Research Paper

Volume : 3 | Issue : 3 | March 2014 • ISSN No 2277 - 8179

Propelling Security by Secure Cluster Formation and Certificate Revocation in Manets

Computer Science

KEYWORDS :Mobile Ad Hoc Network, Certificate Revocation, threshold, Node Verification, Fuzzy Relevance Degree

AMBARISH A. Department of Computer Science, Nehru Institute of Technology, Coimbatore.

GOWTHAMANI R. Deprtment of Computer Science, Nehru Institute of Technology, Coimbatore

ABSTRACT

Mobile ad hoc networks (MANET) are infrastructure less one where there is no architecture. There will be security concerns in MANET since it is an open environment. Certificate revocation scheme addresses a lot of security issues in MANETs. It follows a technique of revoking the certificate of the nodes that are considered to be malicious. Once the certificate is revoked, the node is free and can't take part in any of the communications in the network. In order to enhance the security the threshold based mechanisms are used in the cluster to vindicate warned nodes from the legitimate nodes. In this paper we are building on the certificate revocation scheme, to make the cluster secure by choosing the cluster head effectively. The security is being enhanced by the proper selection of cluster head using Fuzzy Relevance Degree. In a given cluster, the cluster head monitor their Cluster Members and watch for the accusations by means of node position or node verification algorithms. The proposed work is focusing on the selection of cluster head using Fuzzy Relevance Degree in a MANET by considering the parameters additional to the normal one. The parameters include the distance, the degree called FRD, the velocity by which the nodes are moving and the distance between them.

INTRODUCTION

With the advancement of wireless technology, mobile communication becomes popular in recent years. A lot of increasing attention is going on the research of mobile distributed computing. A mobile ad hoc network is a collection of nodes with no infrastructure and these nodes are connected with wireless communication. Also, the topology of the ad hoc network is dynamically changing and the nodes of the ad hoc network are often mobile. The ease of mobility within the network is a major advantage in mobile ad hoc networks. In addition to the mobility, mobile devices cooperate and forward packets for each other to extend the limited wireless transmission range. The development in ad hoc networks helps in the creation of on demand network in areas like disaster relief, war field and in emergency communication areas.

A major challenge in the design of mobile ad hoc networks is to protect their vulnerability from security attacks. The certificate revocation scheme plays an important role in ensuring security. There are lots of challenges in ensuring security [1]. Due to the absence of a clear line of defence, a complete security solution for MANETs should integrate both proactive and reactive approaches [2], and encompass all the three components like prevention, detection and reaction. The fundamental vulnerability of MANETs comes from their open peer-peer architecture. The nodes in the MANETs have an additional functionality of forwarding the packets for the other nodes in the network. In wired network there will be dedicated routers to do the packet forwarding. The wireless channel is accessible to both legitimate network users and the malicious attackers. Hence the wireless on demand MANETs are more susceptible to the attacks considering the wired networks

Enabling security, conveying real trust, ensuring integrity etc thus becomes an integral part and certificate revocation scheme provides fundamental solutions to all. Tremendous amount of research work are happening in the field of certificate revocation which includes the certificate distribution [3] [4] from a trusted third party. It almost becomes a prerequisite in mobile ad hoc network. This will make sure that every node joining the network has a trusted third party digital signature. The attack detection [5] [6] [7] [8] is another area of concern in wireless medium since any node can freely join the network at a particular instant of time. In my work, we are focusing mainly on the security issue of MANET and how certificate revocation provides it. I go deeper in to the selection of the cluster head using a different method and compares the performance of the technique which I have used with the existing ones.

My paper is organized as follows: The next section (Section 2) gives you an idea of the current and existing methods in the assurance of security. Section 3 gives the proposed schema used. Then I conclude the paper in the following section. Last section is fully dedicated to the papers which I have refereed to make do my research work.

RELATED WORKS

Researchers pay a whole lot of attention in ensuring the fundamental security of infrastructure less MANETs. Many approaches took centre stage in enabling trustworthiness in certificate revocation. This section I introduce some of the currently used ones like voting based and non voting based mechanisms.

