for RTSR; and 1.6 for AODV. At 100 m, the packet delivery rate is 2.4 for proposed method; 2.3 for RTSR; and 1.7 for AODV. At 110 m, the packet delivery rate is 2.6 for proposed method; 2.5 for RTSR; and 1.9 for AODV. At 120 m, the packet delivery rate is 3 for proposed method; 2.8 for RTSR; and 2.1 for AODV.

**Table 3: End-to-End Delay**

| Time (M) | Proposed Method | RTSR | AODV |
|---|---|---|---|
| 10 | 0 | 0 | 0 |
| 20 | 10 | 8 | 12 |
| 30 | 13 | 12 | 16 |
| 40 | 17 | 18 | 28 |
| 50 | 19 | 28 | 31 |
| 60 | 25 | 31 | 36 |

| | | | |
|---|---|---|---|
| 70 | 33 | 39 | 47 |
| 80 | 41 | 47 | 51 |
| 90 | 49 | 53 | 61 |
| 100 | 58 | 61 | 69 |
| 110 | 61 | 68 | 73 |
| 120 | 73 | 79 | 85 |

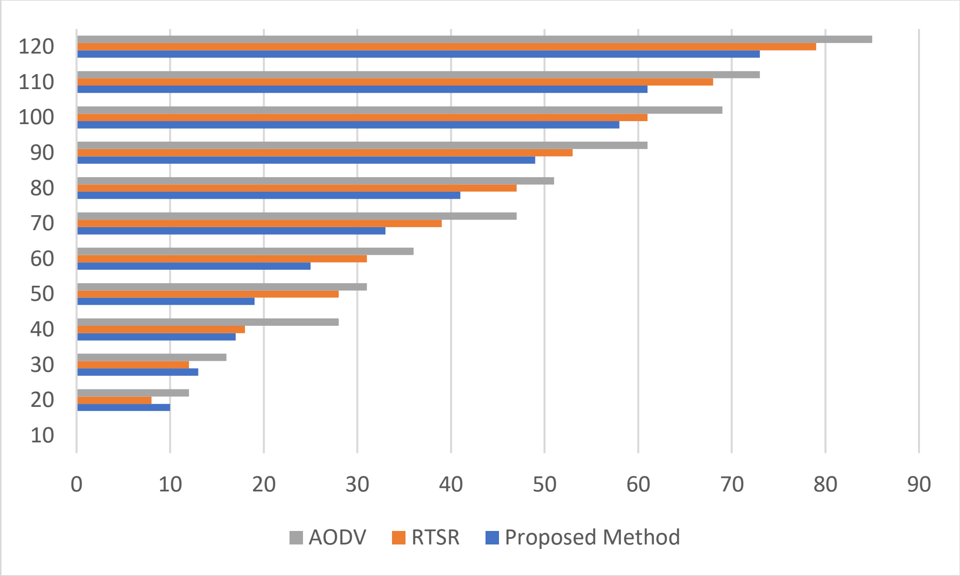

**Figure 3: End-to-End Delay Comparison**

The results for end-to-end delay are provided above. For 10m, the delay for end-to-end is 0 for proposed method is; 0 for RTSR; and 0 for AODV. At 20 m, the end-to-end delay is 10 for proposed method is; 8 for RTSR; and 12 for AODV. For 30 m, the end-to-end delay is 13 for proposed method is; 12 for RTSR; and 16 for AODV. For 40 m, the end-to-end delay is 17 for proposed method is; 18 for RTSR; and 28 for AODV. At 50 m, the end-to-end delay is 19 for proposed method is; 28 for RTSR; and 31 for AODV. At 60 m, the end-to-end delay is 25 for proposed method is; 31 for RTSR; and 36 for AODV. At 70 m, the end-to-end delay is 33 for proposed method is; 39 for RTSR; and 47 for AODV. At 80 m, the end-to-end delay is 41 for proposed method is; 47 for RTSR; and 51 for AODV. At 90 m, the end-to-end delay is 49 for proposed method is; 53 for RTSR; and 61 for AODV. At 100 m, the end-to-end delay is 58 for proposed method is; 61 for RTSR; and 69 for AODV. At 110 m, the end-to-end delay is 61 for proposed method is; 68 for RTSR; and 73 for AODV. For 120m, the end-to-end delay is 73 for proposed method is; 79 for RTSR; and 85 for AODV.

## CONCLUSION

the aim of the study was to propose a trust-based algorithm which works on the cluster technique and enable higher energy efficiency and trust calculation using the nodes rather than the centralized controlling body. The proposed solution is based on hexagonal clusters which makes the network more efficient and consumers less energy because of reduced distance between the nodes. For comparison, a stimulation was performed at different time interval. The results shows that proposed method had better throughput compare to the RTSR and AODV. Similarly, the proposed method shows better performance in terms of packet delivery rate and end-to-end delay compared to the RTSR and AODV. So, we conclude that the proposed method is a suitable solution for the mobile ad hoc based network.

## References

Tseng, Y. C., Ni, S. Y., Chen, Y. S., & Sheu, J. P. (2002). The broadcast storm problem in a mobile ad hoc network. *Wireless networks*, *8*(2-3), 153-167.

Taha, A., Alsaqour, R., Uddin, M., Abdelhaq, M., & Saba, T. (2017). Energy efficient multipath routing protocol for mobile ad-hoc network using the fitness function. *IEEE access*, *5*, 10369-10381.

Desai, N., Chong, W., Achilles, H., Daijavad, S., & La Porta, T. (2019, June). Large-scale hybrid ad hoc network for mobile platforms: Challenges and Experiences. In *2019 IEEE International Conference on Smart Computing (SMARTCOMP)* (pp. 332-339). IEEE.

Raza, N., Aftab, M. U., Akbar, M. Q., Ashraf, O., & Irfan, M. (2016). Mobile ad-hoc networks applications and its challenges. *Communications and Network*, *8*(3), 131-136.

Borkar, G. M., & Mahajan, A. R. (2017). A secure and trust based on-demand multipath routing scheme for self-organized mobile ad-hoc networks. *Wireless Networks*, *23*(8), 2455-2472.

Elhoseny, M., & Shankar, K. (2019). Reliable data transmission model for mobile ad hoc network using signcryption technique. *IEEE Transactions on Reliability*.

Sarkohaki, F., Fotohi, R., & Ashrafian, V. (2020). An efficient routing protocol in mobile ad-hoc networks by using artificial immune system. *arXiv preprint arXiv:2003.00869*.

Rath, M., Pattanayak, B. K., & Pati, B. (2017). Energetic routing protocol design for real-time transmission in mobile ad hoc network. In *Computing and Network Sustainability* (pp. 187-199). Springer, Singapore.

Marchang, N., Datta, R., & Das, S. K. (2016). A novel approach for efficient usage of intrusion detection system in mobile ad hoc networks. *IEEE Transactions on Vehicular Technology*, *66*(2), 1684-1695.

Singh, S., Woo, M., & Raghavendra, C. S. (1998, October). Power-aware routing in mobile ad hoc networks. In *Proceedings of the 4th annual ACM/IEEE international conference on Mobile computing and networking* (pp. 181-190).

Nesargi, S., & Prakash, R. (2002, June). MANETconf: Configuration of hosts in a mobile ad hoc network. In *Proceedings. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies* (Vol. 2, pp. 1059-1068). IEEE.