Clone attack detection using Area-based PEAS Protocol for Wireless Sensor Networks

S. Raja Rajeswari [1], Dr. V.Seenivasagam[2], D.Karthiga[3]

[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

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

***Abstract*- Several protocols have been proposed to make the lifetime of the sensor network balanced by making the nodes sleep or work depending upon availability of nodes. The problem with the existing approaches are with the attackers who can do malicious activities by replicating the nodes thereby taking the control of the entire network. And these attackers can either make the entire nodes sleep making the network disconnected or make all nodes working leading to energy drain. To overcome these difficulties, we have proposed a protocol namely, Area- based PEAS Protocol which makes use of the location of sensor nodes to detect the cloned node. The performance analysis shows that this protocol makes use of the limited energy and storage resources than the existing 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 network operations in the same way as the legitimate node, and thus launches large variety of insider attacks, or even take over the entire network. If these node replications are left undetected, the network is unshielded to attackers and thus extremely vulnerable to several kinds of attacks. Therefore, attackers are severely destructive and effective. Efficient solutions for node replica attack detection are needed to limit their damage. Nevertheless, detecting node replication attacks is not trivial at all.

The fundamental challenge comes from the fact that the replicas own all the security information (ID, keys, codes, etc.) of the original compromised sensor. Thus, they can pass all the identity/security check and escape from being distinguished from a legitimate sensor. In addition, a "smart" node replication may try to hide from being detected by all means. Furthermore, node replications may collude to cheat the network administrator by making them believe that they are legitimate.

This paper proposes two contributions- First to increase the lifetime of the network by making the nodes switch between working and sleeping states. Second to detect the node replication attack in order to secure the network from malicious attackers.

Further the paper is organized as follows. Section 2 discusses the approaches employed in existing protocols. Section 3 explains how the replica nodes are detected in the network while maintaining the lifetime of nodes with the help of Area-based ABCD [8] and Area-based PEAS algorithm. Simulation results are discussed in Section 4. Section 5 gives concludes the paper and gives possible future extensions for our research.

2. RELATED WORK

Probing Environment and Adaptive Sleeping (PEAS) [3] protocol plays a vital role in ensuring the energy balance but it is liable to the attacks. So different protocols have been analyzed and based upon the analysis, we integrated a protocol which balances the energy as well as sustainable to the attacks. Some works has been discussed are enlisted below:

F.Ye et al. [3] describes PEAS protocol that extends system functioning time by keeping only a necessary set of sensors working and putting the rest into sleep mode. Probing Environment determines which sensors should work and how a wake-up sensor makes the decision of going back to sleep state. Initially all nodes are sleeping and they sleep for an exponentially distributed random time. When a node wakes up, it sends a PROBE message within a certain probing range R_p. Any working nodes within R_p should send back a REPLY message. A sleeping node starts working continuously only if it does not hear any REPLY message. Otherwise, it goes back to sleep again for another random time. Adaptive sleeping determines how the average sleep times of sensors are adjusted to keep a relatively constant wake-up rate. The basic idea is to let each working node measure the aggregate probing rate 'p', it perceives from all its sleeping neighbors. The working node then includes the measured rate 'p' while sending a REPLY message to a probing neighbor. Each probing node then adjusts its sleeping times accordingly. PEAS maintain robust operations against node failures. Both the coverage and data delivery lifetimes increase linearly to the number of deployed nodes.

S.Zhu et al.[2] describes LEAP, the key management protocol for sensor networks for providing security. LEAP supports the establishment of four types of keys for each sensor node namely, an individual key, a pair wise key, a cluster, and a group key. Individual Key is a unique key that every node uses to establish a pairwise key with the base station. This key is used for secure communication between the node and the base station. Group Key is a globally shared key that is used by the base station for encrypting messages while broadcasting it to a whole group. A cluster key is a key shared by a node and all its neighbors, and it is mainly used for secure local broadcast messages. Every node shares a pairwise key with each of its immediate neighbors. In LEAP, pair wise keys are used for secure communications that require privacy or source authentication. The key establishment and key updating procedures used by LEAP are efficient as the storage requirements per node is small. LEAP can prevent or increase the difficulty of launching many security attacks on sensor networks. LEAP can prevents the network from launching many security attacks on sensor networks.

