Cluster Based Certificate Revocation Scheme in Mobile Ad Hoc Networks

Megha R Jarang
Department of Information Technology,
Sinhgad College Of Engineering, Pune
Pune -411041, India.
Email: jarangmegha@gmail.com

Prof M V Nimbalkar
Department of Information Technology,
Sinhgad College Of Engineering, Pune
Pune -411041, India.
Email: mvnimbalkar.scoe@sinhgad.edu

***Abstract*— Mobile ad hoc networks (MANETs) have attracted more attention due to their mobility and simplicity of arrangement. However, the wireless and dynamic nature renders them more suspicious to various types of security attacks than the wired networks. To meet these challenges, certificate revocation is an important component for secure network communications. Certificate revocation is used to segregate attackers from participating in network activities in future. A Cluster-based Certificate Revocation scheme is the best scheme used to revoke the certificates of malicious node present in the network. It plays an important role in detecting the falsely accused nodes within the cluster and recovoke their certificates to address the issue of false accusation. To improve the reliability of this scheme, warned nodes are recovered to take part in the certificate revocation mechanism. To enhance accuracy, a threshold-based mechanism is proposed to evaluate and confirm warned nodes as legitimate nodes or not, before recovering their certificate.**

Keywords- ad hoc networks (MANETs), security and certificate revocation

I. INTRODUCTION

Recently mobile ad hoc networks (MANETs) have received increasing attention, due to their dynamic topology, mobility feature, and ease of deployment. MANET is a highly flexible network without infrastructure which is formed by a number of self-organized mobile devices like cell phones, laptops and Personal Digital Assistants (PDAs). Another problem with MANET is that open network environment in which nodes can join and leave the network without any restriction. This leads MANET more susceptible to different types of security attacks than wired network. Certificate management [13] is a widely used mechanism in MANET which provides trust in a public key infrastructure, to secure the applications and network services. For certificate management, a complete security solution [4] consists of three components, prevention, detection, and revocation. To secure many network communications and services, certification process is very important. Many research efforts are made to detect malicious attacks on the network. If any attack is identified, Certificate of attacker node is revoked which plays a major role in enlisting and removing the certificates of nodes which are found to launch attacks on the neighborhood in the network. This helps in removing malicious nodes from the network and blocks them from all its activities in the network. Certificate revocation's basically aimed at providing secure communications in MANETs. In Cluster-based Certificate Revocation scheme, [1] has ability to enhance the performance of MANET in which topology is constructed as clusters and each cluster consists of a Cluster Head and some Cluster Members (CMs) located within the transmission range of the cluster Head. Before joining the network, nodes have to take a valid certificate from the Certification Authority (CA). CA distributes and manages certificates [12] of all nodes present in the network. The CA maintains two list as warning list and black list which are used to hold information of accusing nodes and accused nodes and updates these two lists regularly.

II. RELATED WORK

In this section survey on some of the clustering and certificate revocation scheme is done,

A. Various Clustering Methods

MANETs raise new challenges when they are used in large scale network that contain a large number of nodes. Many clustering algorithms have emerged to address this problem. Some of these are as follows

1. Identifier Neighbor Based Clustering

In identifier neighbor based clustering, a unique ID is assigned to each node. Each node in the network knows the ID of its neighbors. The cluster head is selected based on criteria involving these IDs such as the lowest ID, highest ID...etc.

Chen et al proposed an algorithm [15] that constructs k-hop clusters by generalizing the scheme. Nodes initiate the clustering process by flooding requests for clustering to all the other nodes. Each node has to know its k-hops neighbors. All nodes whose ID is lowest among all their k-hop neighbors broadcast their decision to create clusters to all their k-hop neighbors and becomes CHs. However, the cluster heads can become bottlenecks and consume their resources faster than other nodes.

2. Energy based Clustering

The battery power of node is a constraint that affects directly the lifetime of the network, hence the energy limitation poses a severe challenge for network performance. CH performs special tasks such as routing causing excessive energy consumption.

