ISSN: 2229-6948(ONLINE)
DOI: 10.21917/ijct.2016.0205

TAWS: TABLE ASSISTED WALK STRATEGY IN CLONE ATTACK DETECTION

J. Sybi Cynthia[1] and D. Shalini Punithavathani[2]
[1]*Department of Computer Science and Engineering, C.S.I. Institute of Technology, India*
E-mail: [1]cynthia.sybi@gmail.com
[2]*Department of Computer Science and Engineering, Government College of Engineering, Tirunelveli, India*
E-mail: [2]shalini329@gmail.com

Abstract

Wireless Sensor Networks (WSNs) deployed in the destructive atmosphere are susceptible to clone attacks. Clone attack in wireless sensor network is a complicated problem because it deployed in hostile environments, and also the nodes could be physically compromised by an adversary. For valuable clone attack detection, the selection criteria play an important role in the proposed work. In this paper, it has been classified the existing detection schemes regarding device type, detection methodologies, deployment strategies and detection ranges and far explore various proposals in deployment based selection criteria category. And also this paper provides a review of detection methodology based on various clone attack detection techniques. It is also widely agreed that clones should be detected quickly as possible with the best optional. Our work is exploratory in that the proposed algorithm concern with table assisted random walk with horizontal and vertical line, frequent level key change and revokes the duplicate node. Our simulation results show that it is more efficient than the detection criteria in terms of security feature, and in detection rate with high resiliency. Specifically, it concentrates on deployment strategy which includes grid based deployment technique. These all come under the selection criteria for better security performance. Our protocol analytically provides effective and clone attack detection capability of robustness.

Keywords:

Clone Attacks, Wireless Sensor Networks, Node Replication Detection

1. INTRODUCTION

A spatially distributed autonomous sensor in Wireless Sensor Network (WSN) was used to monitor physical or environmental conditions and also cooperatively used to pass their data through the network to a main location. A single tiny device encapsulates sensing, computation and communication in WSN [1]. In many applications a large number of these sensors can be networked that require unattended operations, hence producing a WSN. It is not possible to protect anything unless one clearly understands the things that to be protected. Things to be considered for networks are server, workstation, storage systems, routers, switches, etc. Threats are of various types and it includes viruses and attacks. Network security concerned with protection, integrity and availability of information. The security trinity involves prevention, detection and response. Prevention is always better than cure. Secondly, detection should be done as quickly as possible before the attack cause large harm in a network. Finally, the third in the trinity is response and it should be made immediately with necessary action like revoking process etc.

In fact, the applications of WSN are quite plenty. For example, military and civil applications involve intrusion detection, weather monitoring, security, target field imaging and tactical surveillance etc. A sensor node is captured by an intruder in clone attack (also called as a node replication attack) and the information was copied into the intruder's own sensor. Then it deploys in the intelligently decided places. Node replication means that it is eventually detected by the node when two intersection path that originates the same ID (identity) with different network position. In fact, if during a check witness will trigger a revocation protocol for a node. Cloned nodes made a number of attacks that are explained by several researchers. The information on the network can be leaked out by the cloned node. The false information can be injected or data can be changed passing through the cloned nodes by an intruder. To detect potential tampering is impossible to monitor the nodes constantly. Therefore, to combat those attacks, real time cloned detection is essential. The ease of deploying sensor networks contributes to their appeal. They can quickly scale to a larger configuration, since administrators can simply drop new sensors into the desired locations in the existing network [2]. To join the network, new nodes require neither administrative intervention nor interaction with a base station; instead, they typically initiate simple neighbor discovery protocols by broadcasting their pre-stored credentials (e.g., their unique ID and/or the unique ID of their keys).

The remainder of the paper is organized as follows: Section 2 discusses clone attack scenario. Section 3 gives an overview of security issues. Section 4 presents a classification of selection criteria. Section 5 explains about the related work. Section 6 analyzes the proposed methodology. Simulation results verifying our analysis of the clone attack detection protocol are presented in section 7 and discussion takes place in section 8. Finally, section 9 gives conclusions and possible future extensions of our research.

2. CLONE ATTACK SCENARIO

In clone attack, an intruder compromises some of the nodes in the network, replicates and then arbitrary number of replicas were inserted. Many internal attacks were held in the network by the intruders. Due to cost considerations, it is left unattended after deployment. Each node forwards the randomly selected witness nodes to the neighbor and the collision arises if the network had two nodes with same ID but in a different location and clone attack was detected in WSN as shown in Fig.1. However, many approaches have been proposed to detect clone attacks which make an essential detection on abnormal sign caused by replicas. The features that made easier for clone attack on the network includes deterministic, non-resilient to smart attack and central control.

2.1 DETERMINISTIC

In each execution, the witnesses of a node are fixed in the protocol in deterministic protocols. The adversary can easily

compromise the nodes and deploys number of replicas if any protocols are deterministic. So it will be vulnerable to clone attacks. The deterministic scheme loses its resiliency.

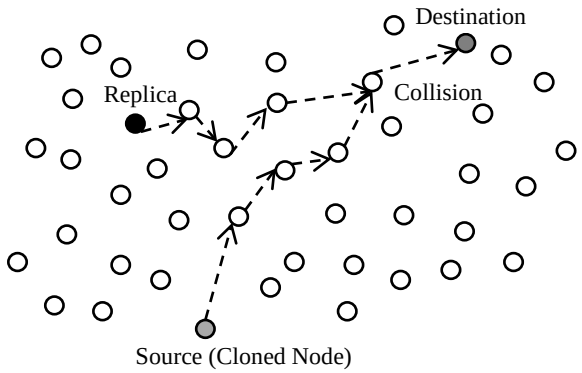

Fig.1. Clone Attack in WSN

2.2 NON-RESILIENT TO SMART ATTACK

Critical witness nodes are the nodes that contain more information about the sensor nodes in the network. If the adversary captures these witness nodes, then the network will be moving on critical state. The non-resilient property makes a way for an adversary to smart attack.

