ISSN 2319 - 6629
Volume 4, No.3, April - May 2015
International Journal of Wireless Communications and Networking Technologies
Available Online at http://warse.org/pdfs/2015/ijwcnt04432015.pdf

A Novel Approach towards Trusted and Stable Cluster in MANET

Kanwaljeet Kaur[1], Himani[2]
[1]M.tech Student, GIMET, Amritsar, India, Krrandhwakanwal@gmail.com
[2] Asst. Prof. GIMET, Amritsar, India, global.himani26@gmail.com

ABSTRACT

MANET has wide impact on research area from past two decades. Its structure less establishment and flexibility increases its growth of popularity. MANET is described as frequent change in network topology and restricted energy. Thus the effectiveness of MANET not only depends on control protocols but also on management of network topology and energy administration. Clustering in MANET is useful to make network more manageable. Many clustering protocols and algorithms are proposed to make network more stable and trusted. In this paper we depict the most prominent factor related to the MANET. The motive of this paper is to perform investigational study including: routing structure, storage method, overhead, cryptographic authentication and misbehavior of nodes to clearly address relevant problem in cluster based routing protocol and provide a suitable solution by proposing a trusted and Stable clustering algorithm.

Keywords: MANET, Clustering, Efficiency, Stability, Security, Trust.

1. INTRODUCTION

MANET is collaboration of wireless mobile nodes that build a temporary network without any centralized infrastructure. In MANET each node play a role of host and router itself. Nodes in MANET are mobile in nature thus building an energy efficient network is a primary issue. MANET is more vulnerable to attack as compared to wired network. Hence designing a trusted and energy efficient network is paramount challenge. Clustering is the best approach for designing and managing the mobile ad-hoc network environments. A good clustering is beneficial in many ways such as: reuse of network resources, efficient and stable network, conserve communication bandwidth and reduce transmission overhead. The main purpose of cluster is to elect a most suitable node as cluster head that can coordinate for its cluster. Moreover it manages the reputation tables of nodes, that how nodes are behaving in the cluster, so that the malicious node can isolated or punished and good reputed node can be elected as future cluster head.

In this paper we present a new, trusted and stable clustering algorithm. This algorithm check the trust value of every invoked node then form a cluster of trusted nodes and later elect the node has best material resources(high energy, low mobility, trust etc.) as cluster head.

This paper is organized as follows: Part II presents an overview of related work in the field of cluster based routing protocols in mobile ad-hoc networks. Part III describes the details of our proposed algorithm. Results of proposed algorithm are discussed in Part IV. Conclusion and future work are drawn in Part V.

2. RELATED WORK

Several clustering protocols were designed for MANET. Each protocol form cluster differently and perform well at specific task.

S. Bansal et al [1] describe a protocol called OCEAN (an Observation-based cooperation Enforcement in Ad hoc network). This protocol directly observe the behaviour of other nodes instead of using indirect reputation method. Decision of routing is taken by directly observing the behaviour of neighbouring node. Simulation study is carried out by calculating average throughput with high and zero mobility of OCEAN.

Zhong, S et al.[2] proposed new protocol called SPRITE. Sprite is simple, cheat-proof, credit base system that encourage the selfish node by giving credit, so that node not behave selfishly. According to SPRITE node get incentive in two ways by paying debit or buy credit working honestly and by cooperating other nodes.

Mehran Abolhasan et al. describe multimedia support in mobile wireless networks (MMWN) [3]:In MMWN routing protocol [4] hierarchical clustering is used to sustain the structure of network and information is stored in dynamic distributed database. Cluster formation is done using switches, endpoints and a location manager (LM). In MMWN the location of each cluster is managed by Location Manager. Network overhead is less in MMWN because only the Location manager is responsible for updating and finding location.

C.-C. Chiang describe Cluster-head gateway switch routing (CGSR). CGSR[5] is a hierarchical routing protocol in where nodes are arranged in cluster. CGSR elects a cluster head, node that having high energy and less mobility and rest of the nodes as member nodes. Maintenance of cluster hierarchy is not required as cluster is maintained by cluster head. The cluster head controls over transmission medium and inter cluster communication. In CGSR member node maintain routes to its cluster head only that lead to reduce overhead.