Enhance Cluster based Energy Conservation (ECEC) algorithm [17] is an enhancement of Cluster based Energy Conservation algorithm (CEC). The authors presented a new topology control protocol that extends the lifetime of large ad hoc networks while ensuring minimum connectivity of nodes in the network, the ability for nodes to reach each other and conserve energy by identifying redundant nodes and turning their radios off. During cluster formation phase, nodes with the highest estimated energy values in their own neighborhoods are elected as CHs. After CHs election process, ECEC then elects gateways to connect clusters. It is shown in [17] that ECEC reduces power consumption which leads to a longer network lifetime. However, this scheme exchanges more overhead to elect the CHs and getaways.

B. Certificate Revocation Schemes

To enhance the network security a number of certificate revocation techniques have been discussed in the literature. There are mainly two existing approaches for certificate revocation, which are basically classified into two categories: voting-based mechanism and non-voting-based mechanism.

1. Voting-Based Mechanism

The voting-based mechanism is defined as the means of revoking a malicious attacker's certificate through votes from valid neighbouring nodes. URSA [6] proposed by Luo et al. uses a voting-based mechanism to evict nodes. The certificates of newly joining nodes are issued by their neighbours. The certificate of an attacker is revoked on the basis of votes from its neighbours. In URSA, each node performs one-hop monitoring, and exchanges monitoring information with its neighbouring nodes. When the number of negative votes exceeds a predetermined number, the certificate of the accused node will be revoked. Since nodes cannot communicate with others without valid certificates, revoking the certificate of a voted node implies isolation of that node from network activities. Determining the threshold, however, remains a challenge. If it is much larger than the network degree, nodes that launch attacks cannot be revoked, and can successively keep communicating with other nodes. Another critical issue is that URSA does not address false accusations from malicious nodes. The scheme proposed by Arboit et al. allows all nodes in the network to vote together. As with URSA, no Certification Authority (CA) exists in the network, and instead each node monitors the behavior of its neighbours. Since all nodes are required to participate in each voting, the communications overhead used to exchange voting information is quite high, and it increases the revocation time as well.

2. Non-Voting-Based Mechanism

In the non-voting-based mechanism, a given node deemed as a malicious attacker will be decided by any node with a valid certificate. Clulow et al. proposed a fully distributed "suicide for the common good" strategy [7], where certificate revocation can be quickly completed by only one accusation. However, certificates of both the accused node and accusing node have to be revoked simultaneously. In other words, the accusing node has to sacrifice itself to remove an attacker from the network. Although this approach dramatically reduces both the time required to evict a node and communications overhead of the certificate revocation procedure due to its suicidal strategy, the application of this strategy is limited. Furthermore, this suicidal approach does not take into account of differentiating falsely accused nodes from genuine malicious attackers. As a consequence, the accuracy is degraded.

III. CLUSTER-BASED CERTIFICATE REVOCATION SCHEME

A cluster-based revocation scheme can quickly revoke attacker nodes upon receiving only one accusation from a neighboring node. The scheme maintains two different lists, warning list and blacklist, in order to protect against malicious nodes to take part in framing other legitimate nodes. Also, by adopting the clustering architecture, the cluster head can address false accusation [8] to revive the falsely revoked nodes. The main focus will on the procedure of certificate revocation once a malicious attacker has been identified, rather than the attack detection. Each node is able to detect its neighboring attack nodes which are within one-hop away. CCRVC has ability to enhance the performance of MANET [5]. In this scheme, topology is constructed as clusters. A cluster consists of a Cluster Head (CH) and Cluster Member (CM) nodes within its transmission range. There is a central Certification Authority (CA) which issues the valid certificate to each node. Nodes having a valid certificate are allowed to join the network. The CA maintains and updates two lists regularly, one as Warned list and another as Black lists that holds information of accusing and accused nodes where BL is composed of fully revoked nodes. Initially the WL contains both the accusing and accused node of the cluster, where as the nodes in the WL are analyzed to detect the attacker node in cluster and revoked completely from the network and stored in the BL.

System Architecture

The system involves the different steps in the proposed Cluster-based Certificate Revocation scheme. The entire process is summarized in the fig.4.1 which gives an idea about the proposed method.