2.3 NEED OF CENTRAL CONTROL

It is necessary for the central base station to receive all nodes' neighbor list and its claim location with ID in the centralized scheme network. The base station should check all nodes for the list of conflicting claims and it confirms complexity in the network. The major creating problem in centralized approaches was single-point of failure. If a smart attack is done by an intruder in the base station, then the entire network gets collapsed. If the central node fails the reliability will be dropped off and the data collection performance suffers a lot. Thus, it increases the rate of clone attack in the network.

3. SECURITY ISSUES

Security issues in computer networks were the most important areas of research with the fantastic propagation of networking, and the appearance of a series on sensitive functions. Hiding sensitive communication from trespasser as well as afford a trustworthy means for authenticating oneself is a very important area of research.

3.1 NON-DETERMINISTIC

The witnesses of a node are different, i.e. not fixed in each execution of the protocol. The adversary cannot compromise a node's witness by compromising a subset of nodes in the network. In neighbor witness, the witness selection may be deterministic, so randomly selected nodes for witness to be non-deterministic. In each round, each witness node will be given a different probability to be the witness node. But all the nodes have equal probability to be witness nodes, so that the adversary may not get more information from the particular critical witness node and avoid the network from critical state.

3.2 FULLY DISTRIBUTED

Each sensor in the network schedules its own activity concern probabilistically with node degree in the fully distributed scheme. The scheme never depends on the base station. Since the nodes surrounding the base station are subject to an undue communication burden that may shorten the network's life expectancy. So it is necessary for a fully distributed network to prevent clone attack.

3.3 RESILIENCY

The normal operation in computer networking challenges to provide and maintain an acceptable level of service is resiliency. Threats in the range were different and it may be from simple to complex targeted attacks. This network resilience covers a maximum topics. The plausible risks and challenges must be recognized and suitably resilience metrics have to be protected by service definition. By specific context, resiliency and survivability are interchangeably utilized.

4. CLASSIFICATION OF SELECTION CRITERIA

To collect and verify evidence of clones, the detection schemes are classified into four types. They are device type, detection methodology, deployment strategies and detection range. Each were categorized as shown in Fig.2, the taxonomy of selection criteria and explained briefly [3]. In the selection criteria, device type is further classified into static, mobile and similarly detection methodology classified into centralized and distributed. Then deployment strategies are again classified into random uniform and the grid. Finally the detection range is further classified into whole and local.

4.1 STATIC VS. MOBILE

A sensor network may be either stationary or mobile in nature. In static, the sensor nodes are deployed randomly, but after deployment their position do not change and it is said to be stationary (static) positioned. On the other hand, in mobile, the sensor nodes can be moved on their own even after deployment and also they can interact with the physical environment by controlling their own movement.

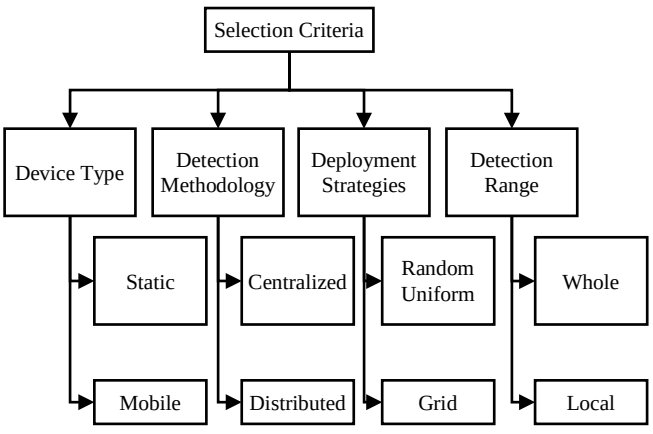

Fig.2. Taxonomy of Selection Criteria

4.2 CENTRALIZED VS. DISTRIBUTED

In centralized, time sharing system and time sharing OS provide the security. But in distributed networking, three approaches to security are identity of users, client system authenticate themselves and user to prove identity.

4.3 RANDOM VS. GRID

During deployment the grid will be more effective than the random. The grid deployment makes sure of non-deterministic and it is helpful to make away the adversary from smart attack. The grid-based torus structure (i.e., a grid graph that is wrapped in both north-south and east-west directions) is made to simplify the analysis [4]. A grid-based deployment provides high resiliency and connectivity. In some protocols, the random deployment scenario makes high collision probability and also relatively high cost for storage.

4.4 WHOLE VS. LOCAL

The WSN network requires a higher communication cost since location claim is forwarded to a multiple zone and a powerful adversary could compromise a whole zone. The localization technique requires an effective concentration on local and no need on the whole in the network. And thus communication cost and computation cost may be reduced.

5. RELATED WORKS

5.1 CLONE ATTACK DETECTION TECHNIQUES

Clone detection scenario depends on node movement, topology, traffic pattern, direction, geographical location, routing, etc. Normally, clone detection technique needs security requirements in order to control security breaches. The clone attack detection technique works with the following steps. Initially nodes in the network broadcast the location claim with signed. Each node's neighbor forwards probabilistically the claim. The forwarded claim was received by randomly selected some nodes. Now this few selected nodes start a walk in the network and the passed node will be the witness nodes. The claim will be stored only in the witness nodes. When the witness nodes receive the claim, it checks for ID and location. If it has found same ID for two nodes with different locations in the network, it implies that network contains or affected by clone. It is necessary for revoking action immediately. This is the general step to be worked out for the clone attack detection technique.

At a high level, RAWL works with the following steps in each execution (recall that our four protocols all can be scheduled to run periodically): (1) Each node broadcasts a signed location claim. (2) Each of the node's neighbors probabilistically forwards the claim to some randomly selected nodes. (3) Each randomly selected node sends a message containing the claim to start a random walk in the network, and the passed nodes are selected as witness nodes and will store the claim. (4) If any witness receives different location claims for a same node ID, it can use these claims to revoke the replicated node.

