Network Management by Tackling Replication Attacks: A Comparative Study

Deepa Byadgi
Student
DSI, Bangalore

A M Prasad
Associate Professor
DSI, Bangalore

Suma V
Dean, RIIC
DSI, Bangalore

ABSTRACT
Network is an interaction or engaging in formal or informal communication among systems to exchange information by mutual assistance or support. The sharing of resources helps the users on the network to communicate with each other. Node in a wireless sensor network that is capable of performance handling, gathering information and communicating with other connected nodes in the network are called sensor nodes. Sensor nodes, despite of having limited resources are useful in many applications. Wireless sensor networks have become an intensive research area where the security is of concern. An adversary can capture a node with a very little effort, analyze and replicate them easily. If a node is captured, an adversary reprograms it and replicate into larger number of clones, thus disrupts the entire network. Security is the most important criteria for senor networks. Various approaches are proposed for effective management of replication attacks. This paper thus shows the different approaches involved in detection of replicated nodes in mobile sensor networks and comparison of the methods involved and hitches of the previous approaches.

General Terms
Security, Attack, Network

Keywords
WSN, MSN, Adversary, Replica

1. INTRODUCTION
A network is vulnerable to various types of attacks. An assaulter launches attacks and by a little effort he/she gains the trust of other nodes. The information possessed by the nodes should be secure at any point of time. The network information should be confidential, accurate and available all the time when required and should posses the characteristic of integrity; in the sense the information should be complete and uncorrupted. Security is the quality or state of being secure from danger. In simple words, protection against adversaries, from those who could be purposely harmed or otherwise-is the goal [16].

A wireless sensor network (WSN) is composed of a huge number of sensor nodes with limited resources. Wireless Sensor networks (WSNs) are used in various applications of military, health and environments and civil use. The new nodes can be added to the network without any intervention of base station or the administrator. These nodes initiate neighbor discovery protocol. As WSNs are not deployed in amicable environment, designing an efficient method to detect attacks is of great importance for information security in WSNs.

A Mobile sensor network (MSN) is a group or gathering of sensor nodes which are having the mobility, such as unmanned vehicles equipped with sensors. Improving of the sensing coverage of network can be achieved through the mobility of sensor nodes. However, there exist some of the reasons for incorporating mobility in the sensor nodes.

They include possibility of occurrence of attacks in the network that are caused by the attacker. As time evolves, a network loses its coverage in some specific areas either due to jamming attacks or due to natural causes such as node failure which leads to severe effects in the network despite of achieving successful deployment. Hence, there is a need that sensors should have mobility so that they can autonomously heal the coverage holes caused from catastrophic incidents such as wind or obstacle after landing. Other situations where mobile sensor nodes are desired include, tracking of moving objects whose exact trajectory is unpredictable in a large area. To chase some object it is desired to use mobile sensor nodes, as static sensor nodes involves cost and are inefficient. Each node is able to communicate with its surroundings with the help of some protocol. It is worth to note that any action that comprises the security of information is termed as attack. Wireless sensor network is hence prone to attacks. The attacker captures one node and obtains information about its unique ID and creates many such nodes having the same ID and inserts the nodes into the network in order to create the adverse effect to the network. With the help of this he can launch many attacks. Such a type of attack which is popularly known as Replication attack

D, A, S, G are all unique nodes. However, the adversary gets the information about the security is one of the non tolerable attacks in wireless sensor networks. Thus, it is imperative to overcome or reduce such type of unwanted attacks. Fig 1 depicts occurrence pattern of replication attack.

The Fig 1 infers that the adversary can fabricate large number of replicated nodes and insert at specific positions in the network. We can see the credentials of the node U which is fabricated. The replicated node which is shown in boxed node named U has the ID of the legitimate node and look like the authorized node.