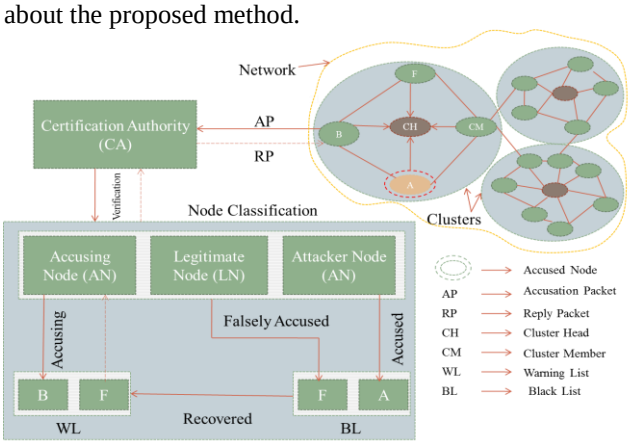

Fig 1. System Architecture

The scheme can be constructed in three different modules as follows.

The CCRVC scheme can be studied in three different steps as follows.

1. Cluster Construction
2. Certification Authority Function
3. Certificate Revocation

1. Cluster Construction

Nodes arrange themselves to form the clusters, along with a CH and some of the cluster members. Using various clustering algorithms [11], [12], CH can be selected. Fig.1 shows an example of how clusters are constructed in the system. By constructing such clusters, each CH can be aware of false accusation against any CM nodes. To maintain clusters, CH and CM nodes continuously confirm their existence by exchanging messages among all the nodes within the network. CH periodically broadcasts CH Hello Packets to all the CM nodes within its transmission range and each CM replies to the CH with the CM Hello Packet [10].

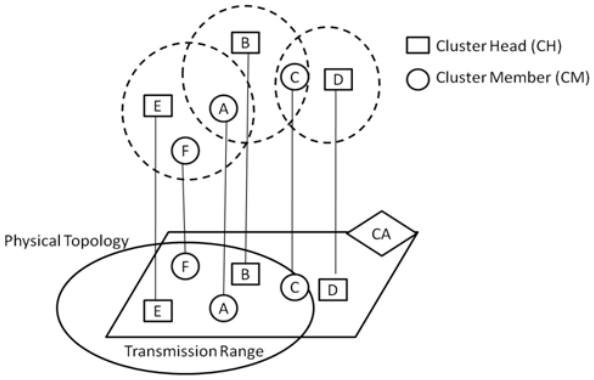

Fig 2. Clustering of Nodes

Here a weight based clustering algorithm is used for the construction of cluster, which is discussed below in details.

a. Weight Based Clustering

Weight based clustering is divided into three sections. section I includes cluster head selection procedure, in section II cluster formation technique is described. In last section data communication procedure is discussed.

i. Cluster Head Selection Procedure

In cluster head selection procedure we have to calculate weighted factor for each and every node using following parameters: such as highest degree heuristic (HD), Less Mobility Factor and Large Transmission Range

Highest Degree Heuristic:

Nodes broadcast a req_msg {Nod_id, Nod_Posn, Msg_ID, Info, Tm_stmp} message to all its neighbors. By using the unique identifier a neighbor node can uniquely identify the message and can understand if it is a new message or duplicate message. After receiving this req_msg {snd_nod_id, snd_nod_pos, recv_nod_id, msg_id, ack_id, Tm_stmp} message, each neighbor node sends a rep_msg mentioning its own position at time instance. After time instance sender node stores all information received from its neighbors. According to above technique nodes having maximum neighbors are termed as the highest degree node i.e. HD

Less Mobility Factor:

Mobility means the rate of change of position of mobile node with respect to time. Nodes which travel at high speeds send update packets more frequently. This leads to

$$M_p \infty\ O_n \ \ldots\ldots\ldots\ldots\ldots\ldots\ldots (i)$$

Where Mp is mobility of particular node at particular time, On is overhead for maintaining information of particular node. Thus from equation (i), we can conclude that in order to minimize the overhead of maintaining information about each node, only the node with less mobility has to be considered. Mobility can be computed by using the following equation.

$$M_p = \frac{1}{T\sum^{T}\sqrt{((X_t - X_{t-1})^2 + (Y_t - Y_{t-1})^2)}} \ldots\ldots\ldots\ldots\ldots (ii)$$

Transmission Range:

After receiving the rep_msg{Nod_ID, Nod_Posn, Msg_ID, Info, Tm_stmp} message, sender node can calculate the distance from its neighbours node to itself the node from which last acknowledgement has come will be maximum distant node. By using the coordinate system the distance between sender node and neighbor will be calculated as

$$d = \sqrt{\{(X_a - X_b)^2 + (Y_a - Y_b)^2\}} \ldots\ldots\ldots\ldots\ldots (iii)$$