Anderegg et al [6] introduce a cost effective new VCG protocol that is used to works over dynamic source routing. This uses the cost of energy parameter to find the cost of the node who is forwarding the packet of other nodes. In this protocol a node has to indicate the signal strength at which it emit and it also has to forward the detail about the neighbour received signal strength that is like to be cheat. Author proved that to make this protocol workable there should be only one cheating node.

Yang et al. [8], introduce a scheme that protects both routing and packet forwarding in the context of the AODV [9]. It is self-forming, without any assumption and any previous knowledge about the trust between the nodes or presence of any intermediate trust entity. It detach the node that misbehave and provide threshold cryptography to increase the endurance against misbehaving nodes. This scheme is completely localized and its strategy of giving credit generates overhead that is considerably reduced when network is safe.

M. Jiang et al. describes Cluster-based routing protocol (CBRP). In CBRP [10] cluster based routing protocols nodes are arranged to form cluster. Each cluster has a cluster-head, which coordinates the data transmission within the cluster and to other clusters [3]. In CBRP routing information is transferred through cluster head only, thus the number of control overhead carried through the network is far less as compared to the convention flooding techniques.

Pushpita Chatterjee [11] describe a game theoretic routing model. Two mechanisms Credit and reputation are to force the nodes to work honestly. This model mainly proposed to overcome the problem of selfish behaviour of node, where the node behave idle and stop the transmission. Cost of forwarding packet for intermediate nodes are calculated using Procurement and Dutch mechanism. STACRP find selfish nodes and force them to cooperate, so that the throughput of network can be increased.

Mohamed Dyabi et al [12], propose a new clustering algorithm for ad hoc networks, where the clusters are formed around the most powerful nodes, i.e. the node that has the best material resources such as residual energy, free memory, processor speed and hard disk space is elected as cluster head.

Subbian Umamaheswari et al [13] propose an AntHocNet + Security (ANTSEC) framework that includes an enhanced cooperative caching scheme embedded with artificial immune system. This framework improves security by injecting protection into the data packets, improves the packet delivery ratio and reduces end-to-end delay using cross layer design.

Table 1. Compression Table of previously proposed clustering Techniques

Protocol [Ref. no]	Misbehaviour detection	Storage method	Frequency of updates	Route structure	Cryptography authentication	Critical nodes	Overheads
OCEAN[1]	Selfishness	No previous route information, only the reputation of node is stored	Periodic	Rank based routing	No	No	Small overhead
SPRITE[2]	General	No previous route information, only the reputation of node is stored	Periodic	Rank based routing	Yes	No	Small overhead
MMWN[3]	No detection of misbehaviour	Maintains a database	Conditional	Hierarchical	No	Yes, Location Manager	Least overhead and minimized control overhead
CGSR[5]	No detection of misbehaviour	Tables	Periodic	Hierarchical	No	Yes, Cluster Head	Less overhead
VCG[6]	Selfishness	Maintains a database	Conditional	Hierarchical	No	No	Overhead increases with large size network
TOKEN[8]	General	Maintains a database	Conditional	Hierarchical	Yes	No	Less overhead
CBRP[10]	General	Tables	Periodic	Hierarchical	Yes	Yes, Cluster Head	Less overhead than the traditional methods
STACRP[11]	General	Table	Periodic	Hierarchical	Yes	Cluster Head	Less overhead

3. PROPOSED WORK

We observe from previous research that the number of algorithms have been proposed and all are beneficial in specific tasks. Some are good in detecting the malicious (a node that misbehave in network) nodes and isolate them, some punish and manage reputation table. In some algorithms nodes are encourages to cooperate and not to misbehave by giving credit. Some algorithms are energy efficient but the network is more vulnerable to attack because these algorithm are not meant for security. By keeping all these things in mind we proposed an algorithm that is trusted as well as more stable.

3.1 Design of Proposed ALGORITHM

Initially when a node is invoked trust value of the node will be calculate that whether the node is trusted or node. If the node will be trusted then it will be registered as one of node of MANET. Otherwise the trust value of the node will be calculate until it will start behaving well. Once the node will be registered, network establishment will be divided into two parts: setting up of cluster and maintenance of cluster.

