International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

A PROFICIENT DISTRIBUTED SELF MANAGED PROTOCOL FOR NODE CONFIGURATION IN AD HOC NETWORKS

T.Mildred Lily Roselyn[1], S.Thiyagarajan[2]
[1]JP College of Engineering, Ayikudy.
[2]JP College of Engineering, Ayikudy.
[1]mildredlily@gmail.com
[2]jpcoehodcse@gmail.com

***Abstract*— The main objective of this project is to develop an addressing protocol for node auto configuration in mobile ad hoc network and also develop a technique for replica node finding. The Mobile ad hoc networks do not have a permanent infrastructure because of its mobility. So the Address assignment is a big challenge work in mobile ad hoc networks. To solve the problem this project uses a distributed and self-managed addressing protocol, called Filter-based Addressing Protocol. This protocol works well for dynamic ad hoc networks with fading channels, frequent partitions, and joining/leaving nodes. This protocol is a lightweight protocol because it configures mobile ad hoc nodes based on a distributed address database stored in filters that reduces the control load. This protocol uses the address filters to avoid address collisions, reduce the control load, and decrease the address allocation delay. Based on this protocol each node has all address of all nodes. So, at the time of any replica attack performed on the network it collapse the whole network. So to avoid that attack this project also finds the replica node attack. This project finds the replica node by random number exchanging. The replica node meets each node at any time it request its random number for verifying. Suppose the replica node encounters one node it compromise the node and copy all the information including IP address and act as the affected node. So when doing verification the information of the two nodes are same. At that time the two nodes are identified as the replica and it is blacklisted.**

***Keywords*— MANET, Auto-configuration, IP address, Attack, Blacklist.**

I. INTRODUCTION

A mobile ad hoc network (MANET) consists of collection mobile nodes which communicate over radio and do not need any infrastructure.

The each node should be a self configurable one and also have the capability to maintain all the resources of the network in a distributed fashion. The each mobile node in MANET is to move independently in any direction. The IP address assignment is challenging problem in the ad hoc network. When a new node want to join a network it has to be assigned an IP address uniquely.

MANET nodes communicate with each other by exchanging IP packets. As the corresponding nodes may not be directly reachable from each other, intermediate nodes have to forward IP packets [1]. Auto-configuration is a desirable goal in implementing mobile ad hoc networks. Specifically, automated dynamic assignment of IP addresses is desirable [3][5]. Evenly distributed Duplicate-IP Detection Servers are used to ensure the uniqueness of an IP address. Any new node requiring an IP address picks up a random IP address and sends a query to this special node to verify whether this randomly chosen IP address is already chosen by some other nodes [4]. The Duplicate Address Detection protocol is used for addressing protocol. This protocol does not take into account network partitions and is not suitable for ad hoc networks. Due to the poor physical protection of mobile nodes, it is generally assumed that an adversary can capture and compromise a small number of sensors in the network. In a node replication attack, an adversary can take advantage of the credentials of a compromised node to surreptitiously introduce replicas of that node into the network. Without an effective and efficient detection mechanism, these replicas can be used to launch a variety of attacks that undermine many sensor applications and protocols [10].

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

To proposed an addressing protocol for node auto configuration and also reduce the control load in mobile ad hoc network and also develop a technique for replica node detection. The mobile ad hoc network does not have any permanent infrastructure. Because of the mobility the address assignment is the major problem. This problem handled by the light weight protocol that avoid the address collision problem and also reduce the control load. During that time the any replica attack performed on the network it collapse the whole network. So want to find the replica and detect from the network. The replica node finds by the random exchanging. If the node meets each node at any time it requests its random number for verifying. If its verify by nodes it can exchange the information. Suppose the replica node encounters one node it compromise the node and copy all the information including IP address and act as the affected node. During verification the two nodes have same information. At that time the two nodes are identified as the replica and it is blacklisted.

The remainder of this paper is organized as follows. In section 2 describe about Methodologies section 3 explains the Experimental setup and section 4 Concludes the paper.

