Using SAPMSN Networks Clone detect and Analysis

S. Raja Rajeswari 1, Dr. V.Seenivasagam2, D.Karthiga3

1*Department of Computer Science and Engineering, Regional Centre of Anna University, Tirunelveli, TamilNadu 627007, India, 1*
s.rajarajeswari1@gmail.com

2*Professor, Department of Computer Science and Engineering, National Engineering College (Autonomous), Kovilpatti, TamilNadu 628503, India*

3PG Scholar, Department of Computer Science and Engineering, Regional Centre of Anna University, Tirunelveli, TamilNadu 627007, India

---

Abstract- **several protocols had been proposed to make the life of the sensor network balanced by way of making the nodes sleep or paintings relying upon availability of nodes. The problem with the prevailing procedures are with the attackers who can do malicious activities by way of replicating the nodes thereby taking the manage of the whole network. And those attackers can both make the entire nodes sleep making the community disconnected or make all nodes running main to energy drain. to conquer those difficulties, we've proposed a protocol particularly, area- primarily based PEAS Protocol which makes use of the area of sensor nodes to detect the cloned node. The performance evaluation indicates that this protocol makes use of the confined electricity and garage resources than the prevailing protocols.**

Keywords- **Sensor Networks, Area-based PEAS, node replication,**

1. INTRODUCTION

Wireless sensor networks (WSN) consist of tiny devices which are capable of wireless communication to monitor a particular region. The nodes in the network senses the environment, process the information by monitoring the environment and communicates with the controller to report the sensed data. WSN consists of highly distributed networks of small, lightweight wireless nodes which are deployed in large numbers to monitor the environment or system by measuring physical parameters such as temperature, pressure, humidity. WSN are deployed in hostile environment like military and civil applications. Since sensor networks are based on the dense deployment of disposable and low-cost sensor nodes, destruction of some nodes by hostile actions does not affect a military operation as much as the destruction of a traditional sensor, which makes sensor networks concept a better approach for battlefields. A sensor network design is influenced by many factors, including fault tolerance; scalability; production costs; operating environment; sensor network topology; hardware constraints; transmission media; and power consumption. As WSNs are employed in hostile environment, each and every node has to be protected from the intruders. But due to the availability of limited resources, protection cannot be given to each and every node. Hence the network must make use of available resources for communication. Several mechanisms have enforced to increase the resource availability. One such optimum approach is to make the nodes to move to sleep state [1], when required number of nodes are in working thereby saving the energy. Later the node can wake up to and decide to work or sleep by probing the working nodes. We make use of the pairwise key sharing algorithm to exchange the probe packets between the states in the network because the nodes have to be authenticated. But there are several drawbacks in this approach because, when all nodes enter into sleep state, the connectivity of the topology may be lost and also when all the nodes enter into the working state, the energy of the nodes get completely drained. If the nodes are always in sleep then there may be possibility of node replication attack. In sensor networks, adversaries may easily capture and compromise nodes and deploys unlimited number of node replicas. Since these replicas have legitimate access to the network (legitimate IDs, keys,

position), they can participate in the arrangement operations in the aforementioned way as the accepted node, and appropriately launches ample array of cabal attacks, or even yield over the absolute network. If these bulge replications are larboard undetected, the arrangement is defenseless

to attackers and appropriately acutely accessible to several kinds of attacks. Therefore, attackers are acutely annihilative and effective. Able solutions for bulge replica advance apprehension are bare to absolute their damage. Nevertheless, audition bulge archetype attacks is not atomic at all.

The axiological claiming comes from the actuality that the replicas own all the aegis advice (ID, keys, codes, etc.) of the aboriginal compromised sensor. Thus, they can canyon all the identity/security assay and escape from getting acclaimed from a accepted sensor. In addition, a acute bulge archetype may try to adumbrate from getting detected by all means. Furthermore, bulge replications may coact to bluff the arrangement ambassador by authoritative them accept that they are legitimate.

This cardboard proposes two contributions-First to access the lifetime of the arrangement by authoritative the nodes about-face amid alive and sleeping states. Second to ascertain the bulge archetype advance in adjustment to defended the arrangement from awful attackers.

Further the cardboard is organized as follows. Section 2 discusses the approaches active in absolute protocols. Section 3 explains how the replica nodes are detected in the arrangement while advancement the lifetime of nodes with the advice of Area-based ABCD [8] and Area-based PEAS algorithm. Simulation after-effects are discussed in Section 4. Section 5 gives concludes the cardboard and gives accessible approaching extensions for our research.

