Energy Aware Replica Node Detection using Location and Interval Time in Wireless Sensor Networks

R. Sivaraj
PG Scholar, Department of Computer Science and Engg
Kongu Engineering College, Erode
Anna University Chennai, India

R. Thangarajan
Professor, Department of Computer Science and Engg
Kongu Engineering College, Erode
Anna University Chennai, India

***Abstract*–A Wireless Sensor Network (WSN) consists of several sensor nodes that are deployed in a aggressive environment to monitor and record the changes that take place in certain parameters of the environment. Sensor nodes that can communicate with each other over a wireless channel can be captured and compromised by an adversary. After such a compromise an adversary can replicate a few sensor nodes, and insert arbitrary number of replicas in the network field to undermine the operation of the network. Several clone detection protocols have been proposed in the literature as a framework to maximize the lifetime and security of the wireless sensor network. These are based on device types, deployment strategies, detection methodologies and detection ranges and try to mitigate the threat against wireless sensor networks. The Location Claim Approach is an effective clone detection protocol based on grid deployment. It can detect the clone nodes by sending each node's location claim (location and ID) to other nodes in a predetermined zone. However there are certain limitations in the current study. The unnecessary forwarding of location claim between the sensor nodes will increase the claim storage, communication and computation overhead. Hence in the proposed study the methodology is developed to overcome these problems by making the deployment location more accurate. This is achieved by assigning the time interval for all sensor nodes. Hence in this proposed work, an erroneously deployed node which is marked as untrusted node finishes the neighbor discovery before the time interval. Therefore it can be remarked as trusted node. Finally the total energy consumed by the proposed method consumes less energy.**

***Keywords* – Clone attacks, replica nodes, wireless sensor networks, location claims, deployment time interval.**

I. INTRODUCTION

Wireless sensor networks are deployed in aggressive environments that are used for monitoring and recording the environmental changes. Wireless sensor networks play a major role in both the military and civil applications [1]. In Wireless sensor networks sensor nodes are used to measure the environmental conditions like temperature, wind speed, air direction, pressure, tracking the moving object. These nodes are very compact and low cost. Due to their low cost it is possible to deploy thousands of sensor nodes in a particular group of area. These nodes will be highly autonomous and it require only minimal amount of supervision. Since tiny sensor nodes in WSNs have meager resources for computation, communication, power, and storage, it is challenging to provide efficient security functions and mechanisms for WSNs.

Sensor nodes that are deployed in harsh environment are captured and compromised easily by an adversary. After such compromise the attacker can extract the credential information (node id, nodes location, codes and keying materials) from the captured nodes to build a replica node and inserts an arbitrary number of replicas in to the deployment area such that the adversary can expand the compromised areas by employing the clones. This is termed as clone attack. The replica nodes could be authenticated as legitimate node and to launch various types of attacks like injecting false data, corrupting data aggregation, dropping data packets selectively. Thus, it is essential to detect clone nodes promptly for minimizing their damages to WSNs. Therefore, clone attackers are severely harsh and efficient and effective solutions for clone attack detection are needed to limit their harms.

The simplest protective measure against the clone attacks is to prevent an adversary from extracting secret key materials from compromised nodes by virtue of tamper-resistant hardware. However, the hardware-based protective measures are too expensive to be practical for resource-restricted sensor nodes. For that various kinds of software based clone detection protocols have been proposed to detect and prevent the replica nodes. Based on device types, detection methodologies, deployment strategies, detection ranges [9] several clone detection protocols have been proposed to detect the replica nodes.

The existing clone detection protocols such as Location Claim approach is the effective detection protocol that is based on grid deployment knowledge is used to detect the replica nodes by considering nodes location and Id. In basic approach the node detected in a zone that is far away from a predetermined zone over a threshold distance then it is suspected as a replicated node. If a genuine node located erroneously in a zone that is out of threshold distance it yields a detection error. To overcome these problems the Location Claim Approach is used to reduce these detection error rates. The erroneously deployed node is treated as untrusted node. The replica node contains the node Id as same as the captured node. By forwarding the Location Claim (i.e. Id and nodes location) from both trusted and untrusted node to the set of neighbors for detecting the

clone nodes. If the node in a zone receives two different conflicting claims (different location with the same node Id) means they conclude that node is a clone node. Forwarding of location claim from untrusted will increase high claim storage, communication and computation overhead.