II. METHODOLOGIES

In MANET, the new node can arrive by sending the HELLO message and the node can wait for the reply message. If the node cannot receive any response the network should be initialized. The node can choose its IP address randomly and creates address filter then store it. Otherwise the new node directly joins in the network. Initially the node can use random IP address then check the same address it can be choose if its mean the address collision can check after the address filter can be updated. Otherwise the address collision not occurs in the network that can directly update the address filter with new address. The each node should broadcast its IP address. The partitioning network that has unique network ID. After completing its performance the node can leave from the network. The leaved node may want to join the other network that may allowed by MANET. Then check if the address collision may occur or not and the address value is greater than the network address that increase the address and update the filter.

The address filters to avoid address collisions, reduce the control load, and decrease the address allocation delay. Based on the light weight protocol each node has all address of all nodes. So, at the time of any replica attack performed on the network it collapse the whole network. So to avoid that attack this project also finds the replica node attack. To finds the replica node by random number exchanging.

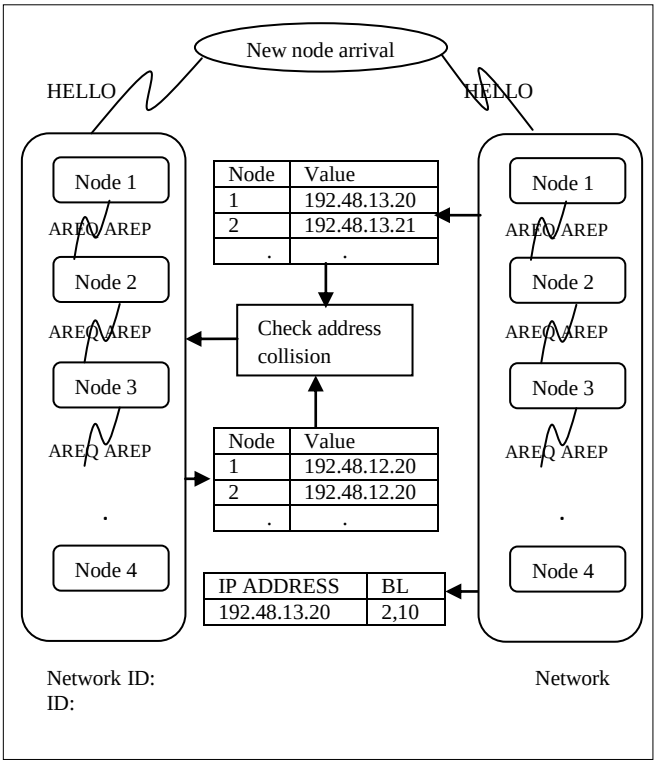

Fig. 1. System design

In MANET create two array to store the random number the each array has n length. If the replica node can arrive the can encounter the nearby node. Then the random number can ask for the data transmission. The random number can exchange after the data can be transmitted that node should not be a replica. If the node cannot exchange the random number that node should be replica. That can add into the Black list

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

A. MANET Initialization

The Initiator of a MANET broadcasts Hello message and waits for a Reply message until the timer expires. If it does not receive any message, it re-broadcasts the Hello message. This is to ensure that, if there are other configured nodes in the network, the event of message losses the node does not assume itself to be the Initiator. After all the failed retries, the node concludes that it is the only node in the network. An initiator node may start the network alone. It then assigns itself the first IP address from the IP address block randomly and creates an empty address filter, initializes the IP set to the rest of the IP address block, and sets its network Id, the initial node and creates a empty filter

