RESEARCH ARTICLE OPEN ACCESS

# Certificate Revocation Mechanism in Mobile ADHOC Grid Architecture

J.Beschi Raja [1], Dr.S.Chenthur Pandian [2], J.Pamina [3]
Assistant Professor [1],
Department of Computer Science and Engineering
Kalasalingam institute of technology
Principal [2]
SNS College of Technology
Assistant Professor [3]
Department of Computer Science and Engineering
Kalasalingam University,
Krishnankoil, Virudhunagar
Tamil Nadu - India

## ABSTRACT

Mobile network system consists of mobile nodes which are movable in nature. Each node consists of different kind of mobility patterns, energy. This will make it more difficult to form a mobile adhoc network. To overcome this grid architecture has been initiated. The main concept behind grid architecture is the sharing of resources within the same network. Thus assigning resources for each device will greatly reduce the load of the network. The mobility of nodes is resolved by careful determination of stability time and position of mobile nodes. In addition to that security is another major concept behind mobile nodes. Since they are mobile nodes it's very easy for the intruders to make the system unavailable to the network system. Certification revocation mechanism is the backbone for the system to be free from malicious attackers. Whenever the network detects the malicious nodes inside the grid architecture it will revoke the certificate of the node in order to remove that node from the network. Falsely accused nodes are get back to the network using the false accusation method. The outcome will be a grid architecture which is free from attacks.

***Keywords:***— Mobileadhoc grid,Mobility, Attackers, Certificate revocation

## I. INTRODUCTION

In a mobile ad hoc network (MANET) [8], a group of mobile nodes will cooperate together in order to tranform information between them. The beauty of Manets is they don't need a specific centralized head known as the central authority. Each and every node can act as both sender and receiver.

Mobile grid architecture [7] overcomes the problems faced by adhoc architecture. The devices are integrated to form a grid architecture. Effective resource sharing is the concept behind grid architecture. A grid by definition is a system that coordinates resources that are not subject to centralized control. The fundamental functions in a grid are resource discovery, negotiation, resource access, job scheduling and authentication. In mobile adhoc grid architecture the mobile nodes are allowed to form inside a grid in order to reduce the burden of the network. Since all the nodes are internally connected to each other resource sharing will be made easy. Thus the GHN,SPN,CN all appear inside the grid which performs variety of operations thus sharing the necessary resources to the customer node. Since the resources are shared there is no need for any central authority which is the major disadvantage of MANETS.Each node can be act as a

GHN,SPN,CN and CA itself. In MANET, nodes are free to join and leave the network at any time in addition to being independently mobile. Consequently, a mobile ad hoc network is vulnerable to many kinds of malicious attacks, and it is thus difficult to ensure secure communications. Malicious nodes directly threaten the robustness of the network as well as the availability of nodes. Protecting legitimate nodes from malicious attacks must be considered in MANETs. This is achievable through the use certificates or so called node ID's.Each node is assigned by a specific Id or Certificate. Whenever the node is detected as a threat to the network its Id or certificate is revoked [18] from the network, thus by securing the whole network system.The revocation mechanism is already been done for adhoc networks. Hence,it is now being applied to a sharing architecture called Mobileadhoc grid architecture.

## II. RELATED WORK

Grid architecture allows the network to share and use resources available efficiently without any problem between them. The certification revocation mechanisms is used to avoid malicious nodes to freely roam inside the wireless architecture. Several researchers have been done some works related to grid architecture and certificate revocation they are as follows:

Anda et al [9] have proposed a computing grid over a vehicular ad hoc network (VANET).It is used to exchange.Information between the vehicles on the road to

avoid traffic in the network. This can be done due to the energy available in the vehicle.In previous researches two types of mechanisms were used [19].The voting based mechanism in which the neighbor nodes will vote about the nearby malicious nodes. The non-voting based mechanism is one in which the accusing node will also sacrifice itself by revoking both the accusing and accused nodes certificates.

Our approach varies from the above mentioned works and we have used trace based approach in order to trace the mobile nodes to form a grid architecture and then to use the threshold mechanism to revoke the certificate of the malicious node.

## III. PROPOSED ARCHITECTURE FOR GRID FORMATION

The stability of the grid is the major challenge in mobile grid. Since the nodes are allowed to move freely inside the network it is difficult to form a grid with these mobile nodes. A Mobile Ad-Hoc Network (MANET) is a self-configuring network of mobile nodes connected by wireless links, to form an arbitrary topology. The nodes are free to move randomly. If nodes change their location over time, they have to update their location estimates frequently in order to avoid inaccuracies resulting from using outdated location estimates. Moreover, node movement during the measurement of parameters needed for location computation can cause inaccuracies in the estimated location.