The transmission range of a node will be calculated as,

$$TR_p = \pi * d^2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots (iv)$$

By using these parameters, cluster head selection has been made, degree, node mobility and transmission range is calculated for each and every mobile node. The main objective of cluster based algorithm is to reduce overhead of communicating with each and every node. For these we have assigned highest priority to large transmission range least priority is assigned to less mobility factor [1]. The algorithm is defined below

Cluster Head Selection Algorithm

Step 1. *Identify node with highest degree, less mobility and larger transmission range individually.*

Step 2. *Taking highest value as 100% individually, find out the percentile value of all nodes in different characteristics.*

Step 3. *Identify such nodes which have percentile value between 80 to 100 percent*

Step 4. *Find out such nodes which intersect the value in all three conditions of HD, LMF and LTR.*

Step 5. *Calculate weighted sum*

$$Wp = \{(w1 * HDp) + w2 * LMF(Mp) + w3 * LTR(TRp)\}$$

Step 6. *End*

The node with highest weighted sum is selected as cluster head.

ii. Cluster Formation Technique

Every cluster head maintains a priority list {clsr_Hd_ID, Ngh_Nod_Id,Nigh_Type,Own_Clsr_Mem_ID,Tm_Stmp} a routing table and a counter which counts number of its cluster members. Every node maintains the same counter and has the capacity of handling nodes up to ceiling of twice of its transmission range. The counter only enabled when the node selected as cluster head. After selected as cluster head it has to maintain information about its cluster member s. this technique is described on the following algorithm.

Cluster Formation Algorithm

Step 1. *Cluster head broadcasts membership message*
Step 2. *Counter is set to 0*
Step 3. *Do*
Receive a reply from a node
Counter = counter + 1
Step 4. *Node is added as member of the corresponding cluster.*
Step 5. *End*

iii. Communication Procedure

In this section we have described how communication takes place among different clusters.

Cluster Head Communication Algorithm

Step 1. *CH broadcast a request message.*
Step 2. *Nodes within its communication range receive this message.*
Step 3. ***if***
receiver node is cluster head, then send acknowledgement message
else if
any other cluster member receives this broadcast message Then it redirects. This message to its cluster head.
else
node of the same cluster receives the message, Then it search for another cluster head within its range and act as common gateway between these two clusters
Step 4. *End.*

By using above discussed algorithm any node can communicate with others.

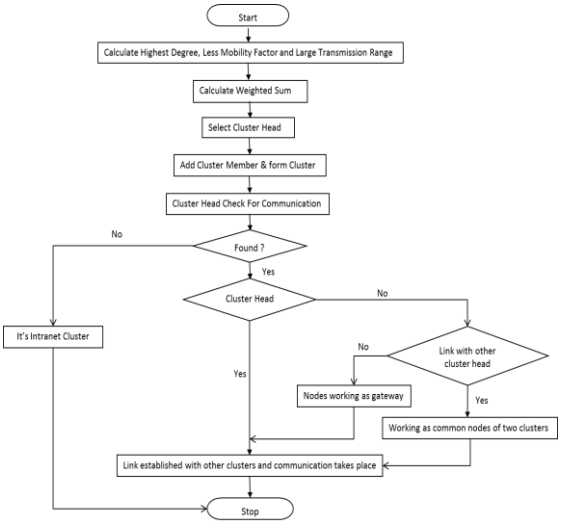

Fig 3. Weight based clusturing algorithm

2. Certification Authority Function

Certification Authority (CA) is deployed in the cluster-based scheme, to distribute certificates among all the nodes. The CA is also responsible for revocation of malicious nodes certificate and maintains WL and BL for accusing and accused node. The CA updates each list periodically according to the received control packets. Nodes can be classified into three types as: A legitimate node is a normal node in the network which is deemed to secure communication with other nodes and is able to correctly detect attacks from malicious attacker nodes and accuse them positively and for revoking their certificates. A malicious node does not execute misbehavior identifying protocols. An attacker node is a special malicious node which can launch attack in the network and disrupt the secure communication.