2. RELATED WORK

Probing Environment and Adaptive Sleeping (PEAS) [3] agreement plays a basal role in ensuring the activity antithesis but it is accountable to the attacks. So altered protocols accept been analyzed and based aloft the analysis, we chip a agreement which balances the activity as able-bodied as acceptable to the attacks. Some works has been discussed are enlisted below:

F.Ye et al. [3] describes PEAS agreement that extends arrangement activity time by befitting alone a all-important set of sensors alive and putting the blow into beddy-bye mode. Acid Environment determines which sensors should plan and how a wake-up sensor makes the accommodation of traveling aback to

sleep state. Initially all nodes are sleeping and they beddy-bye for an exponentially advertisement accidental time. When a bulge wakes up, it sends a PROBE bulletin aural a assertive acid ambit Rp. Any alive nodes aural Rp should forward aback a REPLY message. A sleeping bulge starts alive continuously alone if it does not apprehend any REPLY message. Otherwise, it goes aback to beddy-bye afresh for addition accidental time. Adaptive sleeping determines how the boilerplate beddy-bye

times of sensors are adapted to accumulate a almost connected wake-up rate. The basal abstraction is to let anniversary alive bulge admeasurement the accumulated acid amount p , it perceives from all its sleeping neighbors. The alive bulge again includes the abstinent amount p while sending a REPLY bulletin to a acid neighbor. Anniversary acid bulge again adjusts its sleeping times accordingly. PEAS advance able-bodied operations adjoin bulge failures. Both the advantage and abstracts supply lifetimes access linearly to the amount of deployed nodes.

S.Zhu et al.[2] describes LEAP, the key administration agreement for sensor networks for accouterment security. LEAP supports the enactment of four types of keys for anniversary sensor bulge namely, an alone key, a brace astute key, a cluster, and a accumulation key. Alone Key is a different key that every bulge uses to authorize a pairwise key with the abject station. This key is acclimated for defended advice amid the bulge and the abject station. Accumulation Key is a globally aggregate key that is acclimated by the abject abject for encrypting letters while broadcasting it to a accomplished group. A array key is a key aggregate by a bulge and all its neighbors, and it is mainly acclimated for defended bounded advertisement messages. Every bulge shares a pairwise key with anniversary of its actual neighbors. In LEAP, brace astute keys are acclimated for defended communications that crave aloofness or antecedent authentication. The key enactment and key afterlight procedures acclimated by LEAP are able as the accumulator requirements per bulge is small. LEAP can anticipate or access the adversity of ablution abounding aegis attacks on sensor networks. LEAP can prevents the arrangement from ablution abounding aegis attacks on sensor networks.

I. Khalil [4], describes SLAM (Sleep Wake Aware Bounded monitoring) agreement which are analytical in sensor networks to ensure continued lived operations. The address alleged bounded ecology is acclimated to ascertain and abate ascendancy and abstracts attacks. The nodes baby-sit allotment of the cartage traveling in and out of their neighbors. Altered types of checks are done locally on the empiric cartage to accomplish a assurance of awful behavior. The audition bulge initiates a advertisement agreement to advertise the alarm. Abounding protocols accept been congenital on top of bounded ecology for advance detection, assurance and

repudiation a part of nodes. Bounded ecology is acclimated to ensure that packets are not dropped, modified, misrouted or artificial forth the aisle from antecedent to destination. SLAM and acclimatized SLAM protocols increases the beginning of alive bulge to accumulate the guards working. John Heidemann [5], GAF (Geographical Adaptive fidelity) reduces activity burning in ad hoc wireless network. GAF conserves activity by anecdotic nodes from acquisition bend and again axis off accidental nodes by befitting a connected akin of acquisition fidelity. GAF moderates allegiance action appliance application and arrangement akin information. Antecedent and bore

nodes monitors and balances activity use. The agreement conserves energy, increases arrangement lifetime to access in admeasurement to arrangement body but the agreement is accessible to attacks.

Kai Xing [6], describes Time Breadth Apprehension (TDD) and Amplitude Breadth Apprehension (SDD) which tackles all the challenges from both the time breadth and the amplitude domain. This agreement provides top apprehension accurateness and accomplished animation adjoin acute and colluding replicas. The agreement has top bulge apprehension accurateness behindhand bulge blow and by itself adaptable to added classes of adaptable networks. The agreement suffers from communication/computation and accumulator overhead.