B. New node joining the network

After MANET initialization, any new node appearing in the neighbourhood of existing node(s) broadcasts an Address Request message with address filter signature and starts the timer by using Filter based addressing protocol (FAP). This signature identifies the network and is used to detect partitions, in case they occur. The each node can have own IP address before that the node can enter into the network. The address information should be broadcasted as the Address Request message. The Address Request message is used to advertise that a previously available address is now allocated. . Each Address Request has an identifier number, which is used to differentiate Address Request messages generated by different nodes, but with the same address. Each address allocation is assigned a unique transaction id. If the initiator node receives any Address request with the same address that it has chosen, but with a different identifier number, which means that there is an address collision, the node waits for a period Tc and then chooses another available address and sends another Address Request. During the period Tc, the node receives more Address Request's with other already allocated addresses. Therefore, after Tc, the node knows a more complete list of allocated address, which decreases the probability of choosing a used address. Hence, the period Tc decreases the probability of collisions and, consequently, reduces network control load. All initiator nodes have chosen a unique address due to the random address choice and the validation using AREQ messages with identifier numbers.

Additionally, every node knows all currently allocated addresses with a high probability and also that check the false positive value for address allocation in the network by using Po. Po=(1-1/m)^(k ,n) and false positive probability for k bit Pfb =(1-Po)^k

C. Departure of a node

The nodes in the network can either depart abruptly or gracefully from the network. The IP addresses and the IP sets of nodes that abruptly depart the network are reclaimed during subsequent IP address allocation processes. A node that wishes to gracefully depart the network sends a Hand Over message with its IP address, IP set, and pending IP set to one of its neighbors before leaving the network. The neighbor on receiving the Hand Over message, appends the received IP address, IP set, and pending IP set to its own IP set.

D. Management of the network merging and partitioning

During the course of MANET operation, nodes can split from a network and form/join other networks. These networks can later merge into one. To detect merging of networks, each network needs a unique identifier (network id). The probability of two nodes having the same address is low. Furthermore the probability of nodes having the same address getting assigned identical IP addresses with equal timestamps is even lower. Add the random number field to network id, makes the probability of duplicate network ids negligible. Thus, for all practical purposes, network ids can be considered to be unique. The network id of a network is changed every time address reclamation is performed. By changing the network id it is ensured that networks have unique network ids. The inclusion of timestamp as part of the network id ensures that even if the same allocator performs IP address reclamation more than once, the resulting networks would still have different network ids.

E. Replication attack and replica node detection

The replicas are all clones of the captured nodes, the replicas can be considered as legitimate members of the

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

network, making detection difficult. Every node is having a random number generator. When a node encounters another node, they exchange the random numbers. Once again the same nodes meet, they verify the random numbers exchanged already. If no match, clone node found and it can be blacklisted. By using XED algorithm the replica can be found. The algorithm has 2 phases 1.offline phase 2.online phase. The former is executed before node cans deployment while the latter is executed by each node after deployment.

1. Offline step

A security parameter b and a cryptographic hash function h(.) are stored in each node. Additionally, two arrays Lr(u), and Ls(u) , of length n , which keep the received random numbers and the materials used to check the legitimacy of received random numbers, respectively, along with a set B(u) rep- resenting the nodes having been blacklisted by u , are stored in each node u . Lr(u), and Ls(u) are initialized to be zero-vectors. is initialized to be empty.

2. Online step

If u encounters v for the first time , u randomly generate α € [1,2^b -1], computes h(α),sends h(α), to v, and stores Ls(u)[v]= α. Note that it encounters v for first time if Ls(u)[v]=0. When u encounters v, it first checks if v is in the blacklist B(u). If so, this means that v is considered a replica by u and v refuses to communicate with v. If not, the following procedures are followed. They exchange the random numbers, Lr(u)[v] and Lr(v)[u]. From the viewpoint of node u, after the reception of the random number Lr(v)[u] sent by v, u checks if Lr(v)[u] is the random number u sent to v last time. This can be accomplished by verifying if Ls(u)[v]=Ls(v)[u] holds. Node v is added into B(u) if the verification fails. Otherwise, the same procedure, including randomly generating a new α , computing h(α) ,sending h(α) to v , and replacing the old Lr(u)[v] with a new Lr(u)[v]= α , is performed. For the replica that does not possess the correct random number, due to the one way property of the cryptographic hash function, the probability of successful verification is only 1/2^b-1. The same procedure applies for node v.