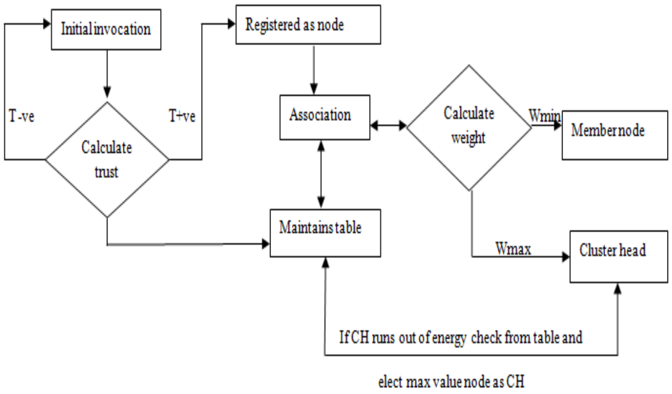

Figure 1. Architecture of Proposed algorithm

3.2 Calculation Of Trust Value

Procedure calculate trust;

```
If ($Node\_Invoked_i$==”Trusted_Behaviour”) Then
    If ( i $\in$ trusted) Then Trust_Value = +ve;
        Begin
Call Register_Node
    Store_value := i{+ve};
End
    Else $Trust\_Value_i$ = -ve;
        Begin
    Call intial_invocation
End
```

3.3 Setting up of cluster

All the nodes having +ve trust value will be registered on the network. Trust value of node is change with the change in behaviour of node and it is updated in reputation table. Then a broadcast message is passed through all nodes to know the mobility and energy of node. This information is gathered to calculate the weight of the node. Weight of the node is calculated by the following formula:

$$\delta \mathbf{W} = \delta \mathbf{T} + \delta \mathbf{M} + \delta \mathbf{E}$$

To compute the weight positive trust value is chosen, low mobility and high energy of node is taken. Then the node having maximum weight is chosen for Cluster Head and the nodes having minimum energy become the member nodes. Computed weight value is stored in reputation table for future use.

3.4 Maintenance of cluster

Trust value of the nodes change with the change in behaviour of node and maintained in table. Current calculated value is also maintained in table. At a point cluster head runs out of energy and new cluster head needs to elect. Before going to die CH choose the node have maximum weight (according to current updates in maintenance table) to delegates the functionality of CH. With the help of reputation table re-election of cluster head can be made easy and can also lead to minimize the energy and time consumption.

3.5 DATA DICTIONARY

Table 2. Data Dictionary

Variable Name	Description
CH	Stands for Cluster Head
δW	Denotes calculated weight of the node
δT	Denotes trust rate of node
δM	Denotes mobility of node
δE	Denotes energy of node
T-ve, T+ve	Denotes the distrust and trust of node respectively
Wmin, Wmax	Denotes the minimum weight and maximum weight of node

4. SIMULATION AND RESULTS

The aim of this section is to study the performance of our proposed work by using NS2. Simulation parameters used are listed in Table 3.

Table 3. Simulation Parameters

Parameters	Values
Area	1000 * 1000 meter
No of Node	30
simulation duration	900 s
physical/Mac layer	IEEE 802.11 at 2Mbps
Initial energy per node	2 Joules
Data Rate	2.0

We consider the following parameters to measure the performance of proposed Trusted and Stable Clustering technique

1. Throughput– It is defined as the amount of data traffic successfully received and forwards to the higher layer by WLAN MAC

$$\text{Throughput} = \frac{\text{No. of delivered packets} * \text{Packet size} * 8}{\text{Total duration of Simulation}}$$

2. PDR– Packet delivery ratio is defined as the ratio between the number of data packets received and the number of data packets sent.
3. Delay Analysis– The average time delay for receiving the data packets.
4. Packet Dropped– It is the difference between total number of packet transmitted by transmitter and total number of packet received by receiver at receiver end.

Figure 1 depicts the average throughput. Graph shows that, the throughput rate of Proposed Algorithm is 97 kb/s with respect to time, the graphs results prove that proposed algorithmic technique has high throughput rate in network.