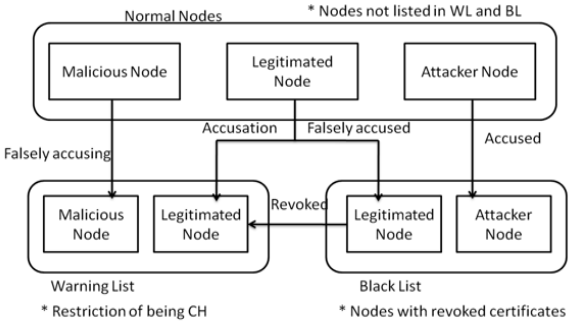

Fig. 4. Classification of Nodes

Classification of the nodes is shown in fig. 4. Based on the reliability, nodes can be further classified into three categories as: normal nodes having a high reliability, warned nodes, suspected as potential attackers, and revoked nodes, accused by a normal node. Newly node joining the network is assumed to be normal node. Warned nodes and revoked nodes are listed in the Warning List (WL) and Black List (BL), respectively. Certificates of the nodes which are listed in the BL are revoked and removed from the network.

3. Certificate Revocation

Certificate revocation procedure mainly focuses on revoking the certificate of malicious node and dealing with falsely accused node to recover them as normal node in the network, which is described below:

a. Revoking Certificate of Malicious node

The revocation procedure [1] [2] begins at detecting the presence of attacker node. When the neighboring nodes in the network detect attacker node and each node sends out an accusation packet against the attacker node to the Certificate Authority (CA).

The procedure for certificate revocation is described below with the example, when a malicious attacker A launches attack within one-hop range as shown in following fig. 5.

i. Node A is a malicious node and is responsible to launch attack on its neighboring nodes B, C, D and E.
ii. Each of the neighboring nodes detects the attacks and sends an accusation packet to the CA against attacker node A. After receiving the first packet from node B, CA holds node B into WL as an accuser node and node A into the BL as an accused node.
iii. CH updates its WL and BL and determines that one of the node was framed.

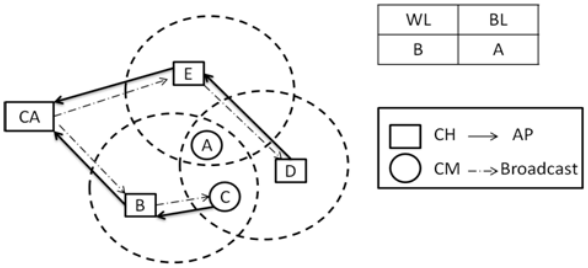

Fig. 5. Revoking a node's certificate

b. False Accusation

If the CH does not detect any attacker node from the accused nodes enlisted in the BL from the CA, CH becomes aware of the occurrence of false accusation [8] and sends a recovery packet to the CA in order to vindicate the node, which causes release of the falsely accused node from the BL and held it in the WL. This information is propagates to all the nodes through the network by CA . Fig .6 shows the process of addressing false accusation as below.

i. CA broadcasts the information of WL and BL throughout the network.
ii. Node E and D which are CH of node A update their WL and BL, and determine that node A was framed as accused node.
iii. E and D send a recovery packet to the CA to recover the certificate of falsely accused node A.
iv. After receiving the first recovery packet from node E, the CA removes the falsely accused node A from the BL, and held it into the WL along with node E.
v. All the nodes will update their WL and BL and the certificate of node A will be recovered.
vi. CA broadcast the revocation message to all the nodes present in the network.
vii. Each Node in the cluster updates their local WL and BL to revokes certificate of node A.

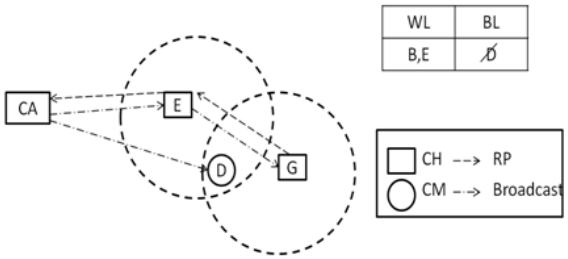

Fig. 6. False accusation

IV. CONCLUSION AND FUTURE WORK

In this paper, a major issue to ensure secure communications for mobile ad hoc networks, namely, certificate revocation of attacker nodes is addressed. In contrast to existing algorithms, we propose a cluster-based certificate revocation scheme combined with the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate and solve the problem of false accusation. The cheme presents the Revocation based on clustering and scheme addresses a major issue to ensure secure communications for mobile ad hoc networks by revoking the certificate of attacker node. A cluster-based certificate revocation with vindication capability scheme combines the merits of both voting-based and non-voting based mechanisms to revoke malicious certificate promptly and also solve the problem of false accusation. Certificate revocation of an accused node is based on a single node which reduces the revocation time in comparison with the voting-based mechanism. Also the cluster model restores the falsely accused node by the CH, which results in improving the accuracy as compared to the non-based mechanism.