Voting based mechanism

This schema introduces a mechanism where all nodes have to participate in a voting system in order to evict the malicious nodes

Several techniques grew hand to hand in the voting based mechanism. URSA [9] proposed by Luo et al. used a voting system to evict nodes. There will be a certificate authority (CA), who issues the valid certificates. The nodes with the valid certificates are considered to be legitimate. The duty of issuing valid certificates to the newly joining nodes, though lies with their neighbors. A major drawback in this technique is that this schema can't address false accusations from the neighbor malicious nodes.

Arboit et al. [10] in their work put another mechanism allows the nodes in the network to vote together. The basic difference from the Luo et al. is that nodes in network vote with different weights ensuring a larger accuracy. Since every node in network has to participate in eviction of one singe node, the overhead induced is much higher than the other schemas.

Non voting based mechanisms

A single neighbor can detect the presence of a malicious node in the non voting based schema which drew forward the certificate revocation mechanisms

'Suicide for the common good strategy' was one of the first methods in these mechanisms which was proposed by Clulow et al. [11] Here the certificates of both the accusing and the accused nodes will be cancelled, thus forcing one to evict forcefully from the network. The major advantage is that the time and overhead will be reduced considerably. This positive though is cancelled out, as this method can't able to differentiate falsely accused nodes from the genuine attackers.

A cluster based scheme [12] was proposed by Park et al. where a Certificate authority manages control messages. There will be black list and warning list created. The accuser node is put in the warning list and accused node in the black list. The certifi-

cate of the malicious attacker node can be revoked by any single neighboring node. It can also deals with the issue of false accusation that enables the falsely accused node to be removed.

Wei Liu et al. [13] came forward with the technique of revocation with vindication capability and it maintains a threshold value to vindicate warned nodes as legitimate or not, before recovering them.

Motivation

In a cluster based method, the selection of cluster head (CH)[15] [16] is of concern and can act as a major parameter in ensuring security. In the existing method described earlier, a node will proclaim itself as a CH. It propagates CH Hello packet (CHP) to notify neighboring nodes periodically. This selection can become somewhat faulty and in this paper we are using the Fuzzy Relevance Degree to select a CH.

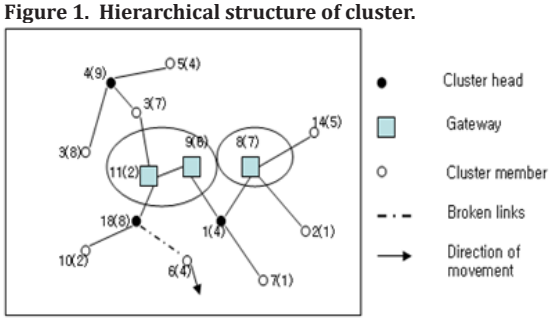
CLUSTER BASED MODEL

In this section, we introduce the model of cluster based on which my work is to be done. Cluster is largely a collection of nodes that are mobile or stationary. The construction of the cluster should be done in a compatible mode, where the work must be done effectively in both mobile and stationary nodes. I made an assumption that the cluster will contain an optimum number of nodes, say 10 to 100. The main aim is to give the cluster head within a cluster to give all the right to revoke the certificate and thus evict the nodes from the cluster. This scheme maintains two lists, the black list and the warning list [6]

Cluster- Basic Idea

Clustering in MANET can be considered as the virtual partitioning of dynamic nodes in the flat structure or distributed network structure into several clusters. Clusters of the nodes in the flat structure or distributed network structure are made with respect to their nearness to each other. Such nodes are considered neighbors when all neighboring nodes are located within their transmission range and set up a bidirectional link between them. Typical algorithms for clustering in the flat structure or distributed network structure are known as one-hop clustering and multi-hop (d-hop) clustering algorithms. In the one-hop clustering, every member node is at most 1-hop distance away from a central node that is called the cluster head. Thus, all member nodes remain at most two hops distance away from each other within a cluster category. On the contrary, in multi-hop clustering, the management of neighboring nodes to the cluster head is performed by allowing the nodes to be presented at most d-hop distance away from each other to form a cluster. A typical MANET cluster structure consists of flat and hierarchical structures. The basic structure of the cluster is given in the Figure 1. This gives an idea of basic cluster structure, where the links in the figure represents the link existing between the nodes. It is a hierarchal one, where gateway that connects the nodes between clusters is represented by shaded rectangular boxes. Within parenthesis the weights of each node is represented. This represented in the figure, provides a complete idea of how the nodes communicate. The gateway represents the channel through which the nodes between the clusters communicate. The cluster head is selected for each of the cluster and the each cluster has only one cluster head. The other nodes in the cluster will represent the cluster members.

