VOL. 10, NO. 9, MAY 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

MAXIMUM TRUSTED CLUSTER HEAD SELECTION ALGORITHM FOR MANET

Rani V. G.
Department of Computer Science, SRI Ramakrishna College of Arts and Science for Women, Coimbatore, India
E-Mail: ranisrcw@gmail.com

ABSTRACT

Mobile Ad hoc Networks (MANET) are self-organizing and self-configuring multi hop wireless networks capable of adaptive re-configuration network. The absence of infrastructure, limited bandwidth, dynamic nature and unpredictable link failure perturbs the efficient network services. Trust is an important aspect in the design and analysis of secure distribution systems. Hence, in this proposed study, trust based security is chosen as a security scheme to strengthen the cluster head. Therefore, a secured cluster head could be selected for each cluster, which guarantees the safe routing. Therefore, to strengthen the selected cluster head, a security measure, called trust mechanism is proposed.

Keywords: MANET, security, trust.

1. INTRODUCTION

Mobile ad hoc network is a group of mobile nodes which communicate through wireless link without any infrastructure. It is an autonomous network consisting of mobile nodes that communicate with each other over wireless links [6].Therefore the ability of mobile nodes roam freely leads to numerous and erratically changes in topology [1]. A successful ad hoc network is achieved if and only if nodes in the network cooperate with each other. When the size of the network increases the handling of nodes become simple if hierarchy structure is used. Clustering is one of the techniques which make the hierarchical structure possible. In clustering, the nodes are grouped and assigned a special role for the nodes. Each cluster has a leader node called as cluster head which form a backbone and lays the foundation of the network. Clustering in which the mobile nodes are dynamically organized into groups called clusters to maintain relatively stable effective topology [10]. Security in MANET faces technical challenges due to the restriction of resource constraints like limited bandwidth, minimum computation power, and infrastructure less network and restricted memory size. MANET, nodes are comprised of resource constrains and therefore they are extremely vulnerable to variety of attacks. The meaning of vulnerability is self-evident where there is no clear secure boundary in the mobile ad hoc network referred by Author [14]. Since the study travels towards the clustering process, the security is given importance for the cluster head which plays an important role in clusters. When providing security for clustering, trust mechanism suits well than the other security methods, because, a cluster head node is the leader node which should be a trustworthy person than the other node.

Therefore, the role of cluster head not only needs a proper selection of cluster head but is essential to include security aspects for selection. Security architecture, where the layered the security as follows:

Table-1. Security architecture.

SL_5	End-To-End security
SL_4	Network security
SL_3	Routing security
SL_2	Communication security
SL_1	Trust infrastructure

- **SL_5 End-to-End security layer:** Security in this layer is highly independent to the parties and the specific applications. This type of security service depends on the requirement of the networking technology.
- **SL_4 Network security layer:** This layer refers to the security schemes used by the network protocols. They generally perform sub-network access operations from end-to-end systems. It includes authentications, confidentiality and integrity.
- **SL_3 Routing security:** It refers to the security mechanism provided for the routing algorithm. The routing security includes secure routing and secure data forwarding. During secure routing the nodes exchange the route regarding information's correctly to the neighbors. As far as data forwarding aspect is concerned, the data packed should be protected from tampering, dropping and modifying by adversaries.
- **SL_2 Communication security layer:** This layer provides security when transmitting data frames between nodes. Providing security during communication will give solutions to the eavesdropping , alteration, etc.,
- **SL_1, Trust infrastructure layer:** Due to the absence of centralized authority, the nodes are free to establish a link between the neighbors when they are in same radio range. Basically, the link establishments are carried during initial stage or

during the topology changes which makes a node to move out of the current position or a node join. During this stage, the neighbor node should trust each other for creating link for communication.

From the above security architecture, trust mechanism, SL1 layer suits for providing security during the initial stage. Moreover, establishing trust infrastructure in the initial stage will provide secured layer for the upper layer to perform the routing without any disturbance. Hence, this paper aims to select a secured cluster head using trust based security.