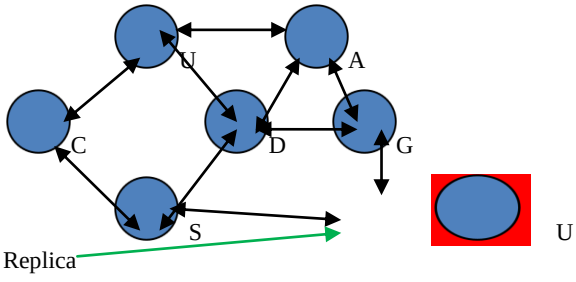

Fig 1: Replication Attack

Thus, it is now possible for the intruder to control the traffic of the network passing through these nodes and may

jam the whole network and inject false data in the network by having huge number of replicated nodes. Thus, the entire network can get disrupted with a little effort. In order to avoid the attack, one should prevent the intruder from getting the secrete credentials from the nodes. Further, threat of this replication attack is that if an adversary can clone a node [5], [13], it becomes possible to launch more attacks and get control over the network. The adversary can compromise with the other nodes too in the network thus should be detected as soon as possible. The network credentials must be kept secure since the other nodes do not know that it is the replicated node so they are enabled to communicate with it. Additionally, replicated node may comprise of false data which gives false information to the legitimate node thereby giving an illusion to the authorized node as the truthful information for their utilization. Since, the attacker can create a lot of replicas by capturing only single node it is dangerous than compromising nodes [10]. The work by Parno [3] states that, the adversary can cause the following damages to the ongoing operations in the network. Assailant may revoke the legitimate nodes, eavesdrop, and compromise the functionality of the network. He can even add false data in the network and pass the same to the other nodes in the network resulting in Suppression of the legitimate data. Thus, he manages the traffic or any activity that undergoes throughout the replicated nodes and disrupts the communication as desired. The replica which acts according to the supervision of the intruder can spread blames on the other authorized nodes. Fig 2 depicts the possible occurrences of the damages by the assaulter in the network.

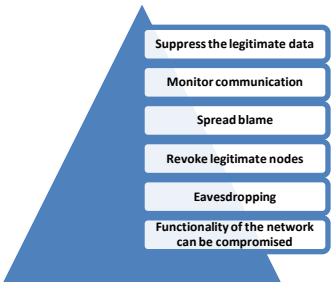

Fig 2: The catastrophe of the replication attacks

Thus, there should be a method to detect the replicated nodes in the network and to remove it from the network. It is must that, an approach should prevent adversary from getting the information from the nodes of the network.

The above stated requirement has directed this part of the research to investigate upon various existing detection schemes and to conduct a comparative analysis of the same.

2. RELATED WORK

Several works has taken place in order to detect the injection of replicated nodes and their preventive measures. Investigation of the related works has indicated that the nodes in the sensor network must broadcast its location claims. The interaction with base station terms the approach called Centralized detection. Distributed detection doesn't involve the concept of existence of the base station. Accordingly, author Xing *et.al* [6] describes the method of centralized detection used in mobile sensor network. It is based upon the Sequential probability ratio test, is fast and effective detection method for replicas in MSNs. The pulling out of security or private credentials from nodes by the intruder should be avoided. It is based upon the concept that nodes in the network move with the predefined speed. The replica moves with the high speed as compared to other legitimate nodes in the network. Thus, the replica can be detected easily.

Further, the concept of distributed detection is to avoid central point's failure. Therefore, author Parno *et.al* [3] describes the distributed approaches applied in the wireless sensor networks for the detection of replicas, called Randomized multicast and Line selected multicast, which gives an idea for using distributed approaches. [1], [6], [7] is based upon the requirement of witness distribution, indicates the selection of the witnesses, analyses the properties of distributed detection in the wireless sensor networks [2].

Additionally, the EDD (efficient distributed detection) approach is proposed by the author of [7], which also involves the scheme called SEDD to tackle the problems against the replication attacks in Mobile sensor networks, and lies on the fact that it shows the individual detection and avoidance of revocation throughout the network. Author Yu *et.al* [8] introduces the concept, XED in which the location information is not required and the communication cost is constant. It involves the strategy called remember and challenge. The basic idea here is to exchange the random numbers between the nodes. The nodes check for the records in order to identify the replica in the network. The random number received by the other node should be same as before.