III. Experimental Results

To analyze the performance of the proposed system, lots of simulation experiments are conducted. The proposed system is implemented in Network Simulator (NS2). In the simulation experiments, the parameters used for our simulations are: an average transmission range of 18.5 m, a maximum carrier sense range of 108 m, and a density of 0.0121 nodes/m . This is shown in the below table

TABLE I Parameter values

Variable	*Description*	*Value*
TO	Bootstrap time	1 s
TP	Min. interval between partition merging procedures	3 s
TT	Time waiting before changing address	0.3 s
TI	Time waiting for AREQs in the initialization	1.2 s
TR	Interval between replications of flooding messages	0.3 s
TH	Interval between retransmissions of Hellos	1s
TS	Time storing filter signatures of its own partition	0.5 s
TS'	Time storing filter signatures of other partitions	3 s
TM	Min. interval between filter renews	5 s

To analysis the performance the proposed method several performance metrics are used. They are Probability of Collision, Control Overhead, Detection Accuracy. Detection time, Communication Range, Movement Velocity and Number of Replica.

A. Probability of Collision

This project analyzed FAP to evaluate the probability that our scheme causes an address collision. A collision occurs when two different joining nodes generate AREQs with the same address and the same identifier number or if two disjoint partitions own exactly the same filters.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

In the first case the joining nodes do not notice that their addresses are the same because the message from the other node seems to the first node like a retransmission of its own message. In the second case, the partition merging procedure is not started because the signatures of the Hellos are the same for both the partitions, and, consequently, the network would have a collision for each of its addresses. This is shown in the below table

TABLE III COLLISION PROBABILITY

Network Size	Collision Probability
10	0.234
20	0.367
30	0.428
40	0.521
50	0.632

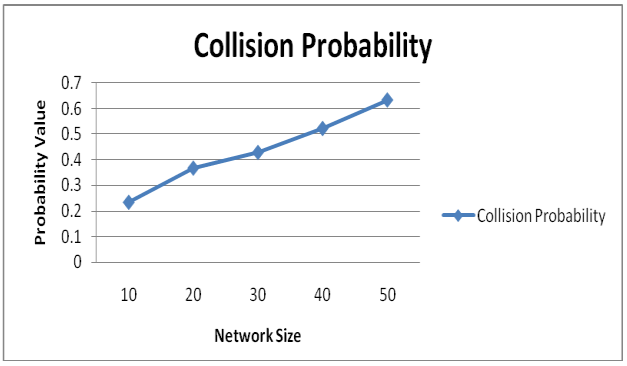

Fig. 2. Collision Probability

The above figure shows the collision probability, considering an address range of 256 entries. This project observe that there is a high probability of address collision, but the AREQ collision probability is negligible, even for a number of nodes greater than the number of available addresses, due to the use of the identifiers.

B. Control Overhead

The main procedures in addressing protocols are network initialization. The protocol generates control overhead, reducing the available bandwidth. This project estimates the number of control messages sent by all these procedures for FAP, the extension of DAD with partition detection (DAD-PD), and MANETconf (Mconf). DAD-PD uses partition identifiers.

This project also compares our protocol with MANETconf, which is based on the knowledge of the Allocated list, which describes the allocated addresses, and the Allocated Pending list, which describes the list of the addresses under evaluation to be allocated to joining nodes. This is shown in the below table

TABLE IIIII CONTROL OVERHEAD

Network Size	FAP	DAD-PD	MANETconf
10	50	70	80
20	55	75	82
30	60	80	86
40	65	85	89
50	70	88	90