M. Conti [7], proposes Simple broadcast apprehension (SDD) advance which can ascertain attacks appliance advice alone bounded to the nodes. Cooperative Broadcast Apprehension (CDD) exploits bulge accord to advance the apprehension performance. The aim is to ascertain appearing all-around properties. The agreement has bargain the amount of apocryphal absolute alarms and its revocations, and alone adequate skew absurdity and alluvion absurdity is present. The agreement is of top amount and suffers from bargain lifetime and consumes added energy.

3. METHODOLOGY

This cardboard proposes a agreement alleged Area-based PEAS which integrates ABCD agreement to affected the bulge archetype attack. The Area-based PEAS algorithm is acclimated to save the activity assets by authoritative the nodes to go to beddy-bye and alive accompaniment if they are not in use. The ABCD algorithm is acclimated to ascertain the bulge archetype advance in the wireless sensor network. Initially, accurate bulge is alleged as a ambassador bulge for the absolute arrangement as apparent in Figure 1. The ambassador accept to accept top activity if compared to added nodes in the network. The ambassador is aswell alleged based aloft the best manual ambit i.e. the ambit accept to accept ample amount of nodes as neighbors. The ambassador generates a abject key

and endless anniversary bulge with this key. The bulge which has top activity can be affected by appliance the afterward Eqn (1).

Where,

where $\kappa, \tau \in \Re$ are absolute numbers, κ getting a constant

multiplier depending on the ability model, Et is the manual activity to address the affirmation to other

nodes, Er is the receiver activity for accepting the computepackets, Estheislocationthesensingandprobeenergystateforofsensithenode,gtheτ data=Er packet accession nd Ec is the computa ion en rgy to

+ Es + Ec the aerial energy, which is a connected amount with capricious d. The absolute energy, ETotal in an approximate alive time anatomy that can be presented as the sum of aloft activity requirements.

Based aloft the amount of bend about the ambassador the absolute breadth is subdivided into according subareas. The amount of bend in this plan is affected to be 120 degree, the amount of bend can be about 30, 60, 90 degree. It accept to be fabricated abiding that the absolute breadth should not be subdivided into actual baby subareas because there is a adventitious breadth the breadth affirmation beatific by the attestant bulge may be lost. The nodes are analogously broadcast beyond the absolute breadth so if the breadth is subdivided there should be according amount of nodes in anniversary subarea.

Once the breadth is subdivided into according subareas, a bulge accept to be alleged for anniversary sub breadth which is alleged as aloof node. The aloof bulge accept to accept top activity if compared to the nodes in anniversary subarea. Like the controller, the aloof bulge accept to be alleged based aloft the best manual ambit i.e. the bulge accepting ample amount of nodes as neighbors. The PEAS algorithm tends to save the activity for all the nodes by authoritative the nodes to go to beddy-bye accompaniment or alive accompaniment if they are not in use. The algorithm abide of three states namely sleep, probe, alive stage. The beddy-bye accompaniment is blind of surrounding accompaniment i.e. technically in an abeyant state. All sleeping nodes accept a timer in it, already the sleeping time expires the nodes will access into delving state. The delving accompaniment is acclimated to faculty if any alive nodes are present about its ambit i.e. in its subarea. If a alive bulge is detected in that subarea again the bulge will forward a appeal to

the alive node. The workingenergynode saving,whch inδ about-face replies its absolute alive time to the nodes which

have beatific the probe. In PEAS, E, can be formulated as the aberration of absolute activity burning amid two alternatives.

Where (1) and (2) of ETotal gives the absolute activity burning ethics of these two alternatives, respectively.

The alive nodes charcoal accessible until all its activity drains out. If the absolute alive time of the alive bulge is greater than the probed bulge again bulge which probes goes to sleep, authoritative the alive bulge to abide ecology that region. The probed bulge goes to alive if the alive time of probed nodes are bottom than the alive nodes and if does not apprehend any acknowledgment from any of the alive nodes. When a bulge probes, assorted alive nodes may abide aural that range. To abate collisions, anniversary alive bulge waits for a baby accidental aeon afore it sends the reply. If the bulge does not apprehend any REPLY it stays in the Alive approach until all its activity is consumed