However, the replicas in the network can destroy the whole network if they are left undetected. Hence, it must be identified as early as possible so to avoid less damage to the ongoing network operations. SPRT [6] is a centralized approach which is for the mobile sensor nodes. When a node moves to new location, its neighbors will ask for the information regarding time and location and decides either to forward the received information to the base station or not. Base station calculates the speed and performs on the speed consideration. When the base station finds that there is a replica detected it starts replica revocation.

Author Conti *et.al* [17], proposed the localized algorithm in which, the method involves, introducing a model of realistic attacker and which can be used to evaluate the provided solution's quality. It includes only one hop node communication and the mobility of the node. In the beginning of each cycle, all nodes are randomly and uniformly placed. All the nodes keep the list which contains IDs of nodes, location and time. For each move, node broadcasts its information to the neighbors, by this we can check whether the any node is appearing in the different locations. Deng *et.al* [9] describes the algorithms for replica detection which are based upon property of mobility and the approaches are called as UTLSE (Unary Time Location Storage & Exchange), MTLSD (Multi Time Location Storage & Diffusion).These methods are encounter based and the messages are sent only when the two nodes meet each other. However, clone attacks pose severe problems. Attacker with less effort can attack without the need to compromise many nodes. He may just capture one node and replicate much more copies of it. As the nodes in MSNs keep moving, the methods applied must be able to distinguish the nodes at different time stamps at different locations. The designs should have high execution speeds and shouldn't involve the high memory

consumption and communication overhead. Some of the methods rely upon the witness finding strategy and some on the knowledge of deployment [9].

There may exist, some pitfalls for the detection method but the identification of replicas must be much faster. Hence, it is vital to have an effective network management system.

3. NETWORK MANAGEMENT

As the replicas are inserted in the network by an intruder, there is a possibility that the entire effort of building a network can go down because the attacker can gain access to all the nodes in the network. The management of security in the network is to detect the replication attack with the high probability and to identify the replica in order to eliminate the replicas from the network. The replicas must be identified in the faster way. The time taken to detect the replica must be much smaller. The accuracy of identification of faults in the network leads to the proper management. Fig 3 shows the management of network.

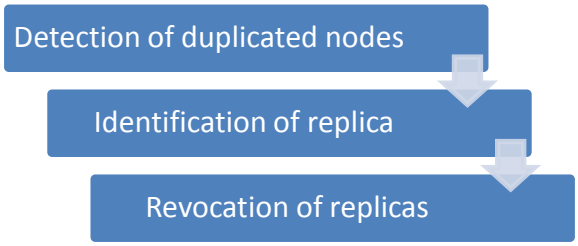

Fig 3: The Network Management Tree

The steps involved in the management are,

3.1 Detection of Duplicate Nodes in the Network

The duplicated nodes will have the same IDs. The replicated nodes in the network can be identified through some of the approaches called Centralized and Distributed and Localized approaches. The centralized detection involves the nodes in the network to communicate with the central body called base station. Base station controls the activity of all the nodes in the network. Each node sends list of its neighbors to the base station. The base station receives the list from all the nodes in the network and searches repeated IDs.

3.2 Identification of Replica

Base station receives the neighbor list and claimed locations. Then it examines the entire neighbor list if there are nodes with conflicting location claims it considers as the replicas. Let us assume legitimate node 1 is having its ID as '*u*' and intruder creates the replica with the same ID '*u*', Then base station gets to know the node ID '*u*' has the conflicting location claims. If it detects the one or more replica it invokes further action, if not no action is taken and network activities are carried out seamlessly**.**

3.3 Revocation of Replica

When the base station receives the conflicting locations it revokes the replicas by sending authenticated revocation messages. All the nodes in the network receive node revocation message and thus the replicated nodes are removed from the network. Since, network management is achieved via two approaches, this research further directed towards comparison of the approaches.