To overcome these limitations of existing approaches incorporate deployment time interval mechanism with previous approach. In the proposed methodology introduce time interval for each and every sensor nodes to reduce the overhead of previous approaches. Hence battery is the sole energy for the sensor nodes, so that finally calculate the total amount of energy consumed [13] by the network field for the replica node detection process.

II. RELATED WORK

The related papers of WSN have many researches and works in different aspects such as energy consumption, throughput, and packet delivery ratio. A simple solution to defend against clone attacks [2] is to let the base station collect the neighborhood information (e.g. neighbors list, location, Id, etc.) from each and every sensor and monitor the network in a distributed manner.

In [3], Parno et al proposed a centralized detection scheme for detecting the replica nodes. It is a Base-Station based scheme that it is a basic clone detection scheme. Presumably, each and every node can send IDs and estimate the locations of its neighbors to a base station. If there is a collision of IDs in far distinct locations at the base station, then the base station can indentified the corresponding sensor node as a clone node that can be easily revoked from the network by broadcasting an authentic command. However there are certain drawbacks with the current study. If the base station fails to detect, BS can controlled by an adversary or if the base station will crash it leads to degrade the network performance.

To overcome the security issues of the previous approach Brooks et al proposed a centralized clone detection technique under the assumption that the keys are randomly predistributed [4]. Before deployment each sensor node is preloaded with the set of k keys. Each sensor node has a key ring of k keys taken randomly from the pool. Base station contains the copy entire key pool. Base station can collects the key usage statistics from the network, if a key is used for multiple times over a predefined threshold, then the BS revokes the corresponding key as a clone key.

The two probabilistic detection protocols [3] which is based on a centralized detection scheme. First, In Randomized Multicast (RM) scheme each sensor announces its locations and each of its neighbors can send a copy of that claim to randomly selected nodes (i.e. witness node) and exploiting the birthday paradox effect to detect the clone nodes. Witness node can receive two different location claims with same ID and then considered the corresponding node as replica node that could be revoked from the network. Second, Line Selected Multicast (LSM) scheme forward the location claim to travel from node x to node y, it must pass through several intermediate nodes as well. If these intermediate nodes also store the location claim, then several lines are drawn across the network. If a conflicting location claim ever crosses the line, then the node present at the intersection will detect the conflict and initiate a revocation broadcast.

The social fingerprint [5] mechanism for detecting the clone attacks by computing each sensor node with social fingerprint by extracting the neighborhood characteristics of the sensor nodes and check the legitimacy of the originator for each message sending. The fingerprint generation is based on superimposed S-disjunctive code. Fingerprint verification can be done in both the neighboring sensor and base station. It requires additional complex process to add new sensor nodes.

The distributed detection scheme called Random Walk [6] mechanism for detecting replica nodes in wireless sensor networks. In RAWL protocol, each node broadcasts a signed location claim then each of the node's neighbors probabilistically forwards the location claim to some of the randomly selected nodes. Each randomly selected node sends a message containing the claim to start a random walk in the network, and the node that receive the claims are selected as witness nodes [12] and will store the claim. If any witness node receives different location claims for a same node ID, it can use these claims to revoke the replicated node. This leads to increase the communication overhead of these protocols.

The two grid-based clone detection schemes, i.e., single deterministic cell (SDC) and parallel multiple probabilistic cells (P-MPC) [7], which improve the collision probability of RM by using grid information given to each node. In SDC, the IDs and locations of the neighbors are forwarded to a single zone that is determined from one-way hash function with a node ID as input. However, in P-MPC, the pair information is forwarded to multiple zones that are determined in the same way. Then, every node checks whether or not the IDs received from the other nodes are in conflict. Although P-MPC requires a higher communication cost than SDC, it can detect clones by virtue of nodes in the other zones, even in the case where all nodes in a given zone are compromised by an adversary.