I. Khalil [4], describes SLAM (Sleep Wake Aware Local monitoring) protocol which are critical in sensor networks to ensure long lived operations. The technique called local monitoring is used to detect and mitigate control and data attacks. The nodes oversee part of the traffic going in and out of their neighbors. Different types of checks are done locally on the observed traffic to make a determination of malicious behavior. The detecting node initiates a distributed protocol to disseminate the alarm. Many protocols have been built on top of local monitoring for intrusion detection, trust and repudiation among nodes. Local monitoring is used to ensure that packets are not dropped, modified, misrouted or forged along the path from source to destination. SLAM and adapted SLAM protocols increases the threshold of working node to keep the guards working. John Heidemann [5], GAF (Geographical Adaptive fidelity) reduces energy consumption in ad hoc wireless network. GAF conserves energy by identifying nodes from routing perspective and then turning off unnecessary nodes by keeping a constant level of routing fidelity. GAF moderates fidelity policy using application and system level information. Source and sink nodes monitors and balances energy use. The protocol conserves energy, increases network lifetime to increase in proportion to network density but the protocol is vulnerable to attacks.

Kai Xing [6], describes Time Domain Detection (TDD) and Space Domain Detection (SDD) which tackles all the challenges from both the time domain and the space domain. This protocol provides high detection accuracy and excellent resilience against smart and colluding replicas. The protocol has high node detection accuracy disregarding node collision and naturally extensible to other classes of mobile networks. The protocol suffers from communication/computation and storage overhead.

M. Conti [7], proposes Simple distributed detection (SDD) attack which can detect attacks using information only local to the nodes. Cooperative Distributed Detection (CDD) exploits node collaboration to improve the detection performance. The aim is to detect emergent global properties. The protocol has reduced the number of false positive alarms and its revocations, and only acceptable skew error and drift error is present. The protocol is of high cost and suffers from reduced lifetime and consumes more energy.

3. METHODOLOGY

This paper proposes a protocol called Area-based PEAS which integrates ABCD protocol to overcome the node replication attack. The Area-based PEAS algorithm is used to save the energy resources by making the nodes to go to sleep and working state when they are not in use. The ABCD algorithm is used to detect the node replication attack in the wireless sensor network. Initially, particular node is selected as a controller node for the entire network as shown in Figure 1. The controller must have high energy when compared to other nodes in the network. The controller is also selected based upon the maximum transmission range i.e. the range must have large number of nodes as neighbors. The controller generates a base key and loads each node with this key. The node which has high energy can be calculated by using the following Eqn (1).

$$C(n) = \left(ETotal(d)\right) \quad .. \qquad (1)$$

Where,

$$ETotal(d) = \kappa d\alpha + \tau \quad .. \qquad (2)$$

$$ETotal = Et + Er + Es + Ec \quad .. \quad (3)$$

where κ ,τ ∈ℜ are real numbers, κ being a constant multiplier depending on the power model, Et is the transmission energy to transmit the claim to other nodes, Er is the receiver energy for receiving the packets, Es is the sensing energy for sensing the data packet arrival and Ec is the computation energy to compute the location and probe state of the node, τ = Er + Es + Ec the overhead energy, which is a constant value with varying d. The total energy, ETotal in an arbitrary active time frame that can be presented as the sum of above energy requirements.

Based upon the degree of angle around the controller the entire area is subdivided into equal subareas. The degree of angle in this work is assumed to be 120 degree, the degree of angle can be around 30, 60, 90 degree. It must be made sure that the entire area should not be subdivided into very small subareas because there is a chance where the location claim sent by the witness node may be lost. The nodes are uniformly distributed across the entire area so when the area is subdivided there should be equal number of nodes in each subarea.

Once the area is subdivided into equal subareas, a node must be selected for each sub area which is called as watcher node. The watcher node must have high energy when compared to the nodes in each subarea. Like the controller, the watcher node must be selected based upon the maximum transmission range i.e. the node having large number of nodes as neighbors. The PEAS algorithm tends to save the energy for all the nodes by making the nodes to go to sleep state or working state when they are not in use. The algorithm consist of three states namely sleep, probe, working stage. The sleep state is unaware of surrounding state i.e. technically in an inactive state. All sleeping nodes have a timer in it, once the sleeping time expires the nodes will enter into probe state. The probe state is used to sense if any working nodes are present around its range i.e. in its subarea. If a working node is detected in that subarea then the node will send a request to the working node. The working node which in turn replies its total working time to the nodes which have sent the probe. In PEAS, energy saving, δ_E, can be formulated as the difference of total energy consumption between two alternatives.

$$\delta E = ETotal^{(1)} - Etotal^{(2)} \text{ ---} \qquad (4)$$

Where (1) and (2) of ETotal gives the total energy consumption values of these two alternatives, respectively.