Figure 1. Hierarchical structure of cluster.



Sources: www.googleimages .com

Basic cluster formation

The creation of topology is based on the cluster based [14] architecture. Nodes in the ad hoc network join together and form clusters. Each cluster will have an optimal number of nodes. The nodes in the cluster can find the attackers node which are only one hop away from each node. A cluster head (CH) will be chosen from the nodes in a given cluster and the rest of the nodes can be called as cluster members (CM). The CM must stay within the transmission range of the CH. The nodes must obtain a particular certificate from the Certificate Authority (CA) to join the cluster.

In the models existing, the main part in the cluster formation is the cluster head selection. While a node take parts in the network, it is allowed to declare itself as CH with a probability R. The links between the neighbouring nodes are checked efficiently by the usage of neighbour sensing protocols.

Existing neighbor sensing protocol

The periodic broadcast of hello messages are effective protocols used to detect the cluster head in the cluster. These are the one which are used in the existing methods. In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in the range of the CH can accept this packet to participate in this cluster as CM. If the node is deemed to be a CM, it has to wait for the CHP. When the CHP is received it will reply with the CM hello Packet (CMP).

Proposed cluster scheme method

The periodic broadcast of hello messages are effective protocols used to detect the cluster head in the cluster. These are the one which are used in the existing methods. In this model, if a node proclaims itself as a CH, it propagates a CH Hello Packet (CHP) to notify neighboring nodes periodically. The nodes that are in the range of the CH can accept this packet to participate in this cluster as CM. If the node is deemed to be a CM, it has to wait for the CHP. When the CHP is received it will reply with the CM hello Packet (CMP).

List Creation

Creation of list includes the black list creation (BL) and the warning list (WL) creation. The Certificate Authority (CA) is the one in charge of updating both the BL and WL. The WL is used to hold the accusing node information and the BL is used to hold the information of the accused nodes. The CA updates the list according to the control packets it received. Another function of the CA is that it will broadcast the information of WL and BL to the entire network.

Classifying nodes in a cluster

The nodes in the network as such can be classified according to their behavioral pattern as legitimate node, malicious node and attacker node. Nodes that are safe and can't cause any of the security violation are considered as legitimate nodes. The identification of the misbihaviourness is not due to the execution of protocols neither by the malicious node nor by the voting of it. The attacker nodes are the one which can launch the attacks on the network and disrupt the communication.

FUZZY RELEVANCE DEGREE

Usage of FRD algorithm [17][18] helps maintenance of cluster, most probably a secured cluster, and thus maintaining it in a stable state. The stable cluster in terms of energy allows for the easier access and transfer of packets from one secured cluster to the other thus reducing the transfer rate and reduces the effect of topological changes that are happening.

FSV Structure

This FSV (Fuzzy State Viewing) structure is the basis of so called Fuzzy Relevance Algorithm. This is virtually a table like shaped structure given below. This structure consists of five parameters. The importance of FSV comes in the transfer of packets when a node communicates among itself. In other words, when two nodes communicate among each other it will pass an FRD value represented by μ. This μ, ranges from 0 to 1, helps in the

Volume : 3 | Issue : 3 | March 2014 • ISSN No 2277 - 8179

avoidance of interference when two nodes exchange the packets. The secured cluster thus formed will have a cluster head selected according to the proposed FRD algorithm. This subsequently results in the selection of Cluster Members. In order to provide the smooth transfer of packets to and from a gateway node is being selected which helps in the broadcasting of packets.

