Cross Layer Integrated Approach for Secured Cluster Selection in Ad Hoc Networks

D. N. Goswami and Anshu Chaturvedi

Abstract—**Mobile Ad hoc Network (MANET) basically, is a collection of mobile hosts incorporating wireless interfaces that forms a transitory autonomous network. They do not base on fixed infrastructure or central administration, rather work on the principle of self-organized interconnections among mobile nodes. Fundamentally, in MANET when nodes come inside the transmission range of neighboring nodes', they can be detected by each other and can communicate directly. However for communication outside this range they have to depend on some other nodes to relay the messages .This is where routing protocols have to play a very important role. Literature for improving the performance of routing protocol is available in abundance. Among these comes, the hierarchical/cluster-based routing protocols that claim to reduce control overheads. Clustering in Mobile Ad hoc Networks (MANETs) has proved to be advantageous compared to the traditional networks. However the highly dynamic and unstable nature of MANETs makes it intricate for the cluster based routing protocols to split a mobile network into clusters and determination of cluster heads for each cluster. Although much previous research has concentrated on cluster-head selection in MANETs, not much effort has been done on the security side of cluster-head selection. This paper emphasize that secure cluster head selection in MANETs has an intense effect on network performance. Specifically, we stress that in ad hoc network where all the participants are self controlled, security is an essential aspect and the effective cluster-head selection can improve network throughput. We propose a secure and effective cluster-head Selection scheme using a cross-layer approach that integrates cluster-head discovery and selection functionality with network ad hoc routing mechanisms and the lower layer drivers built-in the system. Besides, proposed scheme handle the disconnections in ad hoc network due to the effects of topology changes and battery depletion. This scheme allows clients to switch to better cluster-head nodes as network topology changes. Hence, provides better performance to network.**

Index Terms—**Clustering, mobile Ad hoc network (MANET), routing protocols, wireless networks.**

I. Introduction

A collection of wireless nodes that self-configure to form a network without the aid of any established infrastructure is called mobile Ad hoc network (MANET) [1]. They can also be referred as a collection of mobile nodes that intercommunicate on shared wireless channels. Routing messages are an indispensable function of mobile network communications. Each node in MANET can functions as router through which the message passes to reach the destination. Every packet navigates this route from source to destination. Thus, the cooperation from neighboring nodes is vital for secure and authentic communication. Malicious nodes can aim to disrupt this route.

Nodes in MANET are free to join, leave or change their current location. Consequently, we have a network with frequently changing network topology. To cope up with these issues a number of routing protocol with different structures created; flat routing protocols and hierarchical routing protocols. In case of flat routing protocol all nodes are equal in terms of packet forwarding. This results in degraded performances of the protocol when the network size increases. In hierarchical routing protocol fewer nodes known as Cluster-head have outstanding role in packet routing as compared to rest of the nodes. Existing cluster-based routing protocols assume honest cooperation among participating devices. Unlike traditional network this cannot be assured in MANET due to lack of identification and authentication mechanisms. The wireless channel used by mobile nodes is open to all for accessibility. This consequently opens up an easy entry for malicious nodes. Since nodes are mobiles, it is difficult to maintain record of these neighbors behavior. MANETs being dynamic do not define strict margins, which hinder the deployment of policies of security or traffic analysis at particular place. Such vulnerable characteristic of MANET makes it sensitive to attacks. Security in MANET [2], [3] is itself a crucial aspect with its own hindrance because of the vulnerable features of Ad hoc networks and therefore in this paper we are trying to evaluate security issues related to Cluster-head discovery. We propose a cross layer solution to select a more trustworthy Cluster-head node. Our Scheme handles the disconnection as well.

Section 2 discusses the motivation and related study. In section 3, we give a glimpse of the limitations and threats that could arise because of the wrong selection of Cluster-head. We describe and give algorithm of our proposed scheme in section 4. Finally, Section 5 concludes.

II. Related Study

The hierarchical routing is based on clusters. The clusters are the interconnected substructures and this process of dividing the network into interconnected substructures is called clustering. Each cluster can have one or more Cluster-head that acts as a coordinator within the substructure. Each Cluster-head communicates with other Cluster-heads of the network in order to navigate the messages from one group to other. The cluster head needs to manage the cluster activities inside the cluster. The ordinary nodes in cluster have direct

Manuscript received April 30, 2012; revised June 15, 2012.

D. N. Goswami is with S.O.S. in computer Science, Jiwaji University, Gwalior (e-mail: goswamidn@yahoo.com)

Anshu Chaturvedi is with the Deptt. of Computer Applications, MITS, Gwalior (e-mail: anshu_chaturvedi@yahoo.co.in)

access only to cluster head and gateways. The nodes that can hear two or more cluster heads are called gateways [4].