### *A. Parameters Associated*

To overcome this mobility problem we are going to use the following parameters

- Position
- Stability time

*a) Position*

Whenever the nod joins the network it will keep on sending the information about its position. The position table will be updated once the node starts to move from one particular place to another. This will help to determine the status of the particular node. Once the status has been determined it is useful to determine the type of nodes.

*b) Stability Time*

The stability time of the mobile nodes are determined to understand the patter and the manner in which the nodes are moving .The stability time gives the approximate time of the nodes in which they are available ina particular position for a particular period of time

### *B. Grid Table*

Grid formation is the goal of the system. It starts with the grid table. The grid table is formed by using the available information about the nodes being implemented. The positions of the nodes are set to be in random manner. Resource management phase acts the middleware between grid initiation and grid formation. The resources are initially identified and the nodes which are requesting that resources have been found out. The resources are allocated to that particular node by using the service monitoring. The resources are updated once the new GHN has been formed. Hence the necessary functionalities are assigned to the GHN thus by servicing the CN by the SPN. The tables keep on updating due to the mobility of the nodes. Finally the grid architecture has been formed by sharing the resources efficiently between the CN.

Fig 1.1 represents the overall system architecture for grid formation. Initially the process starts with the mobile nodes. The positions and the stability time of the nodes are assigned at random since they move freely around the network. After all the process has been finished a grid table is formed which contains the details about the nodes inside the network. The grid table is then used for the resource allocation for the necessary customer and service provider nodes the resource management part of the system performs the process of allocating necessary resources to the nodes in the network. The resources are the back bone of the mobile adhoc architecture. They are shared between the nodes efficiently using the available grid resources.

## II. GRID FORMATION

The node willing to provide service is called service provider node (SPN) and the node which requires that service is called service provider node. The service provider node which has high stability time near the both customer node and service provider node will act as the Grid head node (GHN).The GHN is responsible for the communication process happening between the SPN and CN.