2. LITERATURE REVIEW

Author [12] proposed an efficient dynamic clustering protocol for MANET. In dynamic clustering protocol they have five state connections. These are un-clustered state, orphan state, election state, cluster node state, in addition to cluster head state. Also, they develop key distribution method for the distribution of symmetric keys in MANETs. In dynamic clustering protocol they designed to verify the protocol and have an estimate of the cost to gather the density information. Author [8] proposed a secured weight-based clustering algorithm allowing more efficiency, protection and trust in the management of cluster size deviation. This algorithm is called Secured Clustering Algorithm (SCA), since it includes security requirements by using a trust value defining how much any node is trusted by its neighborhood, and by means of the Certificate as node's identifier to avoid any possible attacks (Spoofing).By virtue Ad hoc networks poses a real challenge towards establishing trust among nodes within the network Author [4] proposes a novel approach based on clustering, for establishing trust. Novel cluster head approach in this work provides leaner trust establishment when compared to traditional peer-to-peer approach. Author [3] propose and evaluate a security concept based on a distributed certification facility. New nodes start to contribute in the network as guests; they can only become full members with a network signed certificate after their authenticity has been warranted by some other members. Author [15] analyze the security problem in the hierarchical mobile Ad Hoc networks. And then offer a secure clustering algorithm based on reputation in defense of threats in clustering. In this algorithm, the nodes reputation is used to develop security, which is evaluated by combining the experience of the node in the routing process. Author [13] propose a new cluster based multicast tree (CBMT) algorithm for secure multicast key sharing, in which source node uses Multicast Destination Sequenced Distance Vector (MDSDV) routing protocol to collects its 1 hop neighbors to form cluster and each node which have child node is elected as the Local controllers of the created clusters.

3. NEED OF TRUST IN CLUSTERING

MANET faces many difficulties concerning management functions, routing and scalability and so on [1]. Ad hoc is naturally trust-your-neighbor relationship. These network normally developed, used and expire on the fly and have short life. Pure ad hoc network closely resemble human behavior model, here a set of nodes, that have never met each other are able to communicate with one another based on mutual trust level development over a period of time. According to Author [8], trust is defined as "a set of relations among entities that participate in a protocol". Trust is also time dependent it grows and decays over a period of time. As in real life, trust levels are determined by the particular actions that the trusted party can perform for the trustee. Trust can't be treated as a property of trusted systems but rather it is an assessment based on experience that is shared through network of people. Similarly trust levels can be computed based on the effort that one node is willing to expand for another node. The effort can be in terms of battery consumption, packet forwarding or any other such parameter that helps in establishing a mutual trust levels. Hence, the characteristics of MANETs should be carefully defined. The main features of trust are:

- A decision method to determine trust against an entity should have fully distributed when the existence of third party cannot assumed.
- Trust should have highly customizable manner without excessive computation load, while it capturing the complexities of the trust relationship.
- A trust in MANET should not assume that all nodes are cooperative.
- Trust should be dynamic in nature, and that should not be static.
- Trust should be subjective.
- Trust should not be necessarily transitive. For example, A trusts B and B trusts C does not implies that A trusts C.
- Trust should be asymmetric and it is not necessarily reciprocal.
- Trust should be context dependent.

By computing trust levels from the inherent knowledge present in the network the trustworthiness of routers can be computed. The routes computed through this mechanism may not be secure instead provide reliability. Trust computation involves an assignment of weights to the events that where monitored and quantified. Based on the evaluated trust, security measures are taken or security decisions are made.

4. PROPOSED TRUST EVALUATION METHOD

One of the main objectives of the proposed study is to elect a secure cluster head. A trust model is the one which evaluates the trustworthiness of the nodes in the network. Possible events that can be recorded are:

- Data packets forwarded

- Control packets forwarded
- Control packet received
- Data packets received
- Stream establishment
- Data forwarded

The above are the events a node can collect through passive mode. Though there are many events gathered, this study considers only the communication information and the data packet information's. This is because, obtaining so much of information is time consuming and moreover it also consumes more energy to obtain that information Hence, this paper considers the following to evaluate the trustworthiness of a node.