Choi et al proposed a clone detection scheme [10], called SET, to detect clones by set operations, such as intersection and union, of exclusive subsets of IDs in a network. Since the set of IDs are divided by clustering regional sensor nodes after deployment, an intersection of distinct subsets must be empty. If there is a nonempty intersection, then the BS will be reported by corresponding cluster heads to detect cloning activities.

A WSN configured by grid deployment can place sensor nodes in a predetermined zone and utilize their locations to detect clones. In basic approach if a node is detected in a zone that is far from its predetermined zone over a threshold distance, then it is suspected as a replicated node. If a genuine node is located erroneously in a zone that is out of the threshold distance, then the basic approach may yield a detection error (a false alarm) by determining it as a clone node.

To reduce these detection error rates, author proposed Location Claim Approach [8] mechanism by letting the

neighbors of an erroneously deployed node send out its location to the nodes in the predetermined zone in an authenticated manner. The schemes reduce detection errors significantly by checking a collision of ID in two zones.

III. PROBLEM DEFINITION

The main issue in wireless sensor networks is the security. In wireless sensor networks an adversary may launch a clone attack by replicating the captured nodes to enlarge the compromised areas employing clones. Thus the clone nodes promptly damage the wireless sensor network by launching various attacks like inject false data, corrupting data, etc. So an effective clone detection mechanism is devised to enhance the network lifetime by considering the energy consumption. Recent clone detection technique called Location Claim Approach (LCA) is used to detect clone nodes based on nodes deployment location and ID's of every sensor node. In WSN forwarding the location claim from both trusted and untrusted node will reduce the detection error rate. Battery is the sole energy source for the sensor node.

Hence based on clone detection and completion time calculate total energy needed for this detection and process. However there is a drawback with this approach. Forwarding location claim between neighboring sensor nodes will cause high claim storage, communication and computation overhead. Hence in this proposed work, deployment time Interval is added for every node that present in a particular group. This timestamp indicates that every node should finishes the neighbor discovery before time and untrusted node will be remarked as trusted node.

IV. PAPER OVERVIEW AND CONTRIBUTUION

In this paper, the sensor nodes are static [9] and that the network topology, is well known to the base station. In addition, the researcher assumes that the communications between the sensor nodes in the network and base station will be based on multi-hop communications. Each sensor node in the network is required to monitor its detection area in anticipation of an intrusion by an attacker. The attacker can launch clone attacks by replicating the compromised nodes.

In WSNs sensor nodes only forward messages for their trusted neighbors. When the deployment is not very accurate, many benign nodes may be rejected by their neighbor nodes for message forwarding, and the sensor network may be poorly-connected or even partitioned when the application requires high resilience against clone attacks.

To address this problem, sensor nodes also forward messages from untrusted neighbors as long as they provide provable evidence that they are not replica nodes. The message includes the location of the sensor node requesting
message forwarding. The messages from an untrusted node will be sent to a pre-determined location for replica detection [8]; when two conflicting pieces of evidence reach this location, the replica will be detected.

In existing work, due to inaccuracy in deployment the trusted node will be treated as untrusted node. By forwarding the location claims from untrusted node between the sensor nodes in a predetermined zone will increase the claim storage, computation and communication overhead. The proposed clone detection technique will improve the detection capability and the process is based on several stages.

A. Deployment

First we define the deployment zone of a deployment zone of a group as a circle centered at the group deployment point with the radius Rz. The radius Rz is the adjustable parameter from that the group size will increase or decrease. The sensor node u from the deployment zone of a group G_u can discovers its real location, L_u .Equation (1) shows, if the sensor node u resides outside its home zone it produces the location claim

$$C_u = \{u||L_u||sig_u\}, \quad (1)$$

Where sig_u is the signature generated by using u's random numbers.