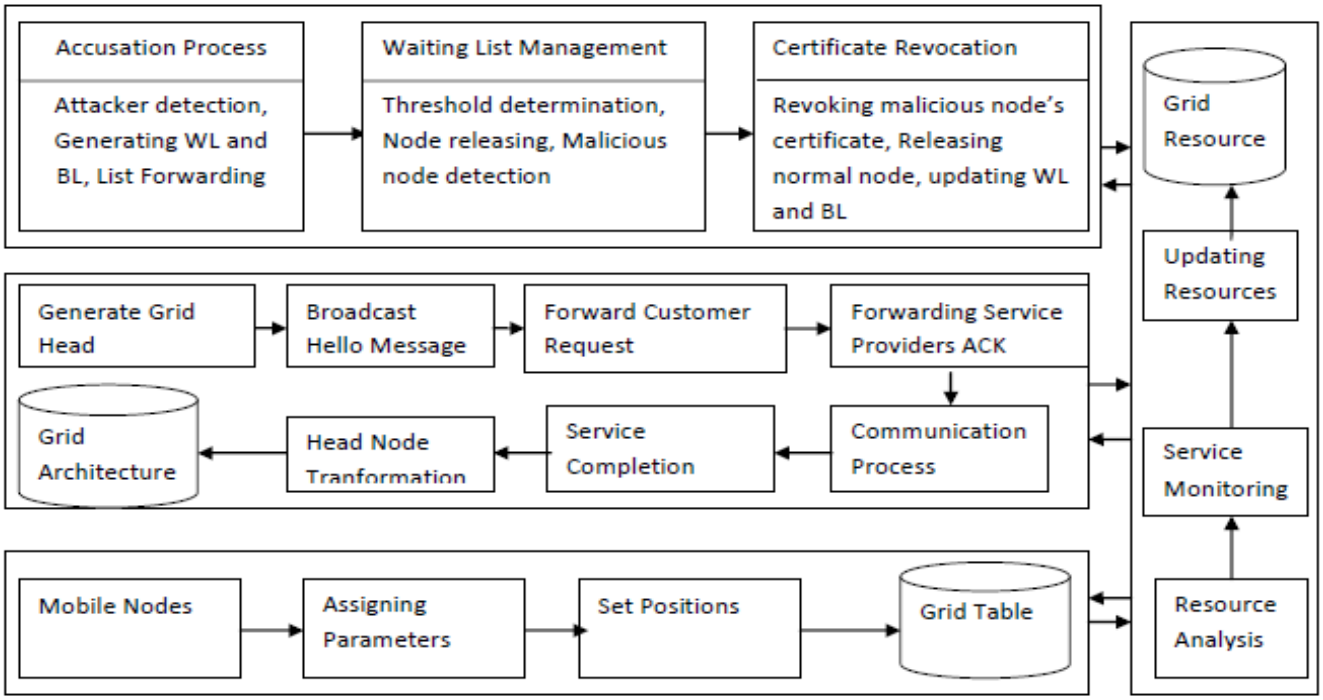
### *C. Resource Allocation*

The node willing to provide service will broad cast the hello packet throughout the network. The hello packet pattern is described in.The table consists of Node ID, Stability time and Hello ID.The node which needs the service will send the service request message to the SPN.The format of the message is shown in Table. The node willing to provide the service to the request will provide the Grid joining message to the SPN.

### *D. Resource Management*

The grid head node act as the centralized server for the communication process. Once the CN request for the service it will look up the grid joining message to select the suitable SPN to allocate it to the required CN.Once the service is allocated it will starts to serve the customer node. The process will be monitored by the Grid head node. After successful completion of the communication the service provider will send the completion message and the customer node will provide the acknowledgment message to the GHN.

The SPN after one successful completing it will send the terminate message if the node willing to exit from the service or it will provide the WTC (Willing To Continue) message if the service provider node wants to continue the service. The SPN will send the denial-of-service message if the SPN doesn't ready to provide the service. The major job of the GHN is not




only control the communication but also broadcasts the hello packets throughout the network such that it will indicate it is "alive" and it will allow the new nodes can join the Grid architecture.

The Grid head node will keep the table updated throughout the communication process, and will hand over the table details to the next GHN for successful communication. When network merge happens it will not affect the existing grid, instead new members will join the grid. But this situation will not happen frequently in a low mobile scenario.

## III. THRESHOLD MECHANISM

The threshold of the network has to be found out in order to decide whether a node is a malicious node or legitimate node. To do so we need an optimal threshold value, this should identify the malicious nodes perfectly. To find the threshold we are going to consider two different factors such as minimizing false release probability and maximizing correct release probability. From this analysis we can find the optimal threshold value. The grid head will wait for the accusation packets raised against a particular node. Once the number of accusation packets reaches the specific threshold the node will be passed to the revocation procedure.

### E. MINIMIZE FALSE RELEASE PROBABILITY

To find threshold value K in which the nodes to get falsely accused should be minimum. This can be achieved by using the below uniform distribution function

$$P_f(K) = \sum_{i=K}^{N} \binom{N}{i} p^i (1-p)^{N-i} \quad \rightarrow (1)$$

p-> probability of node participate in false accusation

### *F. MAXIMIZE CORRECT RELEASE PROBABILITY*

To find the threshold value K in which the nodes to get correctly release is maximum. This can be achieved by using the below condition

$$P_c(K) = \sum_{i=K}^{N} \binom{N}{i} (1-p)^i p^{N-i} \quad \rightarrow (2)$$

p-> probability of node participate in correct accusation

## IV. ACCUSATION PROCESS

The accusation process starts once the consumer generates an attacker packet against a specific service provider node.The threshold for the process will be achieved by using the equations (1) and (2). The problem arises when a service provider node's service gets interrupted. Once the attacker packet reaches the grid head, the grid head will broadcast a list throughout the network. The Black list consists of the service provider ID and its information and an wait list consist of customer node ID and its information. This is to avoid false accusation. False accusation happens when a normal node is

termed as malicious node. This may happen due to network problem. Once the attacker packet count reaches the threshold value the node will be considered as the malicious node and will be forwarded to the revocation process.

## V. WAITING LIST MANAGEMENT

List plays a vital role in the revocation procedure. Once the customer node identifies a malicious node it will create a list. The list contains detail about the malicious nodes in the form of packets. The packets are then forwarded to the grid head node. The grid head node creates a waiting list and black list. The waiting list consists of the details of the accusing node and the black list consists of the details of the accused nodes. The grid head node forwards the list details throughout the network, which allows the nodes in the network to update list details. Updating happens each and every stage of communication. The list details are broadcasted throughout the networks. The nodes on receiving their list details will update the list field.