The cost may be acceptable for small networks. However, for large networks the communication and memory costs per node are $O\left(n\sqrt{n}\right)$ and $O\left(\sqrt{n}\right)$. In RM/LSM each, a node announces its location to neighbor in random multicast. Neighbor sends a copy of location claim to the set of randomly selected witness nodes. Birthday paradox predicts the clone nodes. LSM passing location claim through intermediate nodes and store location claim and a line was drawn across a network. A geographic routing was used [2], but it has a very high communication overhead. The emergent nature of these algorithms makes them extremely resilient, to active attacks, and both protocols seek to minimize power consumption by limiting communication, while still operating within the tremendously limited memory capacity of typical sensor nodes. In a sensor network, a SET [5] is modeled as a non-overlapped sub region. Each node has a unique identifier. Since each node contains information about the neighbors, in each sub region, it forms an exclusive subset. It checks for empty or non-empty subset of the network after intersection of any two subsets. If empty, then it shows that the network is free from node replication attack. If it is found to be non-empty subset, then it implies that an adversary replicates nodes into the network. It means that the network is affected by clone attack. Thus clone is detected. Communication cost is low since the subset division procedure eliminates redundancies in node location reports. ID's appear in different exclusive subgroups. Based on a random value the network was partitioned into clusters and formed trees to check for subgroup's ID's are common. And then SET may have false detections when insidious leaders in the trees forge ID's not in their clusters. In RED (Randomized, Efficient & Distributed) protocol [6], claims sent to witness ID will be lost and nodes deployed after first network deployment could not be used as witnesses until all node's information is updated. It uses geographic routing. In this Active protocol, each node actively seeks to learn whether another node is replicated or not eradicate the memory dissemination issue, while keeping the communication complexity. But in the existing protocol, no storage is done on the node. This protocol actively tests the node by using relays [7]. The various clone attack detection techniques were discussed in this section as shown in Fig.3.

However each existing protocol has its own merit as followed:

In RM/LSM scheme, the communication and space can be saved by reducing the amount of location claims sent on the network. Detection with high probability is done by using only a constant number of line segments [2]. Here storage requirement is reduced by using time synchronization.

SET [5] has the concept which dealt with random seed and thus the adversary cannot predict the node which was selected. When the number of nodes in the network increases, it converges quickly by the expected number of rounds. This protocol uses a re-selection of node in each execution based on a new seed. It is not necessary for the root to keep the subset uninterruptedly.

RED [6] has a benefit that the claim sent to the witness and if ID is no longer present then the claim sent will be lost. This protocol uses relay which is the node that the neighbor closest to the destination.

RAWL [4] have much probability with grid in the centre in which witness will be equally distributed in the network. The reselection of nodes in each execution is done.

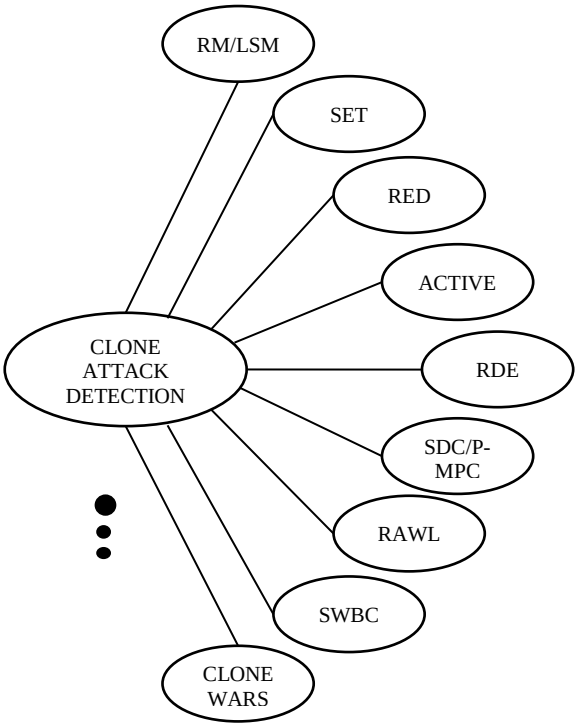

Fig.3. Various Clone Attack Detection Schemes

During the detection procedure in RDE (Randomly Directed Exploration) technique, each node having a neighbor list with a maximum hop limit selects random neighbors and forwards the claim message. The previous claiming message's transmissions form a direction. The intermediate node follows the direction to forward the claim and explore the claiming message. Thus clone attack detection technique in RDE, works. And thus it can efficiently detect cloned node in the denser sensor networks and also minimizes the memory requirement. Each node only needs to know its neighbor nodes. During handling a message, a node compares its own neighbor-list with the neighbor-list in the message, checking if there is a clone. If intermediate nodes are compromised then the forwarding message loses its credentialed. It relies on identity-based public key system and thus guarantees authentication of nodes identity. The performance varies according to the routing type [8]. The localized multicast analyzes two variant approaches. They are Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC), and their name implies differ in the number of cells to which a location claim is plotted and the manner in which the cells are selected. SDC is a deterministic approach. The P-MPC is more robust to node compromise than SDC. The communication overhead is unchanged in P-MPC as in SDC [9]. In RAWL (Random Walk) protocol, if a different location claim for a same node ID was received by any witnesses then it detects clone. To some of the randomly selected nodes, each node's neighbor probabilistically forwards the claim [4]. RAWL comes under the NDFD (Non-Deterministic Fully Distributed) protocol for maximum benefits. In SWBC (Security in Wireless Sensor Networks by Broadcasting Location Claims) technique, network integrated by root node with its neighboring nodes. Root node selection is the node which has maximum number of neighboring nodes. By having their own location they will transfer their location to their root nodes [10]. So the root will differentiate the sub-nodes and the adversary nodes separately. It has a successful detection rate. But number of messages stored after detecting adversary attack percentage are more when compared to LSM and RED and thus storage space required is large. The clone war technique [11] comes under grid deployment strategy. Each sensor records ID and location of met neighbor. It compares the met neighbor with its own record. It checks for the hop count of the neighbor details for hop count of previous jump. If a hop count of previous jump is not two-hop, then it checks the location and ID and identify clone attack on the network. It gives better detection rate and also overcomes computation, communication and memory overheads.