The parameters of the packet are explained as follows:

1. **Identifier (ID*)*:**
   As mentioned above every node that participates in the cluster will have a unique id. This helps in avoidance of interference and will fasten up the cluster head selection process.
2. **Fuzzy Relevance Degree (μ):**
   Fuzzy Relevance Degree value, μ is used by the nodes in communication process. This value will be send by the corresponding neighbor nodes when participating in communication. The above μ value is determined by the parameters like mobility, distance and power. On the larger context, we take the value of μ in range of 0 to 1. This will be formed as a set where the FRD value can be selected accordingly.
3. **Level:**
   The third parameter in the FSV structure is the level. As we arrange the value into sets, this can be further categorized as low level, middle level and high level. Here after it's the level parameters in the FSV which acts as the criteria in selecting the cluster head, cluster members and the gateway nodes.
4. **M-hop (Multi-hop):**
   Based on the μ value calculated the cluster creation and its management also can be controlled. This is being done by separating the transfer process into multihops ranging from 1-hop to several m-hops. The size of the MANET paves way in selection of multiple hops.
5. **Balance:**
   Every node in the secured cluster must be given an equal chance of making into the election of CH. This fair management must help in the proper allocation of the cluster head in a secured cluster. Thus the parameter balance is used for serving the above function.

Fuzzy Relevance Degree

Every node in the network must possess an FRD value denoted by μ. This helps in the formation of secured cluster with high reliability and optimum transfer of data packets. Fuzzy Relevance Degree value, μ is used by the nodes in communication process. This value will be send by the corresponding neighbor nodes when participating in communication. The above μ value is determined by the parameters like mobility, distance and power. On the larger context, we take the value of μ in range of 0 to 1. This will be formed as a set where the FRD value can be selected accordingly.

The power is given prominent importance in the selection of FRD value. This FRCA (Fuzzy Relevance Clustering Algorithm) will help in maintaining a stable energy by deciding the route or path with minimum energy usage. In other words adequate path will be taken for an efficient energy transmission. There arises another question. Why we need the above strategy? When there occurs a communication between nodes in the MANET, some amount of energy will be lost because of the intra packet features and also because of the distance between nodes. So we need a received signal strength function denoted as RS (xi), that can be used for the further calculations. The path thus selected will be providing with low energy transmission features.

As mentioned we denote function RS (xi) for every node xi to measure its received signal strength. In section I we studied about the dynamic features of MANET. Since the dynamic features holds it place in every possible department there will be a lot of ambiguity arising on the efficient cluster head selection algorithm. This ambiguity we avoided in this paper by the introduction of relevance degree. This μ value enhances the election mechanism and also increases the signal strength by a large margin when two nodes xi and yi communicates in the cluster x and j.

Cluster head selection

The selection process begins now. FRD value that is calculated in the previous stages will be taken into account and the nodes that are having high FRD value will be having the highest priority. That is a node within a cluster having more power and the signal strength, calculated from RS (xi) will be selected as the cluster head. Making it simple, the node must own minimal cost to be considered as a cluster head comparing to all other nodes in the cluster. By using NOTICE_CH_CANDIDATE packet, the new cluster head must notify all its neighboring members. The other members in the cluster will be therefore acting as cluster members, some as gateway nodes.

Cluster Formation

Once cluster head is decided each node advocates itself and checks whether clustering is necessary to stabilise or not. This checking with the neighbouring nodes is done by using some criteria's. The energy must be made stable and also nodes within the cluster must possess similar characteristics. We have given two figures, Figure 3 and Figure 4.

The unmodified or the structure before the cluster formation is given in the Figure 3. The modified scheme is given in the Figure 4. This adds to the fact that clustering can enhance the security. Node within a cluster having more power and the signal strength, calculated from RS (xi) will be selected as the cluster head Clustering is done basically on the two structures given, that are in C2 and C3, in order to maintain a balance with the cluster structure C1. The other combinations like C1-C2 or C1-C3 will result in possible imbalance in the structure, thus being rejected.

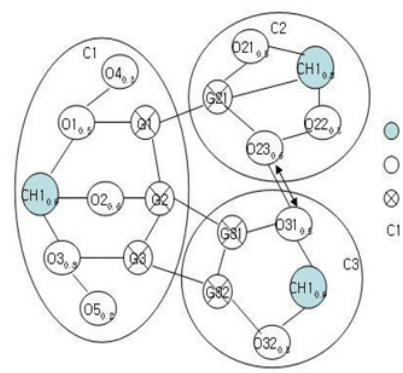


Figure 3. Original Cluster Structure.
Source: www.googleimages .com
The figure below shows the one after clustering.