CBRP comes under the category of hierarchical-based routing protocol design [5]. This protocol divides the network area into several smaller areas called cluster. The clustering algorithm of CBRP is Least Cluster Change or LCC [6] means the node with the lowest ID among its neighbor is selected as cluster head. Other nodes residing in the radio range of this cluster head will be the ordinary nodes of that cluster. Since the nodes in ad hoc network are mobile in nature, the mobility of elected cluster head can lead to adverse effect on network performance. Moreover, because nodes with cluster head role consume more power than ordinary nodes, mobile node with lower ID discharge soon. Because of these reasons cluster head election procedure used in CBRP is not suitable

In [7] Core Location-Aided Cluster-based Routing protocol (CLACR) is proposed which comes under the category of location-based-clustering. The routing space is partitioned into square clusters of smaller range on the basis of location information of mobile nodes. It reduces routing overhead and broadcast storm. The number of nodes responsible for routing and data transfer is decreased considerably by the usage of the cluster mechanism. The routing overhead are minimized to the least and route lifetime increases drastically. CLACR computes the path using Dijkstra algorithm in a cluster-by-cluster basis.

In [8] authors have proposed a modified algorithm that uses Weighted Clustering Algorithm (WCA) for cluster formation and Mobility Prediction for cluster maintenance. For cluster formation, initially, a beacon message containing the state of the node is send by each node to notify its presence to its neighbors. Each node builds a neighbor list based on the received beacon messages. The node with the lowest weight is chosen as the CH. The improvement in the weighted clustering algorithm is due to the use of mobility prediction in the cluster maintenance phase.

In [9] researchers have presented a novel clustering algorithm, which guarantees longer lifetime of the clustering structure. The proposed algorithm has a scheme which accurately predicts the mobility of each mobile host based on its neighborhood stability. They have given a weight formula and the mobile host A having the highest weight among its neighbors sends the message CLUSTER HEAD (A) to its neighbors, declaring itself as the Cluster-head. If the mobile host A does not have the highest weight in its neighborhood, it waits for the decision of all the mobile host with higher weight than its own weight and decides its own role.

In [10] authors have proposed a novel clustering algorithm based on neighbor called Incremental Maintenance Clustering Scheme (IMS) for Mobile Ad Hoc Networks. The proposed work is yielding low number of cluster head and cluster member changes. Thus it maintains stable clusters and minimizes the number of clustering overhead.

In [11] authors have proposed an efficient clustering algorithm based on power. They have proposed a new clustering algorithm, which enable stable clustering architecture. A bottleneck node is defined to be a node with battery power lower than a predefined value. The proposed clustering algorithm is based on the assumption that if the clustering architecture has fewer bottleneck then the cluster heads have a longer lifetime.

III. Limitations And Threats

There are numerous algorithms and enhancements that can be found in cluster based routing protocols, yet none of them tackles the issue of security to the best of our knowledge. The algorithms assume honesty and cooperation from the participating nodes. Now if we eliminate the assumption that all the nodes are non malicious, co-operative and trustworthy and evaluate the situation, we find that there is a chaos in the network. The negative side of above mentioned scheme is that none considers the issue of selfishness, maliciousness and security, which predominantly affect the performance of Ad hoc network. The primary structure of ad hoc network is such that we actually cannot believe all participants. Consequently, in an environment like Ad hoc network we cannot put aside these issues. Hence, we propose a solution to such problems. Henceforth, we first analyze the situations once again with no assumption about all the nodes and discuss the threat that could arise. Our work mainly handles the malicious behavior of a node, therefore we only discuss what threats can occur because of the malicious behavior only.

A. Threat in Cluster Based Architecture

As discussed above, in cluster-based routing all the nodes of the cluster rely on Cluster-head node for route discovery and management. So, if the Cluster-head node behaves maliciously, the whole route discovery and maintenance mechanism will cripple.

When a Cluster-head node turns malicious,

- It can accept to route requests but may not respond.
- It accepts the route information from other Cluster-heads and nodes but don't respond.
- It selectively responds to various requests not to all.
- Does not update the routing list and cache on reconnections.
- It may disconnect whenever it wishes without taking consideration for ongoing connections.
- It may tamper with the messages by deleting legitimate services, inserting bogus messages or by making alterations in the existing messages.
- It can lead to repudiation, i.e. denying performing some particular task in question
- There can be information disclosures by Cluster-head node.
- The Cluster-head node can lead to Denial of Service attack as it possesses the authority to allow or disallow services.
-

IV. Proposed Model

Apart from the aforesaid threats there are certain additional problems in the cluster-based hiearachical model. They are:

- All the nodes including the Cluster-head nodes are mobile.
- The Ad hoc networks are not based on any fixed infrastructure.
- The non-Cluster-head nodes rely on Cluster-head node for the services.
- Above all, the Cluster-head can be a malicious node anytime as discussed above.