5.2 SELECTION CRITERIA BASED ON DEPLOYMENT STRATEGY

The device type, detection methodology, deployment strategy and detection ranges are the different selection criteria that have taken into consideration. In this paper, we discuss SDW (Static-Distributed-Whole) selection criteria with deployment strategy. SDW is taken from the device type, detection methodology and detection range as shown in Fig.4. All the schemes in the protocol have chosen the device type as static and detection methodology as distributed in the selection criteria. None of the existing techniques have concentrated on the four combinations of selection criteria on the whole. Selection criteria based on deployment strategy compared between random and grid with the combination of static distributed whole as shown in Fig.5.

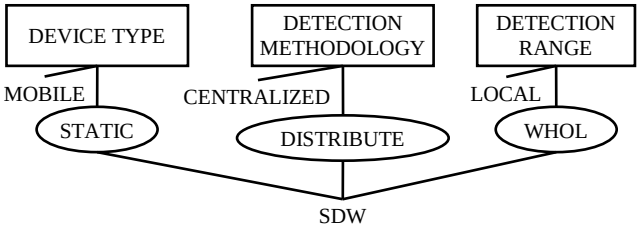

Fig.4. Combination selected from Selection Criteria

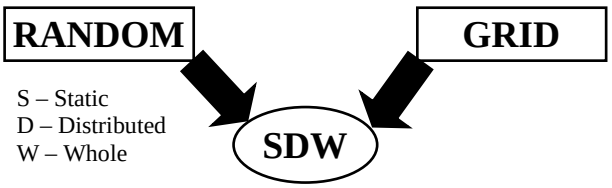

Fig.5. Selection Criteria based on deployment strategy

5.2.1 Random Based Deployment Strategy:

In RM/LSM protocol, a network randomly deployed on the unit square and the average distance will be between any two randomly chosen nodes. It is assumed that the standard unit disc bidirectional communication model and it can adjust the communication range [2]. In RED protocol, it is assumed that the nodes are distributed in the network area in a random way and the geographic routing protocol was simulated. The relay node will be the neighbor's closest to the destination. The routing stops when no node is closer to the destination than the current node. In RDE technique, nodes are randomly deployed, and there exist some outside borders of the network. The techniques used in random based deployment strategies were explained [6], [8].

When reaching some border in the network, the claiming message can be removed directly. Apparently, the randomly directed exploration protocol is highly memory-efficient. It does not rely on broadcasting. As a result, no additional memory is required to suppress broadcasting flood. The Fig.6 shows the various deployment based strategy schemes were reviewed.

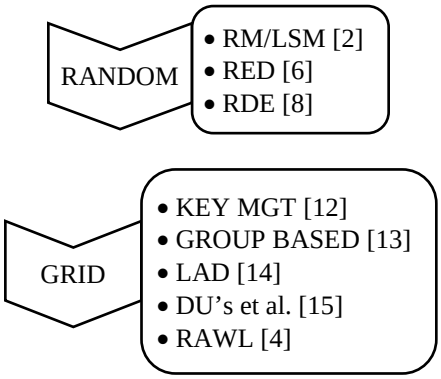

Fig.6. Reviewed paper from an existing deployment based strategy

5.2.2 Grid Based Deployment Strategy:

The key pre-distribution where key information is distributed among all sensor nodes prior to deployment. It is possible for the keys to be decided a priori if it is known about the nodes which are to be staying in the same neighborhood before deployment. Because of random deployment, the set of neighbors deterministically might not feasible and it does not exhibit desirable network resilience [12]. In this scheme, the key pre-distribution with deployment knowledge can substantially improve a network connection (secure link), resilience against node capture and reduce the amount of memory required. Here the nodes are fairly evenly distributed in the whole region.

In group based deployment technique, the sensor nodes in the same group are supposed to be deployed from the same point at the same time. However, we assume the resident points of the sensor nodes in the same group follow the same probability distribution function [13]. We assume that the groups are evenly and independently deployed on a target field such that in each node the probability of finding in each equal size region can be made approximately equal. Memory usage can be determined by counting the number of keys stored on each node.

The deployment area is a square plane that divided into grids. Accordingly, to a certain probability distribution, the sensor node can exist in at points around this deployment. In this scheme, three metrics were used to measure the degree of inconsistency that includes tolerance for malicious attacks, false positive rate and detection rate [14]. In this technique, different thresholds are used to evaluate the detection rate and the false positive rate. If the network density increases, then the detection rate also increases.

To know about the any two sensors' neighbors, a certain degree of deployment knowledge must be known. And based on the deployment model, it trims the original Merkle tree into a set of Merkle sub-trees of different heights. And this scheme shows the best height combination for each type of Merkle sub-trees, such that the communication overhead is minimized. The deployment point can form any arbitrary pattern [15]. The communication overhead decreases with the increase of memory usages. This scheme saves computation substantially even with communication overhead but still saves significant energy consumptions.

RAWL is the grid based deployment strategy for the clone attack detection techniques [4]. The details about distribution, whether uniform or non-uniform and also the probability distribution of each protocol used in the grid based deployment strategy shown in Table.1 below in which benefits explained with different parameters.

Table.1. Summary of the Grid based Deployment Strategy Protocols

Grid Based Deployment Strategy Protocols	Distribution Details			Benefits	Parameters
	Uniform	Non - uniform	Probability		
Key management [12]	✓	–	Gaussian	Deterministic	Connectivity, memory usage, communication overhead resilience against node capture
Group-based [13]	✓	–	Gaussian	Doesn't need any prior knowledge of location	Memory constraints, Probability of direct keys and indirect keys
LAD [14]	✓	–	Gaussian	Makes difficult for adversaries to cause localization error	Tolerance, false positive rate and detection rate
DU's [15]	✓	–	Gaussian	The deployment can form any arbitrary pattern	Communication overhead, memory usage, computation costs and energy consumptions
RAWL [4]	✓	–	Normal	Torus network so all nodes obviously have equal probability to be witnesses	Probability of Detection, Communication overhead and memory overhead

6. TABLE ASSISTED WALK STRATEGY (TAWS)

6.1 PROTOCOL DESCRIPTION

Each node broadcast a signed location claim to its neighbors. Each of the node's neighbors probabilistically forwards the claim to some randomly selected nodes. It uses geographic routing (GPSR) to forward the claim to nodes. Each randomly selected node sends a message containing the claim. Each randomly selected nodes start to broadcast claim in horizontal and vertical line (forming of cross) [16]. Each witness node will create a new entry in its trace table for recording the passage of a location claim and it stores the location claim independently. Then it computes the digest of the claim.