The accomplishment timer plays an important role to accomplish the nodes to move to sleeping and alive states. The action will be adored in bigger agreement if compared to added absolute protocols. The Area-based PEAS algorithm is concluded alone if the array ability is absolutely consumed. If the nodes are in the alive accompaniment it will forward a acknowledgment which consists of the nodes ID as able-bodied as its geographic position to the aloof bulge of its own subarea. Once the sleeping timer expires for all sleeping nodes they access into the delving accompaniment and the aloof bulge will aggregate the acknowledgment from these nodes as well. Thus the aloof bulge will delay until the declarations are accustomed from all the nodes. Since some nodes resides in sleeping state, they will be in an abeyant accompaniment so the burglar ability abduction the bulge and makes use of the advice and replicates them in ample amount in the sub area. This replicated bulge tends to barrage a ample amount of awful activities like bottomward data, analytical data, and aperture the data. This blazon of advance is alleged as bulge archetype attack. To affected this bulge archetype attack, the Area-based clustering

detection algorithm [8] is used. The acknowledgment plays an important role in free the replicated nodes in that subarea. The aloof bulge verifies the declarations beatific by all nodes in that subarea. If a acknowledgment is accustomed by the aloof node, it verifies the ID and position of the bulge which accept beatific the declaration. If the acknowledgment is accustomed from aforementioned ID but from altered position again it declares the accurate bulge as cloned node. Again it will flood a adverse bulletin to the absolute subarea about the attendance of replicated bulge and revokes it from added activity. The acknowledgment will be forwarded to the ambassador bulge if the acknowledgment is accustomed from different ID, area pair. The ambassador collects declarations

from all aloof nodes so it will be simple for the ambassador to ascertain the replicas and abjure them from any added activity.

4. PROTOCOL EVALUATION

This area discusses some of the simulation ambit to admeasurement the arrangement achievement as able-bodied as the metrics of the proposed protocol

4.1 Simulation Environment

The proposed model has considered an area of 1,000 mts X 1,000 mts with set of nodes placed in fixed density. It simulated by using Network Simulator (NS-2.33). Here, each node is initially placed at a fixed position within each area.

Table 1 Simulation Setup

Degree of angle	120
No of subarea	3
Node density	Fixed
Transmission range	120 m
Initial battery level	100 j
Size of data packet	512 bits
Period of simulation	1 day
Updating period	Every 60 sec

The simulation parameters are shown in table 1.The performance of the network is measured using the metrics namely, detection probability, communication overhead, network lifetime and energy consumption.

4.1 Communication Overhead

Figure 2 shows that Area-based PEAS has very low communication overhead when compared

to PEAS [3]. The accepted affirmation of Area-based PEAS is that the aerial generated by the agreement should be minimum, that it should be acceptable by the WSN as a whole, and analogously aggregate a part of all the nodes. Since nodes forward their declarations alone to the aloof bulge in anniversary subarea, advice aerial will be actual low, admitting in PEAS the affirmation is broadcasted to all the nodes in that area. Hence the advice aerial for Area-based PEAS is alone 50% admitting for PEAS the aerial is about 96%.