- Direct Observation
- Cluster head Observation

Using the above two observation the trustworthiness of a nodes calculated as below.

a) Trust Calculation Mechanism

When direct observation is considered, a node will provide its trust worthiness using its previous history. The history includes the information of the nodes communications. The cluster head observation will provide two factors namely selfishness of a node and the trustworthiness of a node collected from the previous cluster head of the node. The trust in the proposed method is based upon the information that one node can gather about the other node in passive mode i.e., without requiring any special interrogation packets a node can gather the information of other nodes based on the previous experience.

The trust value calculated for direct observation gathered from all the neighbor nodes, DT(x) is calculated using the below equation.

$$T(x) = D(x) + TCH(x) \quad (1)$$

Where,

The direct observation D(x) of a node is calculated using the following:

$$D(x)=(CR-CD)+(DR-DD) \quad (2)$$

Where,

CR = Communication Packet Received
CD = Communication Packet Dropped
DR = Data Packet Received
DD = Data Packet Dropped

Therefore, trust from cluster head, TCH(x) includes two factors to present its opinion about the node.

- Trust value of the previous cluster head.
- Selfishness factor of the node.

The nodes, called selfish nodes, intend to gain the greatest benefits from the networks while trying to preserve their own resources. The resource includes hardware, battery life or bandwidth. Selfish nodes only attempt to communicate with the nodes it wants to send data packets to. They may refuse to cooperate when it receives routing packets or data packets that they are not interested in. Hence, they either drop data packets or refuse to retransmit routing packets that they have no interest in.

$$TCH(x) = PCH(x) + Self(x) \quad (3)$$

Where,

PCH(x) = Previous Cluster Head experience
Self(x) = Selfishness factor

Self(x) is calculated by considering the battery power of a node

$$Self(x) = BP(x) \quad (4)$$

Where,

$BP(x) =$ Battery Power

Therefore the trust value, T(x) of a node x is calculated using the equation (1) by combining the direct observations and the current cluster head observation.

5. PRIORITY BASED CLUSTER HEAD SELECTION

In this section new priority based cluster maintenance is proposed where the trust value of a node plays a vital role in deciding the cluster head. The following section describes the re-election procedure and the proposed priority scheme.

b) Cluster head re-election

The processing of clustering is never completed without a proper maintenance scheme [2]. When a cluster head node leaves the current cluster, than the new cluster head is elected by calling the cluster head election procedure. This procedure is invoked whenever one of the cluster heads is not able to achieve its responsibilities further due to some unavoidable situations like, minimum battery or mobility. The invocation of the election procedure does not mean that all cluster head are replaced. Only the corresponding cluster members will participate in the election process to elect the new cluster head. The repeated calling of the re-election procedure will make the entire cluster member of the corresponding cluster head to participate in the election. This repeated re-election leads to information overhead and energy drain. To overcome the repeated process, this study introduces a priority scheme which uses the trust value which is calculated in the previous section.

c) Proposed priority method

During the maintenance stage, any node in the cluster will get out of the current cluster due to the mobility nature or for some other reasons. If the

moving node is a cluster head, then the re-election is unavoidable. Frequent calling of re-election procedure will lead to early energy drain. Therefore, to avoid the re-election process, the following key idea is framed.

- To make use of CMT table to reserve second cluster head.
- When a current cluster head leaves the cluster, it handover the cluster head role to the reserved node.

The above are the two simple steps followed when a cluster head leaves the current cluster. The main advantage of the priority method is

- Time taken to elect a new cluster head is minimized.
- Cluster head role is distributed equally.
- Avoid unwanted repetition of cluster head election procedure.

Every cluster head will maintain a CMT Table-11 where all the cluster member entries are stored. Table-2. gives the outlook of the Cluster Member Table (CMT).

Table-2. Cluster member table (SMT)

NID	P(X, Y)	Weight	Trust

Current cluster head will record the cluster member entries along with the trust values. According to the trust values of the member each node will get the priority for the next cluster head role. When the current cluster leave the cluster, it automatically handover the cluster head role to the highest trust value node

After the election of the new secured priority based cluster head node is elected. Thus, using a priority scheme any clustering algorithm can avoid re-election of cluster head which is given in the Figure-5. The proposed priority scheme is included in the Head algorithm (PBCA).