## VI. CERTIFICATE REVOCATION

Once the node is decided as malicious node the certificate of that particular node has to be revoked by the grid head node. Once the certificate is revoked the list details are to be updated. Once the list details are updated the grid head node will broadcast the information throughout the network. This mechanism not only helps the nodes to know about the malicious node but also about the legitimate and falsely accusing nodes. In case if a customer node falsely made a legitimate node as malicious node and send the attacker packet against it, when broadcasting the list throughout the network, the neighboring nodes of that service provider node will send recovery packet and recover the falsely accused service provider node[17] and make the customer node which creates bad impression on that legitimate node will be sent to the black list.

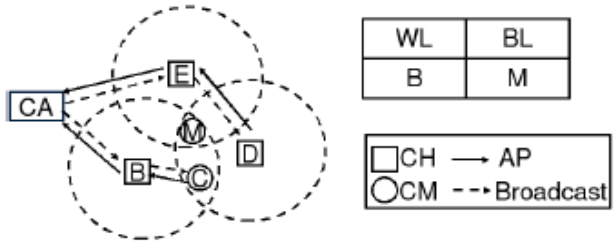



**Figure 8.1**

From the **Figure 8.1** it is clear that the node M in the black list is a malicious node and its certificate has to be revoked. The customer node will send the accusation packet to the central authority which is the grid head. The head node will then broadcast the list details throughout the network. The nodes in the network will know about the malicious node and will stop further activities with them. Finally, the node in the black list is eliminated by revoking the certificate of the malicious node. The process will continue until all the malicious nodes are eliminated

## VII. NORMAL NODE RECOVERY

The normal node recovery starts when the accusation packet does not reach a specific threshold value. We have to consider two conditions,

1. The accusing node may be itself a malicious node
2. The service provider may not work well at that particular time due to network error.

The main objective of this module is to maintain equal number of customer and service provider nodes. Due to the accusation process the nodes starts moving towards the list, hence there exist a deficiency for nodes to communicate. So the normal nodes are got back into the network using the recovery packet.

## VIII. PERFORMANCE EVALUATION USING SIMULATION

Simulation mechanisms are used to evaluate the Grid architecture. The simulation tool used is NS2.The parameters used for the simulation are given in Table 2.

**Table2. Parameters used in NS2**

| Parameter | Value |
|---|---|
| Node Placement | Random Distribution |
| Number Of Nodes | 50 |
| Terrain Dimensions | 1000m x 1000m |
| Transmission Range | 250m |
| Simulation Time | 600s |
| Routing Protocol | AODV |

### G. *Impact Of Threshold*

This evaluation parameter helps us to understand about the detection time of malicious node when altering the threshold value.

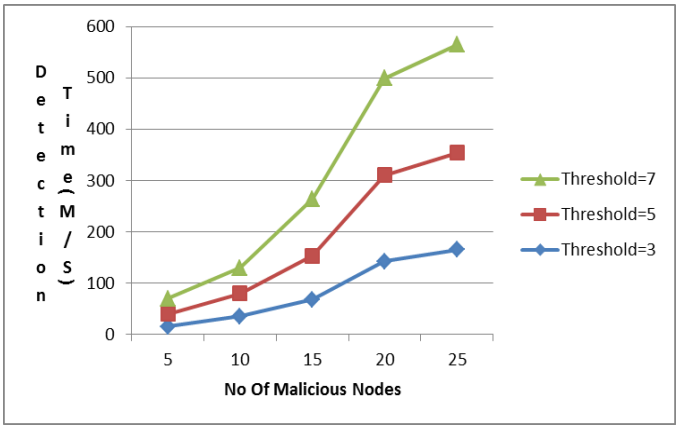


**Figure 9.A Number of malicious nodes vs Detection time. Here X-Axis denoted the number of malicious nodes and the Y-Axis time required to detect the malicious nodes. The graph shows that the detection time increases due to the increase of threshold.**

Thus from the above evaluations by increasing the customer nodes we can complete more number of jobs where the service provider node is static and it is fixed as 5.

### *H. Impact Of Mobility*

This evaluation technique helps us to know about the time required to detect the malicious nodes present inside the network by varying the movability speed of the nodes.