It will start a 'w' step random walk in the network by sending the location claim together with a counter of walk steps (w_c) to a random neighbor whereas 'w' is a system parameter. Initially 'w_c' is initialized to one. It continues to forward the message to a random neighbor by incrementing the counter 'w_c' by 1 until counter w_c reaches 'w'. The distance between two neighbors cannot be larger than the transmission range. The number of walk steps (w) is closely correlated to the detection ability of this protocol. Instinctively, the longer the random walks, the higher the probability that the random walks for replicas intersect. If any witness receives different location claims for a same node ID, the digest comparison with the entry. When two digests are different, the node detects a clone attack. When the clone is detected on network, it immediately goes for revoking process and then frequent level key change process is done. With probability $p(w)$, each neighbor randomly selects 's' nodes. Each chosen node that receives the claim of 't' node first verifies the signature and then it stores the claim, and becomes a witness node of 't'.

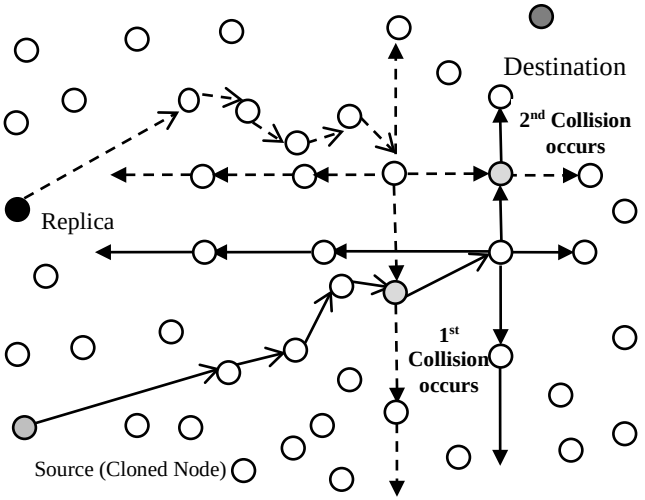

Fig.7. The TAWS approach

6.2 ANALYSIS

The requirements satisfy under TAWS by random walk with torus structure and at least one cross is formed for each node. Considering a $c1\sqrt{n}$ log n-step random walk, it is sufficient for high detection probability with and at each step $c1$ and $c2$ are constant values where 'n' is the number of nodes in the network. This proposed scheme provides a reduced communication cost where, 'd' is the distance between the nodes. A piece of data is hashed to a node based on its content, using a common hash function known to the sensor nodes and the hash value of the message is $h(m)$. Every horizontal line intersects every vertical line. Each node is torus; it has the same geographic property. All the nodes have equal probability to be walked. Based on this grid dimension, each node gets its location and portal ID. In the proposed scheme, it occurs both horizontal and vertical line called as the double ruling technique. The virtual coordinate system defined by the medial axis of the sensor field, there are natural double ruling curves, those are parallel to the medial axis and those perpendicular to the medial axis [10] [16]. Since DR (Double Ruling) scheme only works in rectangular deployment fields but TAWS benefited since it can use arbitrary deployment field. Here, detection probability is higher when compared to other protocols and highly resilient feature to the smart attack. In order to overcome the difficulties faced by the existing schemes in the protocol, we proposed Table Assisted Walk Strategy (TAWS) in which the scheme uses the grid as their deployment strategy and whole as the detection range to provide the best scheme for clone detection as shown in Fig.7. For clarity, notations used in this paper are listed in Table.2.

Table.2. Notations

n	Number of Nodes in a Network
d	Distance between the nodes
$p(p)$	Probability of Detection with respect to transfer of packets
M_d	Minimum Distance between the nodes
K	Key in each nodes
w	Number of walk steps
$p(w)$	Probability of Detection with respect to walk steps
$h(m)$	Hash value of message
M	Message
r	Repeat detection

6.3 TABLE ASSISTED WALK STRATEGY

6.3.1 Table Assisted Strategy:

Each node maintains the trace table and every entry of the table corresponds to the passage of a random walk. The trace table has two columns: *NodeID*, *ClaimDigest*. The *NodeID* is the ID field of claim. The location claim's message authentication (*MAC*) is truncated here as ClaimDigest as shown in Fig.8.

Node	ClaimDigest

Fig.8. The Trace Table in TAWS

When a location claim is received, a node will first find the entries of same node ID as the claim in its trace table. A *ClaimDigest* having 8 bit can be computed by:

$$ClaimDigest = \{MAC_{rand}(Claim)\}_{\mathrm{mod}(256)}$$

where, *rand* is a random value of each node generates itself to prevent false claim with the same value of digest generated by an adversary, and a message authentication code of a given location

claim is MAC_{rand} (*Claim*)**.** Message digest makes the size of location claim and the signature as 3 bytes from 46 bytes. Thus, theoretically, TAWS reduces memory cost.

6.3.2 Walk Strategy:

In this section, we evaluate our walk strategy by relating probability of detection (P_s) values with random walk (r) and walk steps (w). From each node with probability $1/n$, two random walks start having at least one intersection. We assume that two random walks have w-steps, $w \ll cn\log n$.

Since, two random walk starts from the stationary distribution hits a node is given by,

$$P_h = 1\text{-}P(H_i > w) \quad (1)$$

where, H_i is hitting time.

$$P_{h^2} = 1\text{-}(1\text{-}P(H_i > w))^2 \quad (2)$$

Also since,

$$w \ll cn\log n \quad (3)$$

and

$$(-w)/(cn\log n) \approx 0 \quad (4)$$

Then, we use the standard approximation,

$$e^x \approx 1 + x \quad (5)$$

So, we have

$$P_s \approx \left(1-\left(1+\frac{-w}{cn\log n}\right)\right)n \quad (6)$$

$$P_s = 1-\frac{w^2}{c^2 n\log^2 n} \quad (7)$$

Then, if P_S is to be given as P, walk step will be,

$$w = c\sqrt{P}\sqrt{n}\log n \quad (8)$$

Thus, from Eq.(8), we calculate that for any given detection probability, the required number of steps is on the order of $O\sqrt{n}\log n$. For a reasonable comparison, we have P_S as 0.95 for r = 9 and t = 18 in Table.3.