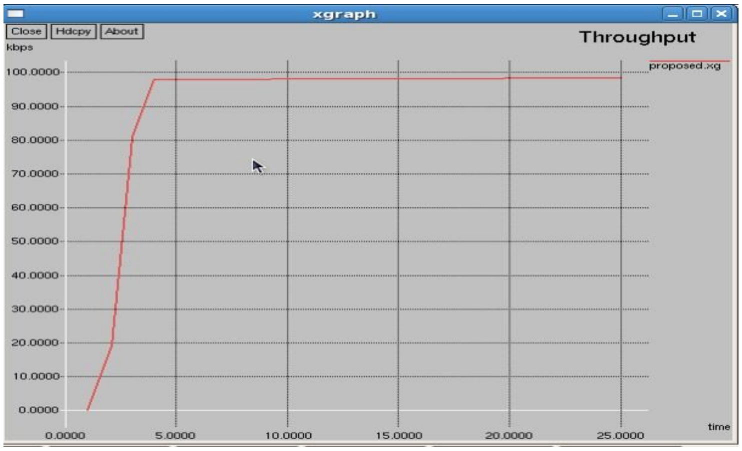

Figure 1 Throughput in proposed Trusted and Stable Clustering technique

Figure 2 depicts the average packet delivery ratio of data. Graph shows the ratio of packet delivery increases with the increase in time. As more as the number of packets transferred they all are received at the receiver side. Packet delivery ratio is of 97% cent as the communication is done by the cluster head and gateway only.

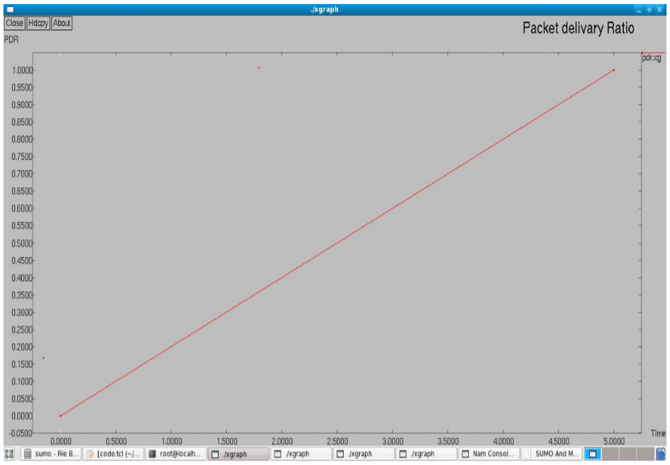

Figure 2 packet delivery ratio in proposed Trusted and Stable Clustering technique

Figure 3 depicts the average number of packets dropped in the transmission of data. Graph shows that there is no packet dropping the transmission. The number of packets are transferred by the sender they all are received by the receiver, hence no packet is dropped.

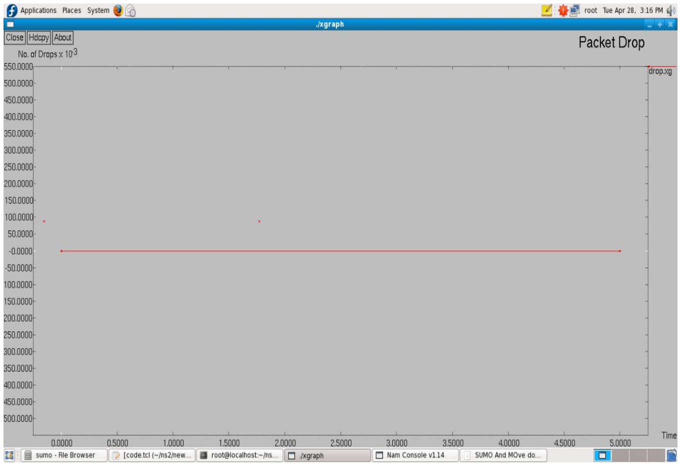

Figure 3 proposed Trusted and Stable Clustering technique

Figure 4 depicts the average delay in data transfer. Graph shows that delay time is estimated as 0.5 sec for Packet transmission in proposed algorithm. The graphs results proved there is a minimum delay in proposed Trusted and Stable Clustering technique.