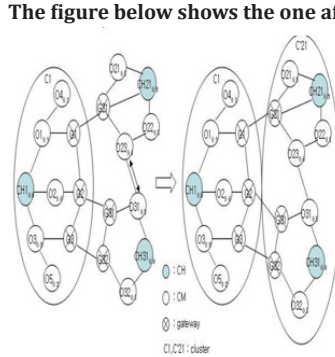


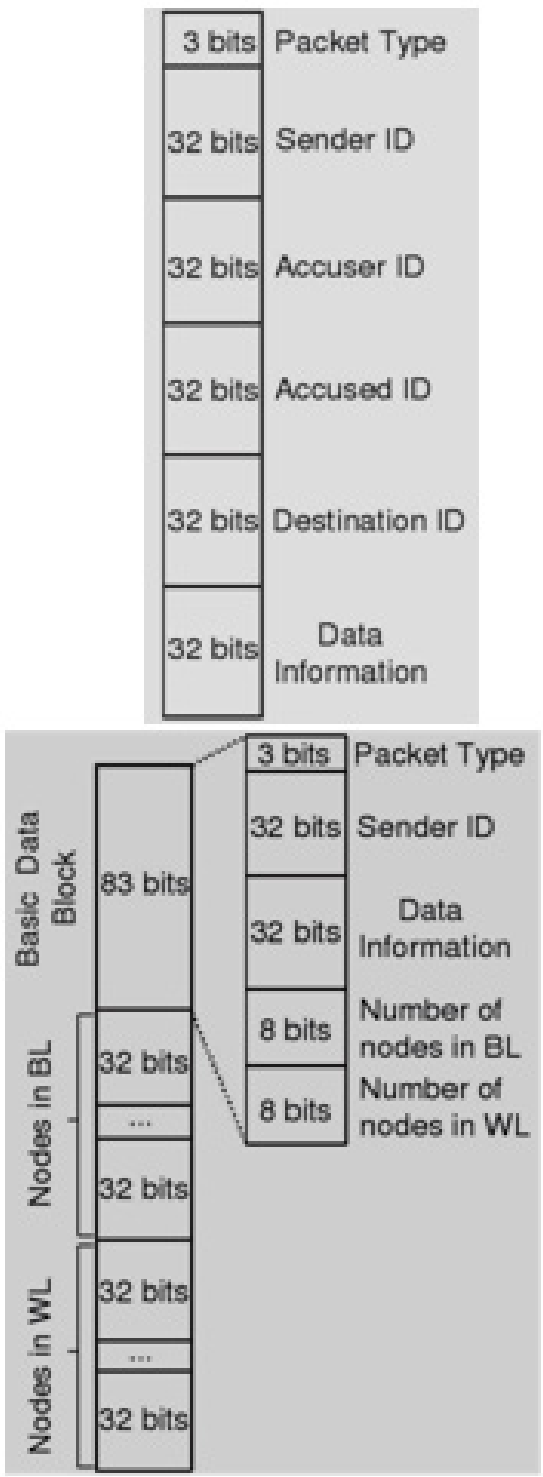
Figure 4. Modified Cluster Structure.
Source: www.googleimages .com

CERTIFICATE REVOCATION

The certificate revocation technique is presented here. Certificate revocation process involves revocation of certificate of malicious nodes thus detecting the attacker nodes presence. There are several challenges arising in this process, such as handling the false accusations, notifying etc. Thus the process is mainly

divided into three stages called by the name accusing, verifying and notifying. In a cluster, the attacker node will launch the attack and the neighboring nodes of the attacker node detect the attacks from the attacker node, say A. The neighboring nodes then send Accusation Packets (AP) to the CA against the attacker node A. CA verifies all the AP, and according to the first received AP, say B, the CA will put B and A in Warning list and in the black list. There is a certificate authority (CA) which helps the Cluster Head in all the processes related to certificate.

Figure 5 shows the format of Accusation Packet and Broadcasting Packet.



Source: www.googleimages .com

The Certificate Authority will use the broadcasting packet to disseminate the revocation messages. Correspondingly every single node in the network updates their Warning and the Black list. Thus revocation of certificate against attacker node A is done. The Figure 5 shows both these packets. The AP has got the fields like Accuser id, Accused id, the source and destination addresses and so on.