We select typical value of 'r' by concerning communication overhead. If we add 'r' by one, it is necessary to add the cost of a path to a random node. The cost comparison of different protocols based on clone detection techniques mentioned in the Table.4.

Table.3. Probability of Detection (P_S) values with respect to Walk Step (w) and Random Walk (r)

w	If r = 9, then P_S value is
12	0.840
15	0.900
18	**0.952**
21	0.973
24	0.985
27	0.990
30	0.995

7. SIMULATION RESULTS

The Fig.9 shows the simulation which is done in VC++. The Fig.9(a) shows the ID for the original node (clone node) which is 30 and the Fig.9(b) shows the ID for the duplicate node (replica) as 4. Server IP and the server port number are also assigned. The Fig.9(c) shows the TAWS. The full network is structured like a grid and it can be further divided into a number of square grids. During the deployment phase the grid dimension is assigned as a pre-processing step. Each of the nodes deployed randomly in the network. We can set one node as original and other one as duplicate node for collision. The Fig.9(d) shows the detection of the clone attack. The Random Walk w-step process is not enough to cover the entire full network. So that it extends the random walk steps into straight vertical line and straight horizontal lines to visit more nodes in the network by double rule approach [16]. Thereby the node detection is faster when compared to the previous random methods. At one point, the node that gets the information about clone, it sends message to the server that one collision had occurred. The Fig.9(e) and Fig.9(f) shows the allocation of key before and after the clone attack. The key allotted after the detection of the clone attack is the Replica Revoke Process. Pairwise key establishment scheme evaluates a pseudo random function to generate their pairwise key is used in table assisted walk strategy (TAWS).

Table.4. Performance Comparison of Different Protocols

Protocol	Communication Cost	Memory Cost	Non-Deterministic	Fully Distributed	Deployment based	Resiliency
LSM	$O\left(\sqrt{n}\right)$	$O\left(\sqrt{n}\right)$	Yes	Yes	Yes	moderate
SET	$O\left(n\sqrt{n}\right)$	$O(n)$	No	No	No	Poor
RED	$O\left(\sqrt{n}\right)$	$O(1)$	Yes	Yes	Yes	Poor
ACTIVE	$O\left(\sqrt{n}\right)$	$O(1)$	Yes	Yes	No	Very poor
RDE	$O\left(\sqrt{n}\right)$	$O(d)$	Yes	Yes	Yes	Very Poor
SDC	$O\left(T\sqrt{n}\right)$	$O(1)$	No	Yes	Yes	moderate
P-MPC	$O\left(\sqrt{n}\right)$	$O(1)$	No	Yes	Yes	moderate
RAWL	$O\left(\sqrt{n}\log n\right)$	$O\left(\sqrt{n}\log n\right)$	Yes	Yes	Yes	Very Strong
TAWS	$O\left(\sqrt{n}\log n\right)$	$O(1)^2$	Yes	Yes	Yes	Very Strong

It experiences high detection rate when compares with an existing LSM and RAWL protocols as shown in Fig.10(a) and Fig.10(b), the simulation result that probability detection with respect to walk steps and number of packets transmitted and in Fig.10(c) resiliency to node failures with respect to number of walk steps that are implemented using NS-2 simulator and Table.5 illustrates the simulation parameters.

Table.5. Simulation Parameters

Specifications	Values / Type
Total number of nodes	36
Server nodes	1
Duplicate node	Node 30
Original node	Node 4
MAC type	802_11
'x' dimension of Topography	800
'y' dimension of Topography	800
Antenna model	Omni Antenna
Link Layer Type	LL
Interface queue (IFQ)	PRIQUEUE Type
Maximum Packet in IFQ	50
Channel type	Wireless Channel
Radio propagation Model	TwoRayGround model
Network Interface Type	WirelessPhy Interface Type
Time of simulation	100 sec