6. RESULT AND DISCUSSIONS

This section discusses the result obtained by the proposed PBCA, using the following Simulation parameter.

Table-3. Simulation parameter

Parameter	Meaning	Value
N	Number of nodes	150
X x Y	Size of the network	1500 X 1500
Speed	Speed of the node	18 m/sec
R	Transmission range	250 m
Time	Duration of simulation	150 sec

It was compared with the WCA algorithm and the efficiency of the proposed PBCA is proved. The efficiency of PBCA was evaluated towards two measures namely Transmission Range and Speed.

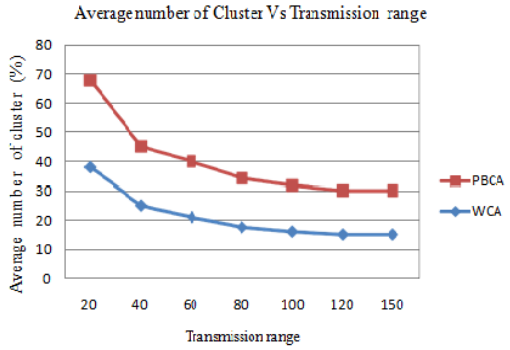

Figure-1. Average number of Cluster Vs Transmission range.

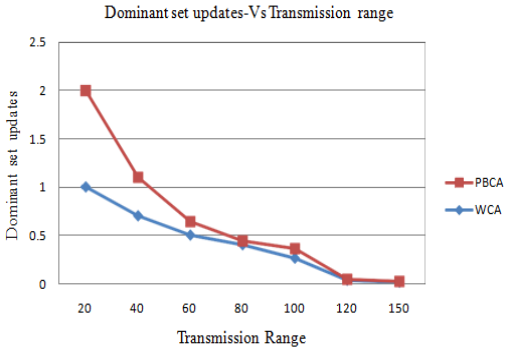

Figure-2. Dominant set updates Vs Transmission range.

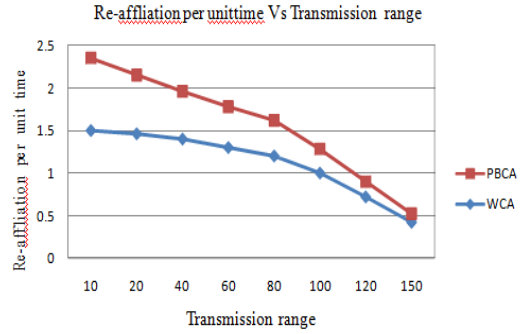

Figure-3. Re-affiliation Vs Transmission range.

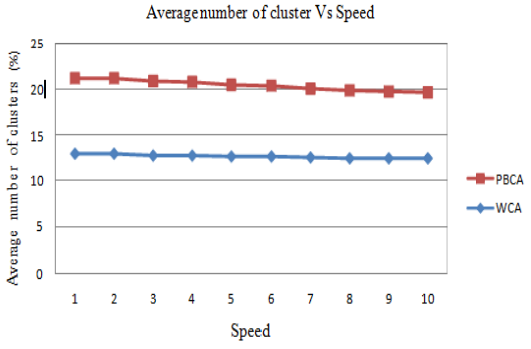

Figure-4. Average no. of Clusters Vs Speed.

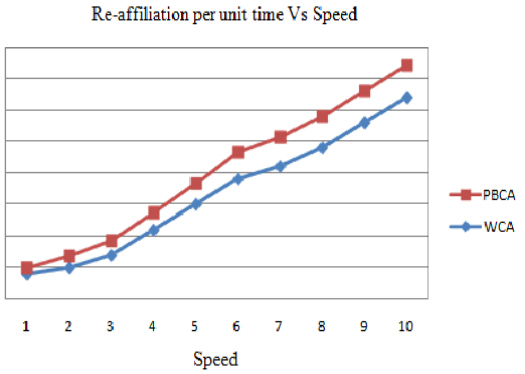

Figure-5. Re-affiliation Vs Speed.