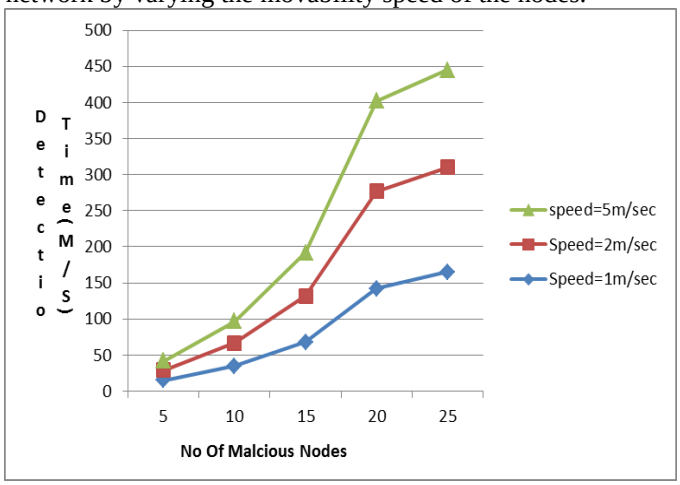



**Figure 9.B Number of malicious nodes vs Detection time graph. Here X-Axis denoted the number of malicious nodes and the Y-Axis denotes the detection time.The graph shows that the detection time increases as the speed of the mobile node increases.**

### *I. False Release Pobability*

This parameter gives threshold value increases in order to minimize the malicious nodes to get falsely reduced.

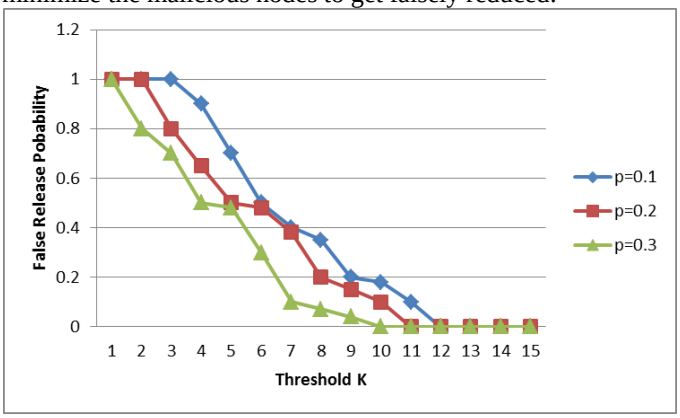



**Figure 9.C.Here X axis gives the malicious node and Y axis gives the detection time.**

Due to the increase in the threshold the number of times the particular malicious node gets accused increases which automatically increases the detection time and its shown in **9.C**

### *J. Correct Release Probability*

This parameter illustrates that the probability of a legitimate to be in waiting list increases as the threshold K increases

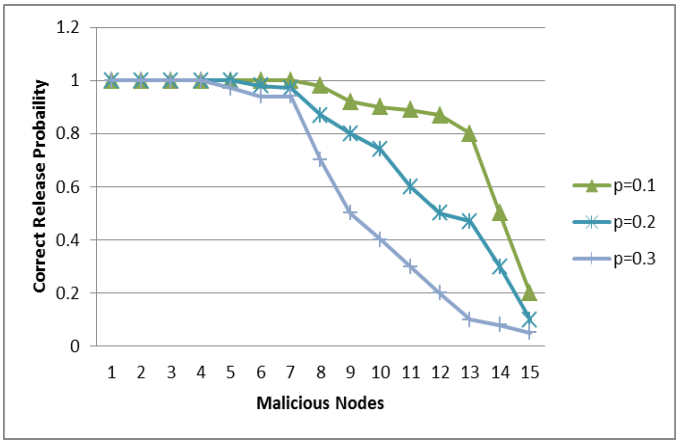



**Figure 9.D.Here X axis denotes the malicious nodes and Y axis denotes the correct release probability.**

This parameter states that since the legitimate stays longer in the waiting list there is a high probability for nodes to release correctly and its shown in **9.D**

## IX. CONCLUSION AND FUTURE WORK

As expected the grid architecture has been formed by using the mobile nodes and the malicious nodes are removed from the architecture by using the revocation mechanism. The mobility of the nodes which is the major problem in the MANET has been resolved by clearly evaluating the Position and stability parameters of the mobile nodes. The grid head node shared the resources among the service providers by itself without the use of any Central authorities which simplifies the process. The revocation mechanism is carried out by means of using the lists created by the grid head node. The threshold mechanism and the broadcasting list information are very helpful to recover the falsely accused normal nodes and falsely accusing malicious node. The number of malicious nodes removed and the efficiency is so high because each nodes are integrated as a grid architecture.