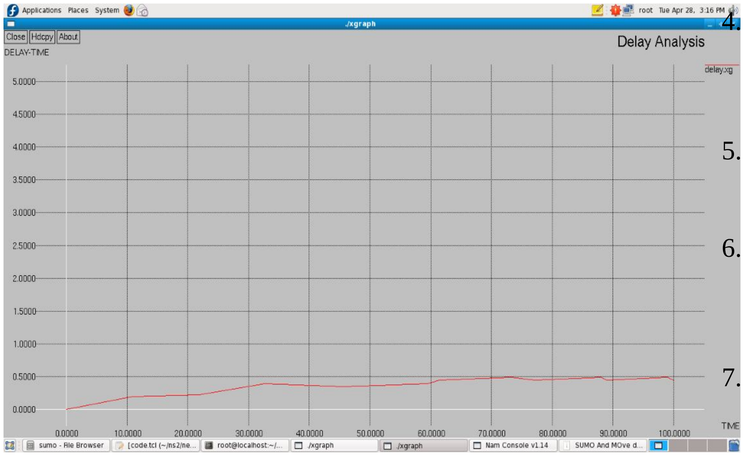

Figure 4 Delay in proposed Trusted and Stable Clustering technique.

5. CONCLUSION

MANET has wide impact on research area from few years, and can engaged in a broad range of applications in both civilian and military scenarios. The design of stable, secure and energy efficient routing protocols for MANETs is a challenging task. In this paper, we have presented an investigational study on clustering routing protocols in MANETs and related different methodologies. Finally, we analyzed a MANET clustering routing protocols and algorithms in deep and proposed a new trusted and stable cluster algorithm. We study the performance of proposed Trusted and Stable Clustering algorithm, where results depict that Proposed algorithm has high throughput, pack delivery ratio, zero packet dropping and less delay in receiving the packet.

As future work we intend being adding some more parameters that affect the performance of ad hoc network and like to propose more stable and highly secured algorithm for MANET.

.

ACKNOWLEDGEMENT

I would like to do special thanks to Ms. Himani for giving her most precious time for guidance and supporting during the research. Finally, I thank to most gracious Almighty, and my parents for their Support.

REFERENCES

1. S. Bansal and M. Baker, "**Observation-based Cooperation Enforcement in Ad Hoc Networks**", http://arxiv.org/pdf/cs.NI/0307012, July 2003.
2. Zhong, S., Chen, J., Yang, Y.R.: Sprite: **A simple, cheat-proof, credit-based system for mobile ad-hoc networks**. In: Proceedings of IEEE INFOCOM 2003, pages, pp. 1987–1997, March–April (2003)
3. Mehran Abolhasan, Tadeusz Wysocki and Eryk Dutkiewicz, “**A review of routing protocols for mobile ad hoc networks,**” 2003 Elsevier
4. K.K. Kasera, R. Ramanathan, “**A location management protocol for hierarchically organised multihop mobile wireless networks”**, in: Proceedings of the IEEE ICUPC_97, San Diego, CA, October 1997, pp. 158–162.
5. C.-C. Chiang, **“Routing in clustered multihop mobile wireless networks with fading channel**”, in: Proceedings of IEEE SICON, April 1997, pp. 197–211.
6. Anderegg, L., Eidenbenz, S.: “**Ad hoc-vcg: A truthful and cost efficient routing protocol for mobile ad hoc networks with selfish agents”.** In: Proceedings of MobiCom 2003, pp. 245–259, September (2003)
7. Hu, Y.-C., Perrig, A., Johnson, D.: “**The dynamic source routing protocol for mobile ad hoc networks (dsr**)”. draft-ietf-manet-dsr-10.txt, July 2004
8. Yang, H., Meng, X., Lu, S.: “**Self-organized network-layer security in mobile ad hoc networks”.** In: Proceedings of ACM WiSe02, September (2002)
9. Perkins, C., Royer, E.B., Das, and S.: “**Ad hoc on demand distance vector (aodv) routing**”. IETF RFC 3561, July 2003
10. M. Jiang, J. Ji, Y.C. Tay, “**Cluster based routing protocol, Internet Draft**”, draft-ietf-manet-cbrp-spec-01 .txt, work in progress, 1999.
11. Pushpita Chatterjee · Indranil Sengupta · S.K. Ghosh, “**STACRP: a secure trusted auction oriented clustering based routing protocol for MANET**”, Springer Science+Business Media, LLC 2012.
12. Mohamed Dyabi and Hakim Allali “**A new MANETs clustering algorithm based on nodes performances**” Fifth International Conference on Next Generation Networks and Services (NGNS), IEEE, May 28-30, 2014.
13. Subbian Umamaheswari and Govindaraju Radhamani “**Enhanced ANTSEC Framework with Cluster based Cooperative Caching in Mobile Ad Hoc Networks** ” Journal of Communications and Networks, IEEE 1, February 2015