The future work focus on the scheme to become more effective and efficient in revoking certificates of malicious attacker nodes by reducing revocation time and improving the accuracy and reliability of certificate revocation scheme.

REFERENCES

[1] Wei Liu, Nei Kato, "Cluster-based Certificate Revocation with Vindication Capability for Mobile ad hoc Networks", IEEE Transactions on Parallel and Distributed systems, vol.24, no.2,doi: 10.1109/TPDS.2012.85. February 2013.

[2] Jane Y.Yu, H. J. Chong, "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", IEEE Communication Surveys, Volume 7, No 1, 2005.

[3] K. Kiruthiga, B. Lakshmipathi, K. Prem, Preetha M. Kurup, "Cluster Based Certificate Authentication for Mobile Ad hoc Network", International Conference on Simulation in Computing Nexus (ICSCN), ISBN : 978-93-83060-45-0, 20-21 March, 2014.

[4] Hao Yang, Haiyun Luo, Fan Ye, Songwu Lu, And Lixia Zhang, ”Security In Mobile Ad Hoc Networks: Challenges And Solutions”, IEEE Wireless Communications, 1536-1284/04, February 2004.

[5] S.Herman Jeeva, D.Saravanan, RM.Chandrasekaran, “Enhancing Security in MANET using CCRVC Scheme”, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801, Vol.2, Special Issue 1, March 2014.

[6] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang, “URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks,” IEEE/ACM Trans. Networking, vol. 12, no. 6, pp. 1049-1063, Oct. 2004.

[7] J. Clulow and T. Moore, “Suicide for the Common Good: A New Strategy for Credential Revocation in Self-organizing Systems,” ACMSIGOPS Operating Systems Rev., vol. 40, no. 3, pp. 18-21, July 2006.

[8] K. Park, H. Nishiyama, N. Ansari, and N. Kato, “Certificate Revocation to Cope with False Accusations in Mobile Ad Hoc Networks,” Proc. IEEE 71st Vehicular Technology Conf. (VTC ’10), May 16-19, 2010.

[9] R. PandiSelvam, V.Palanisamy, “Stable and Flexible Weight based Clustering Algorithm in Mobile Ad hoc Networks”, IJCSIT, Vol. 2 ,824-828, 2011.

[10] Soumyabharat Saha, SuparnaDas Gupta, “Weight Based Hierarchical Clustering Algorithm for Mobile Ad Hoc Networks”, doi:10.1016/j.proeng.2012.06.137,Published by Elsevier, 2012.

[11] Vincent Bricard Vieu, Nidal Nasser, “A Weighted Clustering Algorithm Using Local Cluster-heads Election for QoS in MANETs”, Published in IEEE GLOBECOM, 2006.

[12] Y. Dong, Ai-Fen Sui, “Providing distributed certificate authority service in cluster-based mobile ad-hoc networks”, Elsevier, DOI: 10.1016, 2007.

[13] Jayanta Biswas, S.K. Nandy, “Efficient Key Management and Distribution for MANET”, Published in IEEE ICC, 1-4244-0355-3, 2006.

[14] Abdelhak Bentaleb, Abdelhak Boubetra, Saad Harous, “ Survey of Clustering Schemes in Mobile Ad hoc Networks”, Scientific Research,doi:10.4236/cn.2013

[15] G. Chen, F. G. Nocetti, J. S. Gonzalez and I. Stojmenovic. “Connectivity Based k-Hop Clustering in Wireless Networks,” 5th HICSS, 2002.

[16] M. Gerla and J.T. Tsai. “Multicluster, Mobile, Multimedia Radio Network. Wireless Networks,” 1995.

[17] Ya Xu, S. Bien, Y. Mori, J. Heidemann, D. Estrin, “Topology Control Protocols to Conserve Energy in Wireless Ad Hoc Networks,” CENS Technical Report , 2003.