4. CENTRALIZED AND DISTRIBUTED DETECTION OF REPLICAS: A COMPARATIVE STUDY

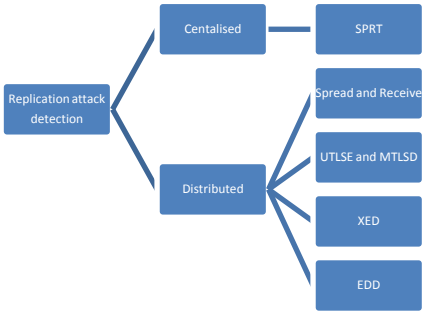

Fig 4: The Approaches for Replica Detection

4.1 Centralized Detection

Centralized detection of replicas in the network involves the intervention of the base station as base station controls the entire nodes in the network. The base station obtains information about the location claims from all the nodes. After the examination of the neighbor list and the location claims, if there are conflicting locations, the network wide revocation message is sent to all the nodes in the network. If a node is found to be deployed in more than location, it is assumed to be a replica incase of static nodes. Then the replicas are removed from the network. Those involve with SET (local detection) [14] and pre distribution keys [11], in which a key is distributed to the entire legitimate nodes in the network at the initial setup of network. However, the approach is not free from drawbacks [3]. They include, Single point of failure, exhausting of nodes near the base station, delay of revocation, and some of the applications may not use centralized approach. SPRT [6] is proposed to detect replicas by using the centralized mechanism.

SPRT: In case of mobile sensor networks the fast detection of replicas is used, SPRT which indicates sequential probability ratio test. It depicts the nodes in the network move with the speed Vmax which is predefined and the speed can't be known to the adversary as the replica should move with the higher speed, this assumption makes the fact that replicated nodes move with the high speed. The nodes which are having the mobility speed as more than the Vmax, it is considered to be the replica [6].At the initial stage of deployment, all the nodes in the network get the materials to generate the digital signature. Here the public key strategy is used. MSNs require more power than the static ones because mobility is involved. It involves two phases namely "Claim generation and forwarding" and "Security analysis". An intruder won't gain much benefit from having several copies or replicas of same node. Attacker will not get more benefits by launching replication attacks in the limited region. And this approach shows the drawbacks of the group attack strategy, in that intruder have a control in the movements of the collection of replicas, and this involves the scheme of random attack strategy in which attacker makes replicas randomly move in the network

Strengths:

- Detects the replicas quickly with less number of location claims

- Optimal storage overhead

Weaknesses:

- Single point of failure
- Network wide synchronization and revocation is required and More communication overhead
- Fast energy depletion of the sensor nodes around the base station
- There may be errors in the speed measurement of the node

4.2 Distributed Detection

Distributed detection involves the strategies of node to network broadcasting, with the deployment knowledge and the witness finding strategies in the static wireless sensor networks. In the mobile Ad Hoc networks the schemes involved are, in order to detect replicas based upon the distributed approach have the concepts of Time Domain Detection (TDD) and Space Domain Detection (SDD) [4] are based upon local information exchange. SDD-LC is used to check the identity and SDD-LWC is for witness check locally. Spread and Receive involves the concept of detection of replicas in the mobile environments. UTLSE and MTLSD are designed to tackle replication attacks in the mobile wireless sensor networks and the detection in static networks involves the approaches as Random multicast; line selected multicast, Deterministic multicast, randomized efficient distributed detection, Localized multicast [12].

UTLSE and MTLSD: These two novels "mobility-assisted distributed" approaches are proposed to detect replicas in the mobile networks. Forwarding of data takes places only when the appropriate witnesses encounter each other. UTLSE has the concept of storing only one time location, where as MTLSD stores many time location claims. MTLSD [9] introduces more cooperation in order to detect replicas with high probability. The time location claims of tracked nodes are collected by MTLSD and it diffuses the collected claims in the witnesses. Thus it needs time synchronization [18].