B. Neighbor Discovery

After deployment of sensor node u each and every sensor node can discovers the set of neighbors N(u) and asks for an authenticated location claim from every sensor node (i.e. $V \in N(u)$). The sensor node finds out the set of neighbor nodes by using Euclidean distance is shown in Equation (2) formula,

$$d(x.y) = \sqrt{(x_2 - x_1)^2 - (y_2 - y_1)^2} \quad (2)$$

If the distance between the two nodes is within its transmission range means, that node will accepted as a neighbor node. Neighbor discovery process model is shown in fig.1. x_1, x_2 and y_1, y_2 are the coordinates of two sensor nodes. The sensor node v sends the location claim C_v to sensor node u, if the sensor node found in a zone is placed outside its home zone. Other the sensor node v sends u the message M_v, it contains information about that particular sensor nodes.

The node u can check every node $\in N(u)$ to see that it is deployed in a right place. This can be done by checking whether the distance between the L_v and the deployment group G_v is less than R_z. The sensor node u will mark node v as untrusted since it is outside its home zone. Otherwise the node v will marked as trusted node.

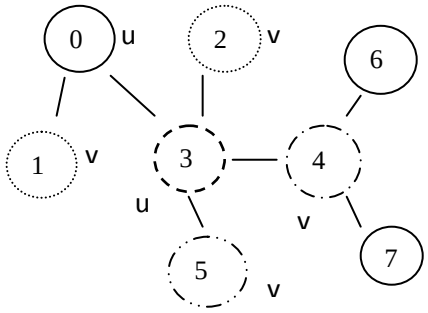

Figure 1. Neighbor Discovery

TABLE 4.1 NEIGHBOR DETAILS

Source	Neighbors	x-pos	y-pos	Distance
0	2,3,4	55	25	222
3	4,5	160	746	186
4	7.6	76	345	197

In Table 4.1 shows the neighbor details of each and every sensor nodes by considering nodes location. By maintaining the neighbors detail, the nodes present in the network maintain its own network topology.

C. Deployment Time Interval

When a group G_v of nodes are deployed, they will be pre-loaded with a time stamp T_v that is digitally signed by a trusted server. This time stamp indicates that the sensor nodes in G_v should finish neighbor discovery before time T_v. If they try to setup neighbor connections with other nodes after time T_v, they are considered to be untrusted nodes. The time stamp T_v should be a function of the deployment time T, the time T_c is the time needed for compromising and replicating a node. Specifically, the network operator should set,

$$T + T_n + \epsilon < T_v < T + T_n + T_c - \epsilon. \quad (3)$$

T_n is the neighbor discovery time, where Tn refers to the time at which the node starts the neighbor discovery process to the time the node finishes the neighbor discovery process, such that no nodes should have clocks too fast to accept the new node, but no new node could be compromised and accepted in time. Consider a particular node u. Assume that its neighbors N(u) has been marked as trusted or untrusted using the deployment location, according to one of our schemes. We attempt to distinguish more benign nodes from those marked as untrusted by checking the deployment times of those nodes. Specifically, for every node $v \in N(u)$ that is marked as untrusted, node u checks whether v was discovered before T_v , the deployment time of G_v . If yes, node v will be re-marked as trusted. Thus the lifetime of the network and energy consumed by each sensor node will be improved by using this technique.

D. Claim Forwarding

Each and every sensor node forward its own location and ID to the neighboring sensor nodes for clone detection process. The sensor node u will also forward regular messages from untrusted neighbor node v. After receiving the node v's location claim C_v to the sensor node u, it sends the location claim C_v to the deployment point of group G_v. Since the group G_v contains many number of sensor nodes.