The working nodes remains operative until all its energy drains out. If the total working time of the working node is greater than the probed node then node which probes goes to sleep, making the working node to continue monitoring that region. The probed node goes to working if the working time of probed nodes are lesser than the working nodes and if does not hear any reply from any of the working nodes. When a node probes, multiple working nodes may exist within that range. To reduce collisions, each working node waits for a small random period before it sends the reply. If the node does not hear any REPLY it stays in the Working mode until all its energy is consumed.

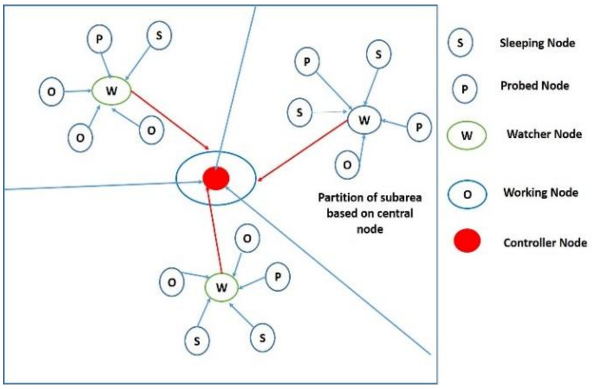

Fig.1. Architectural diagram

The expiry timer plays an important role to make the nodes to move to sleeping and working states. The energy will be saved in better terms when compared to other existing protocols. The Area-based PEAS algorithm is terminated only when the battery power is fully consumed. When the nodes are in the working state it will send a declaration which consists of the nodes ID as well as its geographic position to the watcher node of its own subarea. Once the sleeping timer expires for all sleeping nodes they enter into the probe state and the watcher node will collect the declaration from these nodes as well. Thus the watcher node will wait until the declarations are received from all the nodes. Since some nodes resides in sleeping state, they will be in an inactive state so the intruder might capture the node and makes use of the information and replicates them in large number in the sub area. This replicated node tends to launch a large number of malicious activities like dropping data, tampering data, and leaking the data. This type of attack is called as node replication attack. To overcome this node replication attack, the Area-based clustering detection algorithm [8] is used. The declaration plays an important role in determining the replicated nodes in that subarea. The watcher node verifies the declarations sent by all nodes in that subarea. When a declaration is received by the watcher node, it verifies the ID and position of the node which have sent the declaration. If the declaration is received from same ID but from different position then it declares the particular node as cloned node. Then it will flood a conflicting message to the entire subarea about the presence of replicated node and revokes it from further activity. The declaration will be forwarded to the controller node if the declaration is received from unique ID, location pair. The controller collects declarations from all watcher nodes so it will be easy for the controller to detect the replicas and revoke them from any further activity.

4. PROTOCOL EVALUATION

This section discusses some of the simulation parameters to measure the network performance as well 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 general requirement of Area-based PEAS is that the overhead generated by the protocol should be minimum, that it should be sustainable by the WSN as a whole, and evenly shared among all the nodes. Since nodes send their declarations only to the watcher node in each subarea, communication overhead will be very low, whereas in PEAS the claim is broadcasted to all the nodes in that area. Hence the communication overhead for Area-based PEAS is only 50% whereas for PEAS the overhead is nearly 96%.