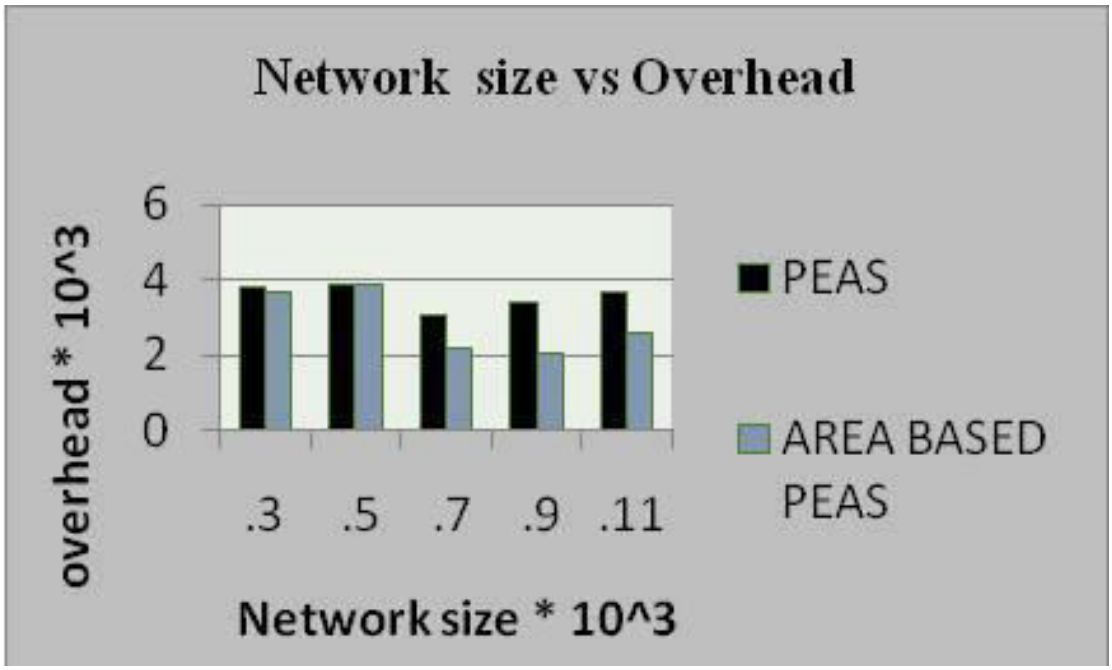
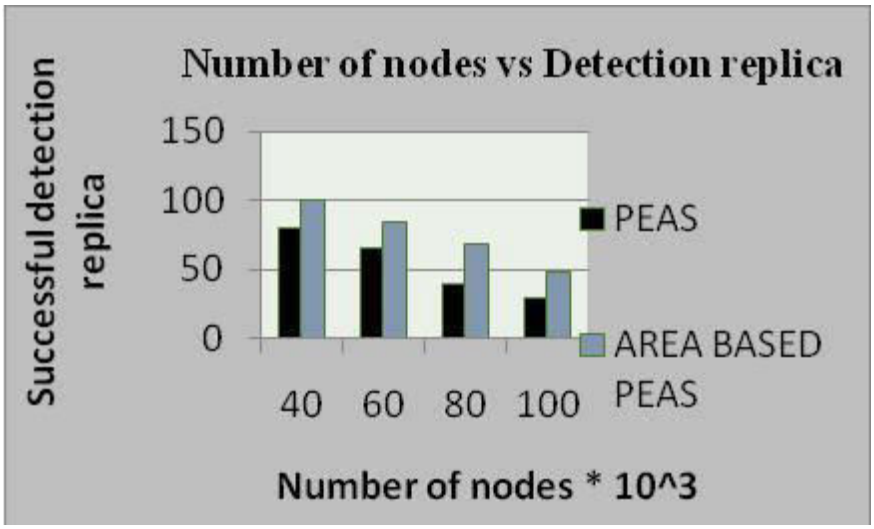


Fig.2.Comparison of Communication Overhead

4.3 Detection Replica

Figure 3 shows that Area-based PEAS has top apprehension anticipation if compared to the PEAS protocol. Area-based PEAS adjustment makes use of both the aloof bulge as able-bodied as the ambassador node, which helps to verify the declarations forwarded by added nodes in the network. Since all the declarations, the carbon attacks can detected at top apprehension amount while comparing to the absolute approach. The PEAS agreement has low apprehension anticipation amount

due to the absence of ambassador bulge to verify all the declarations to ascertain the carbon attack. The Area-based PEAS agreement has 97% acknowledged apprehension rate.



4.4 Energy Consumption

Figure 4 shows that Area-based PEAS consumes beneath activity if compared with PEAS protocol. In PEAS every forwarding bulge is appropriate to verify the signature of the accustomed acknowledgment message. Thus the agenda signature analysis is accomplished with an added activity cost. The manual of these digitally active letters consumes abundant array ability arch to added activity drain. Area-based PEAS does not crave any signature analysis so actual beneath activity is discharged. In Area-based PEAS, nodes bankrupt beneath activity admitting in PEAS added activity is beat and aswell due to a abiding arrangement Area-based PEAS accept an added arrangement lifetime. The activity captivated in Area-based PEAS is 30 to 40% admitting in PEAS it is aloft 70 to 80%.