So certain measures should be considered to handle the problems associated with cluster-based/hierarchical paradigm. Our scheme proposes a cross layer integration approach to enhance the efficiency and security of Cluster-head selection. We emphasize that when a node claims to be a Cluster-head, then there should be some restrictions to be put on it i.e. any node in MANET must possess certain credentials to become a Cluster-head. These could include the minimum trust level as obtained from network/transport layer of the neighbors, the battery life remaining etc. We have routing algorithms at network layer which work on the basis of trust level being enhanced when the nodes are cooperative [12] and forward the packets regularly. At the other end nodes not forwarding the packets properly are black-listed. So this information can be used by nodes to elect any Cluster-head. Our cross layer mechanism is on the one hand choose an efficient Cluster-head, whereas on the other hand also handles disconnection. For selecting a Cluster-head, the condition is that a node wanting to be a Cluster-head must have a threshold value for trust which it should advertise. We can collect the trust values from neighbors for that particular node and calculate the trust average then. Also, its battery life remaining can lead us to choose those Cluster-heads, who can be connected for more time.

Now for disconnections, we believe that if the nodes are not malicious as assured through trust level, then the disconnections could be either due to battery life depleting or due to mobility of the nodes. Hence, we handle such disconnections again using information from the lower layers. To handle the registry/de-registry due to mobility of Cluster-head, we propose that whenever a Cluster-head needs to move out of a particular location or network, it can pass its subscription list to its neighbors and request them to send this until they find a Cluster-head node to hand over to. Rather this task of searching Cluster-head can be done by Cluster-head periodically or as soon as it faces signal reaching problem with the connected nodes or Cluster-heads. Additionally, the current Cluster-head node when moves out of the predefined area, will instantiate informing those who are registered and give them prior information before disconnecting, giving them time to connect somewhere else or can tell them the newly found Cluster-head to connect to. To handle the disconnections due to battery depletion, we are using the battery life information as requested as credential. The node fulfilling the conditions of minimum threshold values only can be accepted as a Cluster-head. The other nodes also, if disconnecting due to battery life, will also inform the Cluster-head. Now suppose if any malicious node claims its credential at the time of establishment as Cluster-head but do not fulfill that thereafter, then the monitoring neighbors can detect that and warn others which will also decrease it's threshold trust level. Decrease in trust level, will warn the non Cluster-head nodes about the Cluster-head and then they can look for certain other Cluster-head in their area. The assumptions made in our algorithms are that

- Every node is capable of becoming a Cluster-head.
- Every node is having a unique identification number.
- The algorithm for Cluster-head selection, Disconnection handling runs at every node.
- Mainly the disconnections are due to battery depletion and mobility once trust is assumed.
- The ad hoc network is set up within a particular geographic area say a site of calamity or military etc.
- Mobility means going out of this area.

Variables used in the algorithm

-role (i): the role currently played by any node i.
-ID (i): Identification number of any node I.
-t-rand (i): Random timer value at any node i.
-NIDB: neighbor information data base maintained at every
node,
tth - threshold value of trust
tavg- average of trust values collected from different neighbors
p- Battery power remaining for node
TReq- request for trust
CrdReq- request for credential
CrdRep- reply for credential

Secure Cluster-head Choice Algorithm ( )

{
Node i when receives a Clus-headAdv from node j
Node i Broadcast TReq to it's one hop neighbors and Unicast
CrdReq to j
Set timer=t-rand
Starts receiving CrdRep (p) from j and t values from neighbors until t-rand expire
Finds tavg taking average of trust values collected from
different neighbors
If(tavg > tth && p>50%)
{if node i wish to provide services i.e. is a cluster-head
{Set role(i)= neighbor-cluster-head(j)
Send ClusReg
Set neighbor-Cluster-head(i)=node j}
Else if (node i wish to request service i.e. is an ordinary node)
{set role(i)=subscriber
Send SrvReq
Set Cluster-head(i)=node j}
Else
Set role(i)=none

}
Else if(tavg> tth && p<.50%)
{if node i wish to provide services i.e. is a cluster-head
{Set role(i)= neighbor-cluster-head(j)
Send ClusReg
Set temporary Cluster-head(i)=node j
}
Else if (node i wish to request service i.e. is an ordinary node)
{set role(i)=subscriber
Send SrvReq
Set temporary Cluster-head(i)=node j
}
Else
{Set role(i)=none}
Repeat Secure Cluster-head Choice Algorithm to look for new Cluster-head until
{Cluster-head (i) OR neighbor-Cluster-head(i) =node j
delete temporary Cluster-head}
}
Elseif(tavg < tth && p<50%)
{doubtful list=j
Don't respond
}
}
}

Since Cluster-head itself is also a node. It will first run Secure Cluster-head Choice Algorithm to find new Cluster-head and then will disseminate the messages using following algorithm.