Strengths:

- Excellent resiliency is provided
- Near optimal probability of detection involving low communication overhead
- Do not rely on specific routing protocol

Weaknesses:

- More communication and storage overhead
- Time synchronization is needed

In case of localized distributed detection [19], each node in the network can communicate with only one hop distant neighbor. For detection of replicas in the Localized manner [15], the proposed approaches are Spread & Receive, Extreme Efficient Detection (XED) and Efficient Distributed Detection (EDD).

SPREAD AND RECEIVE: Is the localized algorithm which has one hop communication and involves the introduction of two adversary models called, vanishing and persistent adversaries [17]. And they are used to evaluate the solutions. It involves two procedures, namely Spread and Receive. The first algorithm has four steps, in which, each sensor fills the message with its ID, its position claim, and the log history till that round, then messages to its neighbors. In the Receive procedure, there are three phases. Collection of messages from the neighbors, comparison of IDs & positions of the neighbors, and then check for the received log histories from the neighbors

Strengths:

- Avoids Network wide revocation
- Low communication overhead and storage overhead

Weakness:

- Every node should broadcast a message that has multiple time points and locations, at which the node encountered the other nodes in the network

XED: Involves the two steps as, offline and online steps [19]. In the offline approach, the security parameter and the hash function are stored at all the nodes. Two arrays are used, one for random numbers and other for the all the parameters to check the legitimacy of the random number which is received and arrays are initialized to zero. Each node contains the set of blacklisted nodes and which is initialized to be empty. In the online step, Random numbers between the two nodes are exchanged, prior to that, if a node encounters the node for the first time, if the node is blacklisted; it refuses to communicate with it. This approach is based upon the assumption that the replicated nodes won't communicate with each other, in the sense we assume there is no collusion of replicas.

Strengths:

- Constant communication cost is needed to detect replicas
- The Sensor node's location information is not necessary
- Minimum communication overhead

Weaknesses:

- Based on the assumption that, replicas wont communicate with each other
- Degrades capability of detection

EDD: Involves two steps as, offline and online steps [19]. In the offline step the two arrays are used. One is used to store the number of encounters with every node at the specified time interval. The other is used for the set containing IDs, if a node is considered as replica. The offline steps are carried out before the deployment of sensor nodes in the network. In the online step, each node maintains the counter to record elapsed time. And the approach depends on the fact that all the nodes broadcast its ID at periodical instants. This approach can be considered when the replicas in the network can communicate with each other. The solutions are based upon the "challenge-response" and the "encounter-number" [19].

Strengths:

- Detection is localized
- Effectiveness

- Avoiding synchronization of time and Revocation throughout the network

The two approaches though has its own strengths and weakness, yet it is difficult to choose the opt approach. Therefore, this research enabled towards conducting a comparative analysis of the methods in terms of two important parameters namely communication overhead and storage overhead. Communication overhead can be considered in terms of bits or records, it can be the number of records to be transmitted by each node. Storage overhead is the number of records, which should be stored at each node. Thus, these parameters should be minimized in order to have the better performance.

Fig 5 provides a comparative analysis of the approaches in terms of communication overhead. The Fig 5 shows the communication overhead for the different methods to detect replicas in the mobile sensor networks. It depicts that SPREAD AND RECEIVE (S&R), XED and EDD are having the lowest communication overhead.

Where,

N- Number of nodes in the network

CO-Communication Overhead

SO-Storage Overhead

Table 1 infers that the approach, EDD has the minimum communication and storage overhead and hence it is better to be opted.