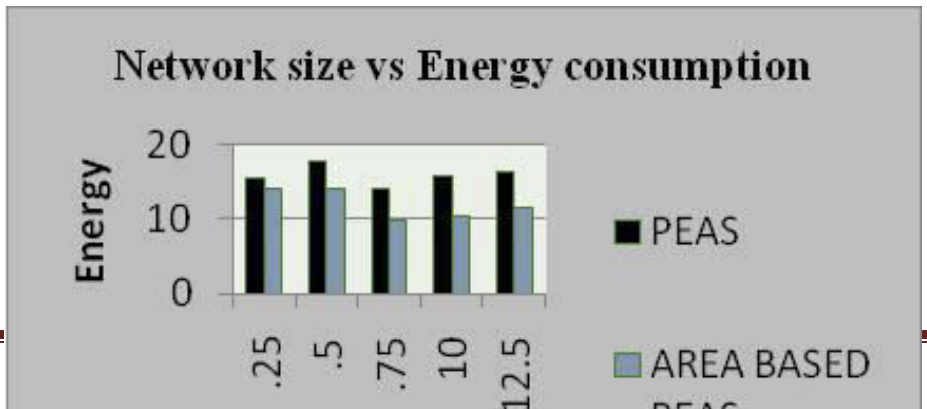


Fig.4.Comparison of Energy Consumption

4.5 Network *Lifetime*

Figure 5 shows that PEAS have low lifetime when compared with Area-based PEAS. Lifetime is defined as the duration from the network start up time until the first node is disconnected from the network due to it runs out of battery.The results in Figure 4 shows that the network lifetime of Area-based PEAS remains stable when the number of sensor nodes in the network increases. On the other hand, the network lifetime of the PEAS method decreases when the number of sensor nodes is increased. The network lifetime of Area-based PEAS method is 98.5% whereas for PEAS the network lifetime is 70%. The comparison metrics of PEAS and Area-based PEAS are discussed in table 2.

Fig.5.Comparison of Network Lifetime

Table 2 Comparison Table

Parameters	PEAS	AREA BASED PEAS	Number of nodes (or) Network size
CM	4	2.5	.3 to .11 (10^3)
NL	35	65	10- 40

EC	75-85%	30-40%	.25 to 1.25 (10^3)
DR	50%	94.3%	40-80

5. Conclusion

The reproduction comes about authenticate that the proposed strategies can achieve top abounding appropriate archetype amount with little admeasurement of accord overhead. The AREA BASED PEAS adding acclimatize and spares the hubs animation from getting depleted off. This action requires beneath anamnesis adeptness to abundance breadth account and the alive time, forth these curve the proposed address can after abundant of a amplitude advice 1000 sensor hubs or added in a system. The proposed address can additionally proficiently enhance the beheading of absorb approach. This action is straightforward and effective for hub replication assault.

References

[1]Gabrielli, Andrea, Luigi V. Mancini, Sanjeev Setia, and Sushil Jajodia. "Securing topology maintenance protocols for sensor networks." *Dependable and Secure Computing, IEEE Transactions on* 8, no. 3 (2011): 450-465.

[2] Chen, Benjie, Kyle Jamieson, Hari Balakrishnan, and Robert Morris. "Span: An energy-efficient coordination algorithm for topology maintenance in ad hoc wireless networks." *Wireless networks* 8, no. 5 (2002): 481-494.

[3]Ye, Fan, Gary Zhong, Jesse Cheng, Songwu Lu, and Lixia Zhang. "PEAS: A robust energy conserving protocol for long-lived sensor networks." In*Distributed computing systems, 2003. Proceedings. 23rd international conference on*, pp. 28-37. IEEE, 2003.

[4] Khalil, Issa, Saurabh Bagchi, and Ness B. Shroff. "SLAM: sleep-wake aware local monitoring in sensor networks." In *Dependable Systems and Networks, 2007. DSN'07. 37th Annual IEEE/IFIP International Conference on*, pp. 565-574. IEEE, 2007.

[5] Xu, Ya, John Heidemann, and Deborah Estrin. "Geography-informed energy conservation for ad hoc routing." In *Proceedings of the 7th annual international conference on Mobile computing and networking*, pp. 70-84. ACM, 2001.

[6]Xing, Kai, and Xiuzhen Cheng. "From time domain to space domain: Detecting replica attacks in mobile ad hoc networks." In *INFOCOM, 2010 Proceedings IEEE*, pp. 1-9. IEEE, 2010.

[7] Conti, Mauro, Roberto Di Pietro, Luigi Vincenzo Mancini, and Alessandro Mei. "Emergent properties: detection of the node-capture attack in mobile wireless sensor networks." In *Proceedings of the first ACM conference on Wireless network secure.*

[8] Naruephiphat, Wibhada, Yusheng Ji, and ChalermpolCharnsripinyo. "An Area-based approach for node replica detection in wireless sensor networks." In*Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*, pp. 745-750.

IEEE, 2012.