Disconnections handling Algorithm ( )

{
node i request for p calling interface module from lower
layer of itself
if (p< 50%) calls SBCA()
{if(role(i)= neighbor-Cluster-head(j))
{Send ClusDReg to node j
}
Elseif(role(i)=Cluster-head)
{ send SrvList/RouteList to new Cluster-head say node j
}
Elseif(role(i)= subscriber)

{send SrvDReg to node j
}
}
}

V. Conclusion

One of the key requirements in an ad hoc network is for nodes to share and utilize each others' resources. To use these resources the nodes in MANET needs to have a knowledge, where these resources are existing in the network. Although much previous research has concentrated on Cluster-head selection in MANETs, not much effort has been made on the security side of Cluster-head selection.

We propose an algorithm which selects a Cluster-head node who is trustworthy enough. Thus we are securing the route discovery and maintenance system. Moreover our scheme handles the disconnections in ad hoc network due to the effects of topology changes. Our algorithm put forward an effective cross-layer approach that integrates Cluster-head discovery and selection functionality with network ad hoc routing mechanisms and the lower layer drivers built-in the system. This scheme allows clients to switch to better Cluster-head nodes as network topology changes. Hence, provides better performance to network. We suggest solution to disconnection due to battery depletions for all nodes.

References

[1] A. Dana, A. M. Yadegari, M. Hajhosseini, and T. Mirfakhraie, "A Robust Cross-Layer Design of Clustering-Based Routing Protocol for MANET," *ICACT*, pp. 1055-1059, 2008.

[2] D. Gollmann, "Computer Security. John Wiley and Sons," West Sussex, England, 2nd edition 2005.

[3] A. Mishra and K. M. Nadkarni, "Security in Wireless Ad hoc Networks. In Ilyas, M., editor," The Handbook of Ad hoc Wireless Networks, *CRC Press, Boca Raton, FL, USA*, Chapter 30, pp. 30.1–30, 2003.

[4] R. Agarwal and M. Motwani, "Survey of clustering algorithms for MANET," *International Journal on Computer Science and Engineering*, vol. 1, no. 2, pp. 98-104, 2009.

[5] M. Jiang, J. Li, and Y. C. Tay, "Cluster Based Routing Protocol," IETF *Draft*, 1999.

[6] C. C. Chiang, H. K. Wu, W. Liu, and M. Gerla, "Routing in clustered multi-hop mobile wireless networks with fading channel," in *Proceedings of IEEE Singapore International Conference on Networks (SICON '97)*, pp. 197-211, 1997.

[7] T. F. Shih and H. C. Yen, "Core Location-Aided Cluster-Based Routing Protocol for Mobile Ad hoc Networks," *WSEAS Transactions on Communications*, vol. 5, no. 9, pp. 223-228, 2006.

[8] S. Muthuramalingam, R. R. Ram, K. Pethaperumal, and V. K. Devi, "A Dynamic Clustering Algorithm for MANETs by modifying Weighted Clustering Algorithm with Mobility Prediction," *International Journal of Computer and Electrical Engineering*, August, vol. 2, no. 4, pp.709-714, 2010.

[9] C. Konstantopoulos, D. Gavalas, and G. Pantziou, "Clustering in mobile ad hoc networks through neighborhood stability-based mobility prediction," *The International Journal of Computer and Telecommunications Networking*, vol. 52, no. 9, pp. 1797-1824, 2008.

[10] N. S. Yadav, B. P. Deosarkar, and R. P. Yadav, "A Low Control Overhead Cluster Maintenance Scheme for Mobile Ad hoc Networks (MANETs)," *International Journal of Recent Trends in Engineering*, vol. 1, no. 1, pp-100-104, 2009.

[11] P. R. Sheu and C. W. Wang, "A Stable Clustering Algorithm Based on Battery Power for Mobile Ad hoc Networks," *Tamkang Journal of Science and Engineering*, vol. 9, no. 3, pp. 233-242, 2006.

[12] P. Michardi, *Cooperation enforcement and network security mechanisms for mobile ad hoc networks*, 2004.