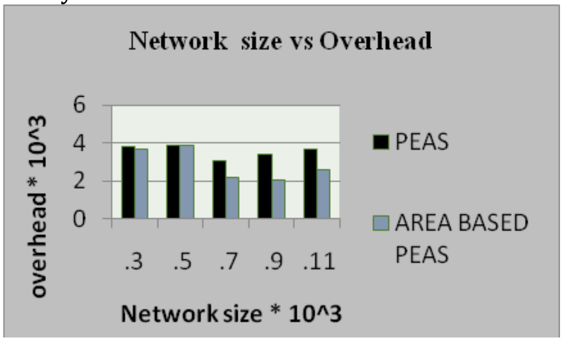

Fig.2.Comparison of Communication Overhead

4.3 Detection Replica

Figure 3 shows that Area-based PEAS has high detection probability when compared to the PEAS protocol. Area-based PEAS method makes use of both the watcher node as well as the controller node, which helps to verify the declarations forwarded by other nodes in the network. Since all the declarations, the clone attacks can detected at high detection rate while comparing to the existing approach. The PEAS protocol has low detection probability rate due to the absence of controller node to verify all the declarations to detect the clone attack. The Area-based PEAS protocol has 97% successful detection rate.

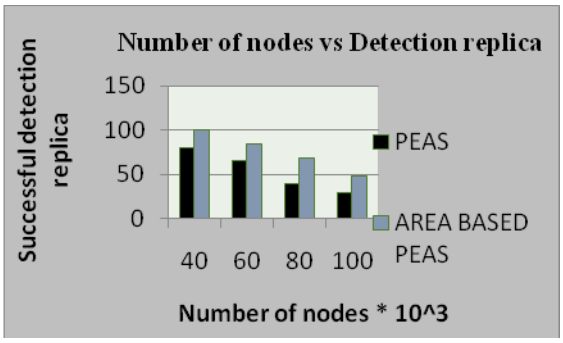

Fig.3.Comparison Detection rate

4.4 Energy Consumption

Figure 4 shows that Area-based PEAS consumes less energy when compared with PEAS protocol. In PEAS every forwarding node is required to verify the signature of the received declaration message. Thus the digital signature verification is attained with an additional energy cost. The transmission of these digitally signed messages consumes much battery power leading to more energy drain. Area-based PEAS does not require any signature verification so very less energy is discharged. In Area-based PEAS, nodes exhaust less energy whereas in PEAS more energy is exhausted and also due to a stable network Area-based PEAS have an increased network lifetime. The energy consumed in Area-based PEAS is 30 to 40% whereas in PEAS it is above 70 to 80%.

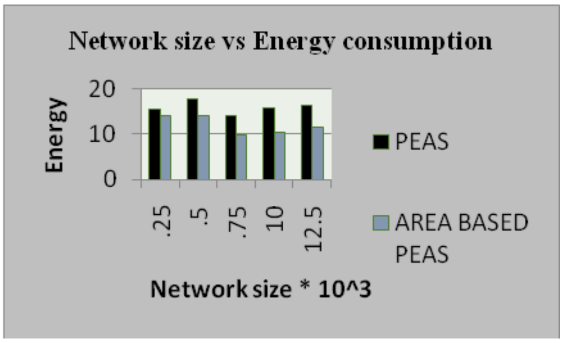

Fig.4.Comparison of Energy Consumption

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.

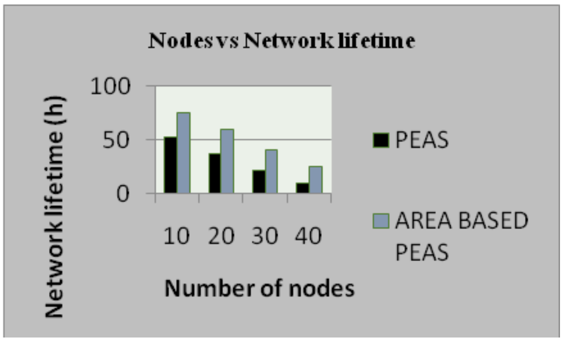

Fig.5.Comparison of Network Lifetime

Table 2 Comparison Table

Parameters	PEAS	AREA BASED PEAS	Number of nodes (or) Network size
C_M	4	2.5	.3 to .11 (10^3)
N_L	35	65	10-40
E_C	75-85%	30-40%	.25 to 1.25 (10^3)
D_R	50%	94.3%	40-80

5. Conclusion

The simulation results show that the proposed methods can achieve high successful detecting replica rate with small amount of communication overhead. The AREA BASED PEAS algorithm balance and saves the nodes energy from being drained off. This method requires less memory capacity to store location declaration and the working time, thus the proposed method can easily support 1000 sensor nodes or more in a network. The proposed method can also efficiently improve the performance of centralize approach. This method is simple and efficient for node replication attack.

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 security*, pp. 214-219. ACM, 2008.

[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.