## REFERENCES

[1] V.Vetriselvi And,Ranjani Parthasarathri "Mobile adhoc grid architecture using trace based mobility model.

[2] Ian Foster, etc., "The Physiology of the Grid-An Open Grid Services Architecture for Distributed Systems Integration" Globus Project, 2002

[3] T. Phang, L. Huang, C. Dulan, "Challenge: Integrating Mobile Wireless Devices Into the Computational Grid", 8th Annual International Conference on Mobile Computing and Networking (MobiCom 2002), June 2002, pp 271-278.

[4] Y. P. Shao, M. K. O. Lee, S. Y. Liao, "Virtual Organizations: The Key Dimension", Academia/Industry Working Conference on Research Challenges 2000 (AIWoRC '00), April 2000, pp 3-8.

[5] L. M. Camarinha, "Matos: Infrastructures for Virtual Organizations - Where We Are", IEEE Conference Emerging Technologies and Factory Automation 2003 (ETFA '03), September 2003, pp 405-414. [6] I. Foster, "The Anatomy of the Grid: Enabling Scalable Virtual Organizations", First IEEE/ACM International Symposium on Cluster Computing and the Grid, May 2001, pp 6-7.

[6] A. Savva D. Berry A. Djaoui A. Grimshaw B. Horn F. Maciel F. Siebenlist R. Subramaniam J. Treadwell J. Von Reich I. Foster, H. Kishimoto, "The open grid services architecture", version 1.0., January .,2008

[7] Imran Ihsan, Muhammed Abdul Qadir, Nadeem Iftikhar, " Mobile Ad- Hoc Service Grid- MASGRID", Third World Enformatika Conference, WEC'05, pp 124-127,April 2005.

[8] Zhi Wang, Bo Yu, Qi Chen, Chuanshan Gao, "Wireless Grid Computing over Mobile Ad-Hoc Networks with Mobile Agent", First International Conference on Semantics, Knowledge and Grid, Nov 2005.

[9] J. Anda, J. LeBrun, D. Ghosal, C-N. Chuah, and H. M. Zhang, "VGrid: Vehicular Ad Hoc Networking and Computing Grid for Intelligent Traffic Control," IEEE Vehicular Technology Conference, Spring 2005.

[10] Roy, N. Das, S.K.Basu, K.Kumar M, "Enhancing Availability of Grid Computational Services to Ubiquitous Computing Applications", 19th IEEE International Symposium on Parallel and Distributed Processing, April 2005.

[11] C. Perkins And E Royer, "Ad Hoc On-Demand Distance Vector Routing", 2nd Ieee Wksp. Mobile Comp. Sys. And Apps., 1999.

[12] D. Johnson And D. Maltz, "Dynamic Source Routing In Ad Hoc Wireless Networks", Mobile Computing, T. Imielinski And H. Korth, Ed., Kluwer, 1996.

[13] Y. Hu, A. Perrig, And D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol For Ad Hoc Networks," Acm Mobicom, 2002.

[14] M. Zapata, And N. Asokan, "Securing Ad Hoc Routing Protocols", Acm Wise, 2002.

[15] P. Papadimitrates And Z.J. Hass, "Secure Routing For Mobile Ad Hoc Networks In Proceeding Of Scs Communication Networks And Distributed System Modelling And Simulation", Conference (Cnds), San Antonio, Tx, Jan. 2002.

[16] P. Yi, Z. Dai, Y. Zhong, And S. Zhang, "Resisting Flooding Attacks In Ad Hoc Networks", In Proceedings Of The International Conference On Information Technology: Coding And Computing, 2005.

[17] K. Park, H. Nishiyama, N. Ansari, And N. Kato, "Certificate Revocation To Cope With False Accusations In Mobile Ad Hoc Networks", In Proc. 2010 Ieee 71st Vehicular Technology Conference: Vtc2010-Spring, Taipei, Taiwan, May 16-19, 2010.

[18] G. Arboit, C. Crepeau, C. R. Davis, and M.Maheswaran, "A Localized Certificate Revocation Scheme for Mobile Ad Hoc Networks," Ad Ho Network,vol. 6, no. 1, pp. 17-31, Jan. 2008.

[19] Claude Crêpeau and Carlton R. Davis," A Certificate Revocation Scheme for Wireless Ad Hoc Networks"School of Computer Science, McGill University,Montreal, QC, Canada H3A 2A7.