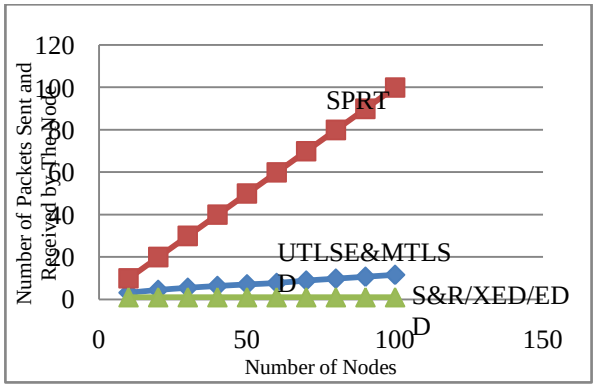

Fig 5: Comparison of Communication Overhead

Table 1 Comparison between the different approaches of replica detection

Algorithm	**CO**	**SO**
UTLSE and MTLSD	$O(N)$	$O(\sqrt{N})$
SPREAD AND RECEIVE	$O(1)$	$O(1)$
SPRT	$O(\sqrt{N})$	$O(1)$
XED	$O(1)$	$O(N)$
EDD	$O(1)$	$O(1)$

5. CONCLUSION

Due to the dependency of networks and wide popularity of wireless sensor networks, it is essential to effectively manage them without being attacked. This is because, there always prevails the threat of replication node attacks in wireless sensor networks which leads towards severe mishandling of the sensitive information and launching of other attacks during communication. If the replicas are left undetected, the entire network comes under control of intruder thus the attack must be detected as soon as possible. The aim of this paper is therefore to identify various approaches that exists to detect such replication attacks and also to analyze their strengths and weakness. Further, the paper put forth a comparative study of the existing approaches in terms of communication overhead and storage overhead. The comparative simulation results indicate that localized distributed approach is most preferable since it has low communication overhead and less storage overhead. Thus, it gives an efficient performance than the centralized and other types of distributed approaches as investigated in this part of the work. And further study can be done on time considerations and detection accuracy of the attacks in the network.

6. REFERENCES

[1] M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. Depend. Secure Comput., vol. 8, no. 5, pp. 685–698, Sep./Oct. 2012.

[2] M. Conti, R.Di Pietro, L. V. Mancini, andA.Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), Montreal, Canada, 2007,pp80–89.

[3] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. IEEE Symp. Security and Privacy (S&P), Oakland, CA, USA, 2005, pp. 49–63.

[4] K. Xing and X. Cheng, "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks," in Proc. IEEE Int. Conf. Computer Communications (INFOCOM), SanDiego, CA, USA, 2010, pp. 1–9.

[5] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 677–691, Jun. 2010.

[6] 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.

[7] C.-M. Yu, C.-S. 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.

[8] 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).

[9] Xiaoming Deng, Yan Xiong, and Depin Chen , "Mobility-assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks" 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications.

[10] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in Proc. IEEE Int. Conf. Network Protocols (ICNP), Princeton,NJ, USA, 2009, pp. 284–293.

[11] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," IEEE Trans. Syst., Man, Cybern. C, Applicat. Rev., vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[12] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[13] 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.

[14] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in Proc. Int. ICST Conf. Security and Privacy in Communication Networks (Securecomm), Nice, France, 2007, pp. 341–350.

[15] 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.

[16] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil attack in sensor networks: Analysis and defenses," in Proc. Int. Conf. Information Processing in Sensor Networks (IPSN), Berkeley, CA, USA, 2004, pp. 259–268

[17] M. Conti, R. D. Pietro, and A. Spognardi, "Wireless sensor replica detection in mobile environment," in Proc. Int. Conf. Distributed Computing and Networking (ICDCN), Hong Kong, China, 2012, pp. 249–264.

[18] Kyoung-lae, N., Serpedin, E., and Qaraqe, K. 2008. A New Approach for Time Synchronization in Wireless Sensor Networks: Pairwise Broadcast Synchronization. Wireless Communications, IEEE Trans. , vol.7, no.9, pp.3318-3322.

[19] Chia-Mu Yu, Yao-Tsou, Chun-Shien Lu, Member, IEEE, and Sy-Yen Kuo,Fellow, IEEE, Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks IEEE Trans. on Information And Security, vol 8, NO 5,May 2013