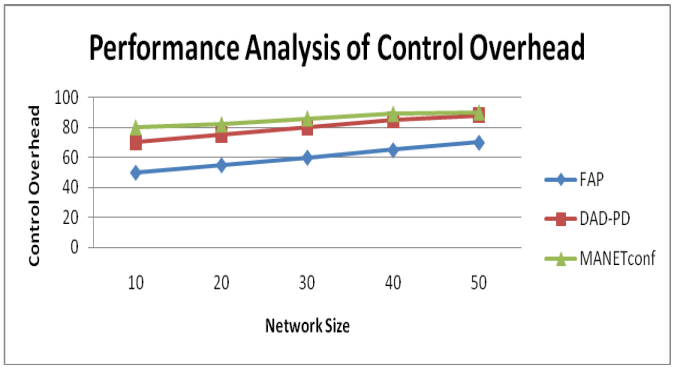

Fig. 3. Performance Analysis Of Control Overhead

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

From the above graph it is shown that, in the initialization, FAP presents a high probability of having the smallest overhead because it is similar to the procedure proposed by DAD. DAD-PD and MANETconf have a larger control load because they specify only a gradual initialization procedure.

C. Detection Accuracy

Detection accuracy is used to represent the false positive ratio and false negative ratio of the underlying detection algorithm, which are the ratios of falsely considering a genuine node as a replica and falsely considering a replica a genuine node, respectively. This is shown in the below table

TABLE IV DETECTION ACCURACY

Network Size	RM	SDD-LWC	XED
10	88.12	89.57	94.35
20	89.35	90.15	95.63
30	87.35	89.42	94.98
40	88.86	90.43	96.82
50	89.53	90.26	95.72

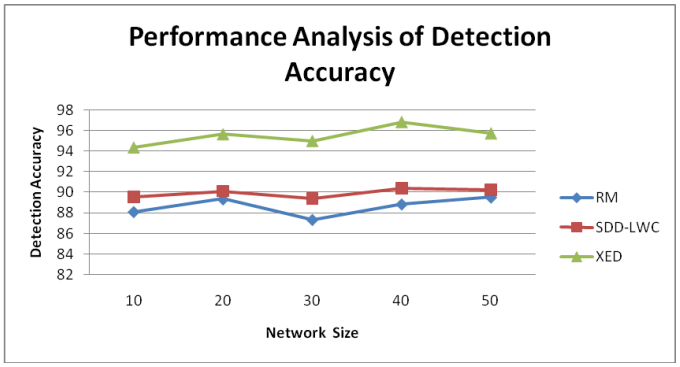

Fig. 4. Performance Analysis Of Detection Time

D. Number Of Replica

The relationship between the detection time and the number of replicas is shown in below graph. The more the replicas, the less the detection time and the better the detection accuracy.

TABLE V NUMBER OF REPLICA

Network Size	Replica Node	Genuine Node
10	0.4	0.1
20	0.8	0.3
30	1.4	0.9
40	2.3	1.2
50	2.9	2.2

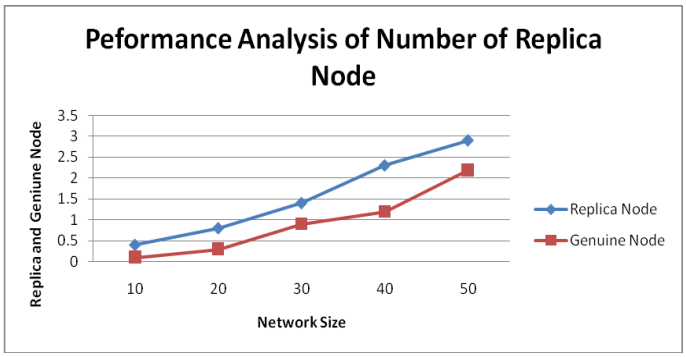

Fig.5. Performance Analysis Of Number of Replica

IV. CONCLUSION

Thus the proposed system dynamically auto configure network addresses, resolving collisions with a low control load by using FAP and also focuses the replica detection. To detect the replica node attacks in MANET by using XED algorithm. That can identify replicas with high detection accuracy. When replicas can communicate with each other, the replica can always share the newest received random numbers with the other neighboring replicas, thus degrading the detection capability because multiple replicas are able to reply with the correct random number to encountered genuine nodes accordingly. In future this technique can be improved to detect the multiple replica communication in self configurable network.