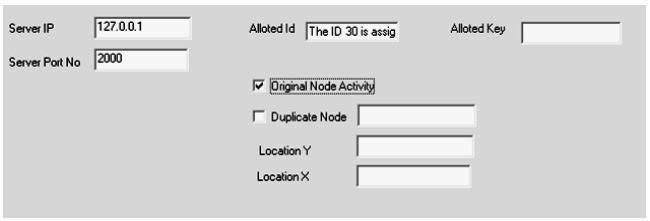

Fig.9(a). Original Node assigned

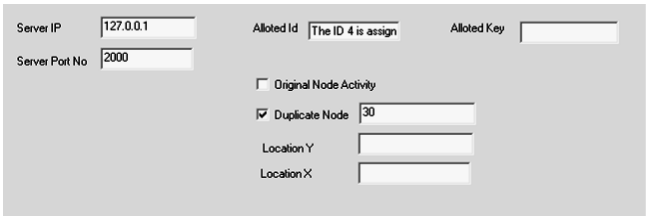

Fig.9(b). Duplicate Node assigned

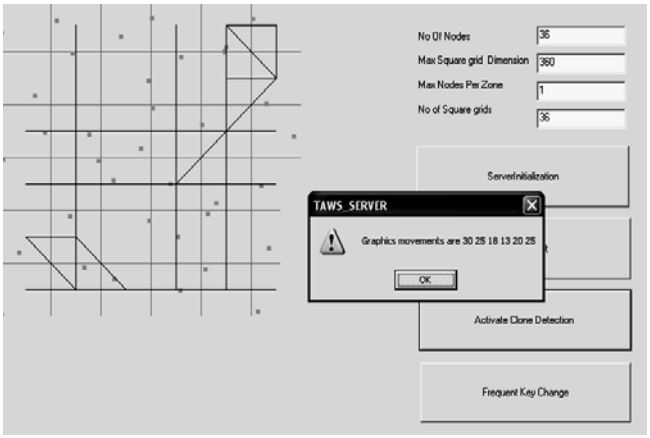

Fig.9(c). TAWS

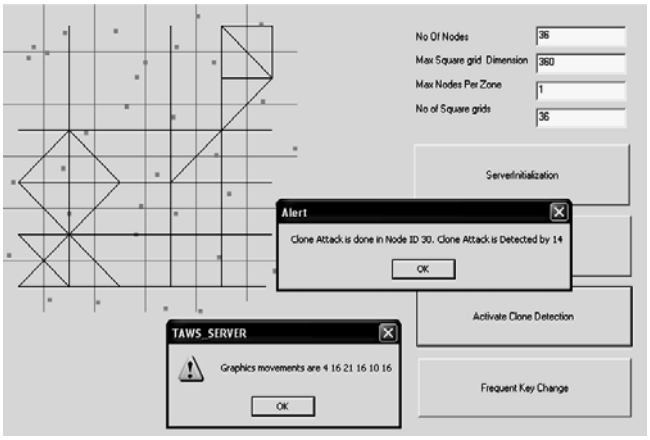

Fig.9(d). Clone Attack Detected

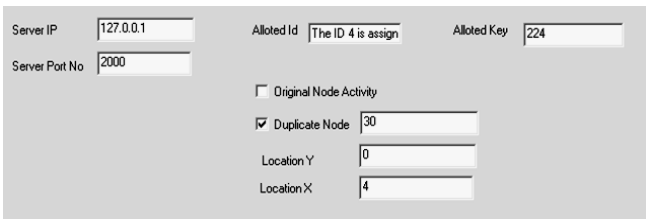

Fig.9(e). Key alloted before Clone Attack

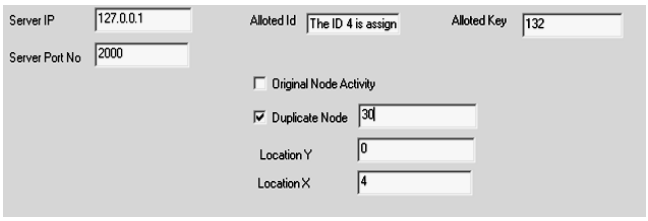

Fig.9(f). Key alloted after Clone Attack

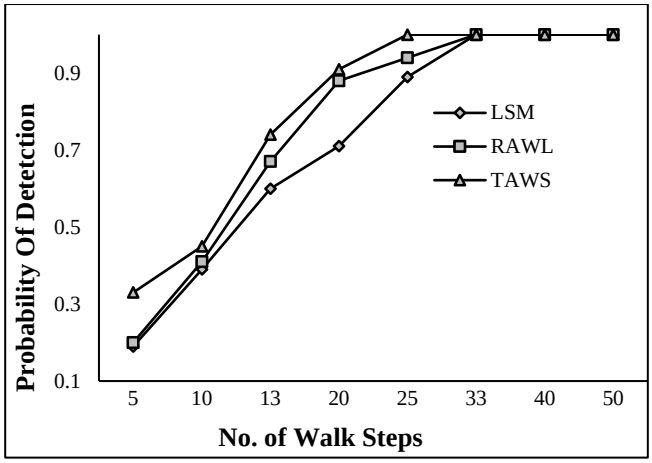

Fig.10(a). Probability of detection w.r.to number of walk steps

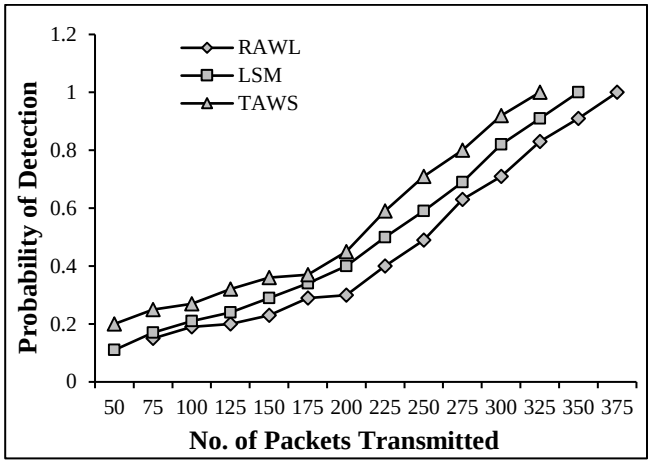

Fig.10(b). Probability of detection w.r.to numbers of packets transmitted

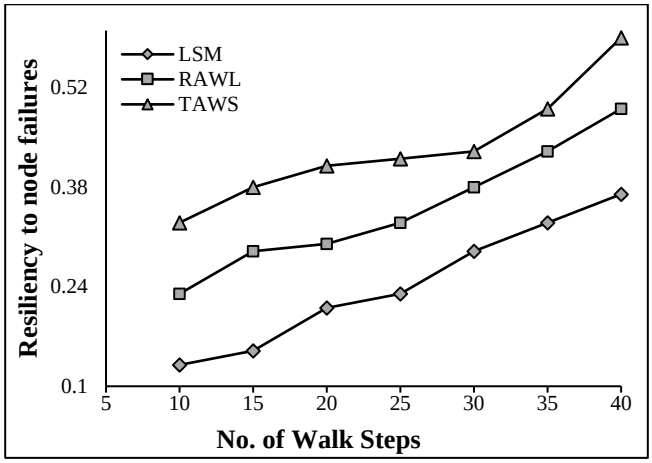

Fig.10(c). Resiliency to node w.r.to numbers of walk steps

8. DISCUSSIONS

For valuable clone attack detection, the selection criteria play an important role in the proposed work. In this paper, it has been classified the existing detection schemes regarding device type, detection methodologies, deployment strategies and detection ranges. And then, this paper provides a review of detection methodology based on various existing selection criteria. It is widely agreed that clones should be detected quickly and it argues that detection methodology based on emergent properties offers the most promising techniques for providing security in sensor network. It is categorized according to the device type, detection methodologies, deployment strategies and detection ranges in terms of Static vs. Mobile, Random vs. Grid, Distributed vs. Central, Whole vs. Local. This paper concentrates on SDWR (Static-Distributed-Whole-Random) and SDWG (Static-Distributed-Whole-Grid) type of selection criteria. It makes an overview of research and makes a clear route that SDWG shown in Fig.12 will be the efficient combination of the existing selection criteria. Grid deployment benefits of reliability, efficiency and security with its main milestone being resilience. Deployment experience indicates significant benefits at different levels in the distribution section.