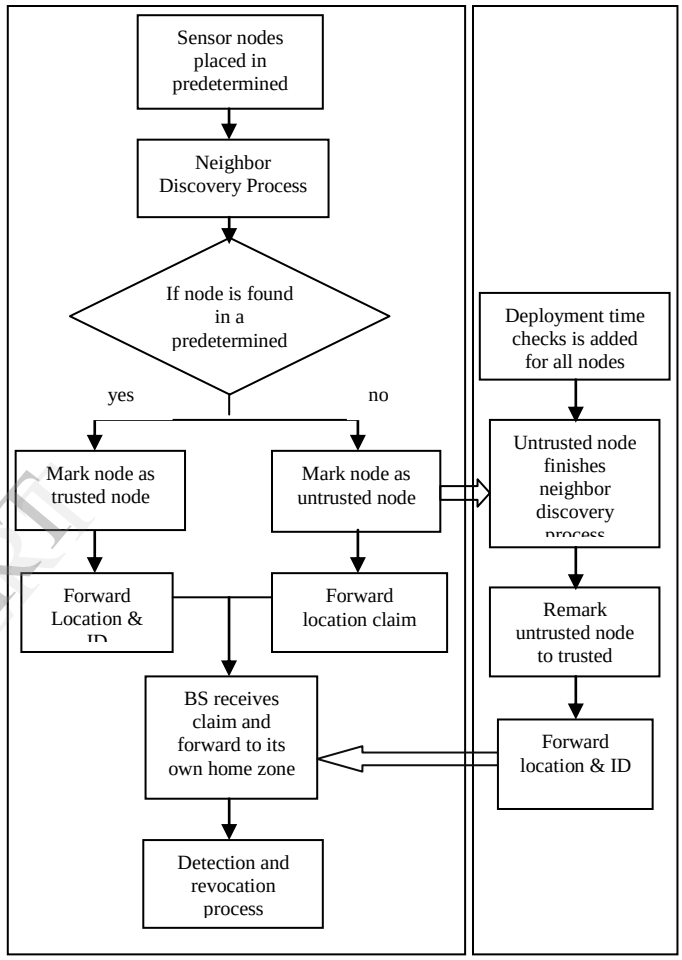

Figure 2. Shows the workflow model of the proposed clone detection technique.

E. *Detection and Revocation*

In these phase once an authenticated location claim reaches the home zone of node v, it will be dispatched throughout the network (i.e. node v's home zone). Every node present in the group G_v will receive the two different location claim (i.e. C_v) with the same ID. At that point collision occurs. Since every node forward their own location and ID to the neighboring sensor nodes. The two conflicting location claim will be used as an evidence to revoke node v from the network.

V. SIMULATION ENVIRONMENT AND RESULT ANALYSIS

The simulation tool used here is network simulator tool version 2.34 to implement the proposed methodology. Static network consists of 50 mobile nodes, where each node uses the IEEE 802.11 as a medium access control protocol that is deployed in a predetermined zone. The total network topology area is 1600 x 800 with the nodes transmission range is 250 m.

Total simulation time for this experiment is 1000s. The size of the data packet for each node transferred is up to the maximum of 500 packets. Protocol used here is DSDV in which each node maintains its own network topology by update its routing table. The initial energy for the static nodes is 100 J. The CBR traffic type is used for initial broadcast between the two nodes.

VI. RESULT ANALYSIS AND DISCUSSION

The energy consumption of the sensor nodes is reduced, the network lifetime and the overall performance of network is improved is shown in the below result. Fig. 3 and Fig. 4 reveal that the proposed DTI methodology outperforms the existing LCA approach for the replica detection process by considering energy consumption.

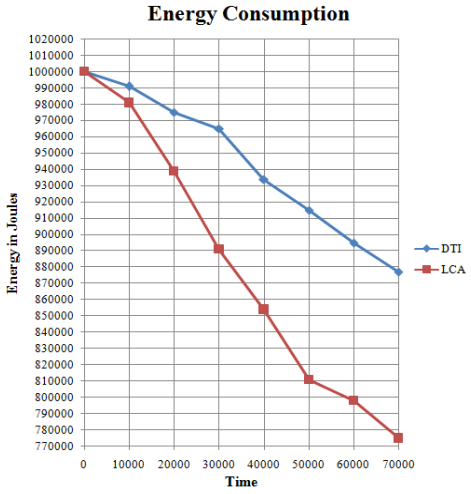

Figure 3. Comparison of Energy Consumption

Since unnecessary forwarding of location claim between the sensor node increases storage overhead, it leads to high packet loss. By deploy the DTI for all sensor nodes will reduce the storage overhead, thus the throughput of the overall network is improved as compared to the existing approach.