For the formation of cluster given in the Figure 4, we use the FRD value denoted by μ. Adequate value will be selected from the set, which will aid in the balancing of the structure using the balance parameters. It also helps in maintaining a fair allocation as well as controlling the management process. Thus we get a secured cluster that have a high transfer rate in terms of the communication between nodes in the MANET. In the figure two clusters communicate effectively by sending packets to and fro. The gateway node is the one responsible in making the communication possible thus having a stable energy occupied in the cluster structure with security prevailing.

CONCLUSION

In this paper, we addressed the basic security of the MANET and how the consideration of Cluster Head impacts the creation of a secured cluster. The existing models emphasis the selection of the cluster head based on the neighbour sensing protocol, just by proclaiming the hello packets. But I considered FRD method in CH selection including various parameters like battery power, life time, the velocity of nodes, the distance between them and also the FRD value. The revocation scheme is basically build up on the existing work of certificate revocation, considering how to revoke the certificates effectively by addressing the problem of false accusation. The efficient selection of cluster head and the revocation process help in the creation of a secure cluster and improve the performance of the network. The usage of network simulator will help in the detection of the enhancement. The overall through put will be increased by the usage and hence be far more efficient.

REFERENCE

[1] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Comm., vol. 11, no. 1, pp. 38-47, Feb. 2004. | | [2] INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies (Volume: 1) | | [3] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002. | | [4] L. Zhou, B. Cchneider, and R. Van Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002. | | [5] P. Yi, Z. Dai, Y. Zhong, and S. Zhang, "Resisting Flooding Attacks in Ad Hoc Networks," Proc. Int'l Conf. Information Technology: Coding and Computing, vol. 2, pp. 657-662, Apr. 2005 | | [6] B. Kannhavong, H. Nakayama, A. Jamalipour, Y. Nemoto, and N Kato, "A Survey of Routing Attacks in MANET," IEEE Wireless Comm. Magazine, vol. 14, no. 5, pp. 85-91, Oct. 2007 | | | [7] H. Nakayama, S. Kurosawa, A. Jamalipour, Y. Nemoto, and N. Kato, "A Dynamic Anomaly Detection Scheme for Aodv-Based Mobile Ad Hoc Networks," IEEE Trans. Vehicular Technology, vol. 58, no. 5, pp. 2471-2481, June 2009. | | | [8] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Network: Analysis & Defenses," Proc. Third Int'l Symp. Information Processing in Sensor Networks, pp. 259-268, 2004. | | | [9] 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. | | [10] G. Arboit, C. Crepeau, C.R. Davis, and M. Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Hoc Network, vol. 6, no. 1, pp. 17-31, Jan. 2008 | . | | [11] 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. | | [12] 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. | | [13] Wei Liu, Student Member, IEEE, Hiroki Nishiyama, Member, IEEE, Nirwan Ansari, Fellow, IEEE, Jie Yang, and Nei Kato, Senior Member, IEEE , "Cluster-Based Certificate Revocation with Vindication Capability for Mobile Ad Hoc Networks" | | [14] J. Lian, K. Naik, and G.B. Agnew, "A Framework for Evaluating the Performance of Cluster Algorithms for Hierarchical Net- works," IEEE/ACM Trans. Networking, vol. 15, no. 6, pp. 1478-1489, Dec. 2007. | | [15] Dai Zhi-Feng,li Yuan-Xiang,HeGuo-Liang Tong Ya-La Shen Xian-Jun,"Uncertain Data Management for Wireless Sensor Networks Using Rough Set Theory",2006 IEEE. | | [16] Ye Tian,Min Sheng,JiandongLi,Yan Zhang,Junliang Yao and Di Tang,"Energy aware Dynamic Topology Control Algorithm for wireless Ad Hoc Networks",2008 IEEE. | | [17] Anitha, V.S.; Sebastian, M.P. SCAM: Scenario-based clustering algorithm for mobile ad hoc networks. In Proceedings of the 2009 13th IEEE/ACM International Symposium on Distributed Simulation and Real-Time Applications, Singapore, October 2009; pp. 97-104. | | [18] Basagni, S.; Mastrogiovanni, M.; Panconesi, A.; Petrioli, C. Localized protocols for ad hoc Clustering and backbone formation: A performance comparison. IEEE Trans. Parall. Distrib. Sys. 2006, 17, 292-306. | |