International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)
International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

V. REFERENCES

[1] Sanket Nesargi, Ravi Prakash "MANETconf: Configuration of hosts in a mobile ad hoc network" INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE (Volume:2)

[2] D. O. Cunha, O. C. M. B. Duarte, and G. Pujolle, "A cooperation aware routing scheme for fast varying fading wireless channels," IEEE Commun. Lett., vol. 12, no. 10, pp. 794–796, Oct. 2008.

[3] Nitin H. Vaidya "Weak Duplicate Address Detection in Mobile Ad Hoc Networks" MOBIHOC'02, June 9-11, 2002, EPFL Lausanne, Switzerland.

[4] Syed Rafiul Hussain, Subrata Saha, and Ashikur Rahma "An Efficient and Scalable Address Autoconfiguration in MANET" Lecture Notes in Computer Science Volume 5793, 2009, pp 152-165

[5] Luis Javier García Villalba, and Julián García Matesanz, "Auto-Configuration Protocols in Mobile Ad Hoc Networks" Published online 2011 March 25.

[6] N. C. Fernandes,M.D.Moreira, and O. C. M. B. Duarte, "A self-organized mechanism for thwarting malicious access in ad hoc networks," in Proc. 29th IEEE INFOCOM Miniconf., San Diego, CA, Apr. 2010,

[7] C. E. Perkins, E. M. Royers, and S. R. Das, "IP address autoconfiguration for ad hoc networks," Internet draft, 2000.

[8] Z. Fan and S. Subramani, "An address autoconfiguration protocol for IPv6 hosts in a mobile ad hoc network," Comput. Commun., vol. 28, no. 4, pp. 339–350, Mar. 2005.

[9] H. Zhou, L. Ni, and M. Mutka, "Prophet address allocation for large scale MANETs," in Proc. 22nd Annu. IEEE INFOCOM, Mar. 2003

[10] Bo Zhu ; Setia, S. ; Jajodia, S. ; Roy, S. ; Lingyu Wang "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks" Mobile Computing, IEEE Transactions on (Volume:9) July 2010

[11] M. D. D. Moreira, R. P. Laufer, P. B. Velloso, and O. C.M. B. Duarte, "Capacity and robustness tradeoffs in Bloom filters for distributed applications," IEEE Trans. Parallel Distrib. 2219–2230, Dec. 2012.

[12] Y.-C. Hu, A. Perrig, and D. Johnson, "Packet leashes: A defense against wormhole attacks in wireless networks," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), 2003, pp. 1976–1986.

[13] J. Ho,M.Wright, and S. K. Das, "Fast detection of replica node attacks in mobile sensor networks using sequential analysis," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), Brazil, 2009, pp. 1773–1781.

[14]] D. B. Johnson and D. A. Maltz, "Dynamic source routing in ad hoc wireless networks," Mobile Comput., pp. 153–181, 1996.

[15] Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo, Fellow, IEEE VOL. 8, NO. 5, MAY 2013

[16] K. Xing, F. Liu, X. Cheng, and D. Du, "Real time detection of clone attack in wireless sensor networks," in Proc. IEEE Int. Conf. Distributed Computing Systems (ICDCS), Beijing, China, 2008, pp. 3–10.

[17] J. Yi, J. Koo, and H. Cha, "A localization technique for mobile sensor networks using archived anchor information," in Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA, 2008, pp. 64–72.

[18] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Mobile sensor network resilient against node replication attacks," in Proc. IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA, 2008, pp. 597–599, (poster).

[19] C.-M. Lu, and S.-Y. Kuo, "Efficient and distributed detection of node replication attacks in mobile sensor networks," in Proc. IEEE Vehicular Technology Conf. Fall (VTC-Fall), Anchorage, AK, USA, 2009, pp. 1–5.