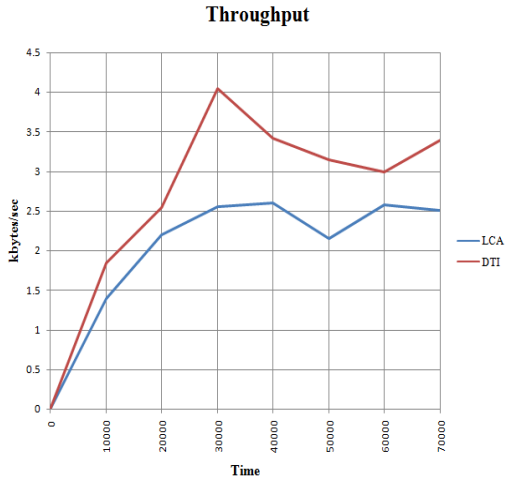

Figure 4. Comparison of Throughput

VII. CONCLUSION

In wireless sensor networks clone attack may play a major role to insert number of replicas by an adversary to undermine the operation of the network. The Location Claim approach (LCA), effective clone detection mechanism based on grid deployment knowledge can detect the clone attacks by considering the nodes location and ID. For, clone detection process this scheme can consume lesser energy than the existing clone detection scheme. By making the deployment locations more accurate, the network operator can arbitrarily reduce the overheads of our schemes without loss of security. At the same time, our approach is flexible and robust when there are errors, with costs rising only gradually when more errors are introduced.

The LCA approach can be further improved by integrating Deployment Time Interval (DTI) mechanism that aid to add time interval for each and every node to overcome the problems such as claim storage, communication and computation overhead. By using this DTI technique erroneously deployed node (untrusted node) can be detected and to remark this node as trusted node. By using the proposed technique each node can consumes lesser energy as compared to existing approach and thus the lifetime of network will be improved.

REFERENCES

[1]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless sensor networks: a survey," *International Journal of Computer and Tele Communications Networking-Elsevier*, 38(4):393–422, March 2002.

[2]. A. Becher, Z. Benenson, and M. Dornseif, "Tampering with motes:Real–world physical attacks on wireless sensor networks," in *Proc. of the 3rd International Conference on Security in Pervasive Computing (SPC)*, pages 104-118, 2006.

[3]. B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in Proc. *IEEE Symp. Security Privacy*, May 2005, pp. 49–63.

[4]. 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.*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[5]. K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real–time detection of clone attacks in wireless sensor networks," in *Proc. ICDCS*, pp. 3–10, 2008.
[6]. 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.
[7]. 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.
[8]. J. W. Ho, D. Liu, M. Wright, and S. K. Das, "Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks," *Ad Hoc Netw*., vol. 7, no. 8, pp. 1476–1488, Nov. 2009.
[9]. Kwantae Cho, Minho Jo, Taekyoung Kwon, Hsiao–Hwa Chen, and Dong Hoon Lee, "Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks," *IEEE Sys. Journal*., vol. 7, no. 1, Mar. 2013.
[10]. H. Choi, S. Zhu, and T. F. L. Porta, "SET: Detecting node clones in sensor networks," in *Proc. Security Privacy Commun. Netw. Workshops*, 2007, pp. 341–350.
[11]. Z. Li and G. Gong, "DHT–based detection of node clone in wireless sensor networks," in Proc. *1st Int. Conf. Ad Hoc Netw*., 2009, pp. 240-255.
[12]. C. A. Melchor, B. Ait–Salem, P. Gaborit, and K. Tamine, "Active detection of node replication attacks," *Int. J. Comput. Sci. Netw. Security*, vol. 9, no. 2, pp. 13–21, Feb. 2009.
[13]. A. Boonsongsrikul, S. Kocijancic and S. Suppharangsan, "Effective energy consumption on wireless sensor networks: survey and challenges," *IEEE Pub.* pp. 469–473, May. 2013.