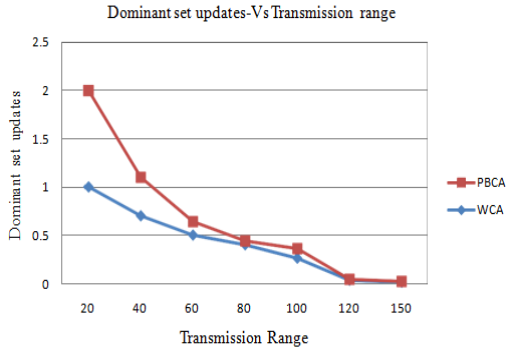

Figure-6. Dominant set update Vs Speed.

In this paper the need of security in MANET is discussed, in particularly for the cluster head. Moreover, a new trust method is proposed which estimate the trust value of a node in the cluster and further it is used as criteria to elect the cluster head. It also discusses the draw backs of the re-election process and a new priority method is proposed which gives an alternative solution for the re-election process. Finally, the proposed algorithm is evaluated using the network simulator NS2 and the results are compared with the existing WCA algorithm and the outperformance are evaluated.

REFERENCES

[1] An B. and Papavassiliou B. 2000. "A Mobility-based clustering approach to support mobility management and multicast routing in mobile adhoc wireless network, Int. J. Netw. Manag., Vol. 11, no.6, pp.387-395.

[2] Agarwal R. and Mahesh Motwani. 2009. Survey of clustering algorithms for MANET. International Journal on Computer Science and Engineering (IJCSE) 1: pp. 98–104. http://arxiv.org/ftp/arxiv/papers/0912/0912.2303.pdf

[3] Bechler M. A. 2004. Cluster-Based Security Architecture for Ad Hoc Networks, IEEE INFOCOM.

[4] Boodnah J. 2010. Trust in Ad hoc Networks A Novel Approach based on Clustering.

[5] Chatterjee M. S. K. Das and D. Turgut. 2000. "An On-Demand Weighted Clustering Algorithm (WCA) for Ad hoc Networks," in Proc. IEEE Globecom'00, pp.1697-701.

[6] Chen G. and Stojmenovic I. 1999. "Clustering and routing in mobile wireless networks," in Technical Report TR-99-05.

[7] Corson S. and Macker J. 1999. Mobile AdHoc networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations, "RFC 2501, January. http://www.ietf.org/rfc2501.txt

[8] Eschenauer L., Virgil D. Gligor and John Baras. 2002. "On Trust Establishment in Mobile Ad Hoc Networks," Proc. 10th Int'l Security Protocols Workshop, Cambridge, U.K., Apr. Vol. 2845, pp. 47-66.

[9] Kadri B. *et al.* 2007. Secured Clustering Algorithm for Mobile Ad Hoc Networks, IJCSNS International Journal of Computer Science and Network Security, Vol.7 No.3, March.

[10] Lin C. R. and Gerla M. 1997. Adaptive clustering for mobile wireless networks", IEEE Journal on Selected Areas in Communications. Vol. 15, No. 7, pp. 1265-1275, September.

[11] Rani V. G. and Dr. M. Punithavalli. 2013. "MPBCA: Mobility Prediction Based Clustering Algorithm forMANET", International Journal of Engineering and Technology", Vol.5, No.1, February-March.

[12] Shubha *et al.* 2011. Efficient Secure Clustering Protocol For Mobile Adhoc Network Volume 2, No. 9, September, Journal of Global Research in Computer Science.

[13] Suganya *et al.* 2009. Cluster Based Multicast Tree for Secure Multicast Key Distribution in Mobile Adhoc Networks, IJCSNS.

[14] Wenjia Li and Anupam Joshi. 2008. Security Issues in Mobile AdHoc Networks- A Survey.

[15] Yao Yu *et al.* 2012. A Secure Clustering Algorithm in Mobile Ad Hoc Networks, IPCSIT Vol. 29.