Our protocols assume that each node knows its own location. Since our proposed work is a randomly distributed witness selection it gains resiliency. We measure resiliency by counting the number of times we must run the protocol in order to detect a single node replication (i.e., we select a random node and insert one replica into the network.)

To reduce memory cost of our protocol, we employ a trace table at each node to record the traces (digests) of random walks.

Memory overhead = average no. of bytes each node store

Randomly selected nodes again have crosses (vertical and horizontal lines) which make better coverage and reduce communication overhead.

Communication overhead = average no. of messages each node broadcasts

The smaller number of walk steps, the less communication and memory overheads results high detection probability.

Probability of detection = No. of successful detection times/No. of repeat times

Non-deterministic property make the network ideal for security applications, particularly in a setting in which an adversary cannot predict the critical nodes. It is hard for an adversary to predict the critical nodes. The protocol is resilient against nodes compromising as extended as an attacker cannot do a smart attack.

Random walks are started for a given node from a random node and each node in a torus which has the same geographic property, so every node have equal probability to be node's witnesses. The Fig.11 summarizes the benefits of our proposed work TAWS.

Features	Performance Evaluation
Random set of witness nodes	Highly Resiliency
Trace table - Message digest	Reduces Memory Overheads
Vertical & Horizontal lines	Reduces Communication overhead
Walk step	High Probability Of Detection
Non- deterministic	Reduce Smart Attacks
Grid – torus structure	Equal Witness Distribution

Fig.11. TAWS Benefits-Summary

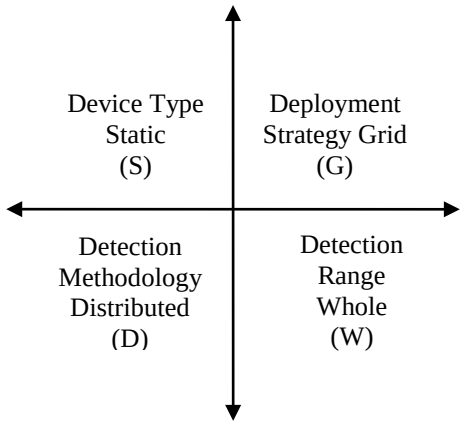

Fig.12. Effective Combinations of Selection Criteria for TAWS

9. CONCLUSIONS

This paper, a new replica-detection protocol, TAWS (Table Assisted Witness Selection) is proposed. Several drawbacks are there in existing protocols such as deterministic, central control and non-resilient issues. This work is exploratory in that the proposed algorithm considers witness selection behavior evaluation to detect clone attack by double rule table assisted walk with horizontal and vertical line (forming a cross) by reducing the number of random walks. The simulation results show that it is more efficient than the previous deterministic and central control mechanism protocols in terms of security feature, communication and memory overhead. We propose a clone attack detection protocol, TAWS protocol, which is fully distributed and designed for stationary WSN in the whole network area. In deployment strategy, it classifies into random and grid based schemes. Specifically, it concentrates on deployment strategy which comprises grid based deployment technique. These all come under the selection criteria for better security performance. To overcome the existing drawbacks, our replica- detection our proposed protocol TAWS overcomes the existing drawbacks by choosing an effective combination of selection criteria. Finally, our work shows the dramatic improvement in detection capability. We believe that our model can open up a new future layer of research in optimization and scheduling techniques.

REFERENCES

[1] Ian F. Akyildiz, Weilian Su, Yogesh Sankarasubramaniam and Erdal Cayirci, "Wireless Sensor Networks: A Survey", *Computer Networks*, Vol. 38, No. 4, pp. 393-422, 2002.

[2] Bryan Parno, Adrian Perrig and Virgil Gligor. "Distributed Detection of Node Replication Attacks in Sensor Networks", *Proceedings of IEEE Symposium on Security and Privacy*, pp. 49-63, 2005.

[3] 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 Systems Journal*, Vol. 7, No. 1, pp. 26-35, 2013.

[4] Yingpei Zeng, Jiannong Cao, Shigeng Zhang, Shanqing Guo and Li Xie. "Random-Walk based Approach to Detect Clone Attacks in Wireless Sensor Networks", *IEEE Journal on Selected Areas in Communications*, Vol. 28, No. 5, pp. 677-691, 2010.

[5] H. Choi, S. Zhu and T.F. La Porta, "Set: Detecting Node Clones in Sensor Networks", *Proceedings of 3rd International Conference on Security and Privacy in Communications Networks and the Workshops*, pp. 341-350, 2007.

[6] Mauro Conti, Roberto Di Pietro, Luigi Vincenzo Mancini and Alessandro Mei, "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks", *Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 80-89, 2007.

[7] Carlos Aguilar Melchor, Boussad Ait-Salem and Karim Tamine, "Active Detection of Node Replication Attacks", *International Journal of Computer Science and Network Security*, Vol. 9, No. 2, pp. 13-21, 2009.

[8] Zhijun Li and Guang Gong, "Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks", *Proceedings of IEEE 6th International Conference on Mobile Ad Hoc and Sensor Systems*, pp. 1030-1035, 2009.

[9] Bo Zhu, Sanjeev Setia, Sushil Jajodia, Sankardas Roy and Lingyu Wang. "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks", *IEEE Transactions on Mobile Computing*, Vol. 9, No. 7, pp. 913-926, 2010.

[10] S. Meenatchi, C. Navaneethan, N. Sivakumar, P. Thanapal and J. Prabhu, "Swbc-Security in Wireless Sensor Networks by Broadcasting Location Claims", *Journal of Theoretical and Applied Information Technology*, Vol. 64, No. 1, pp. 16-21, 2014.

[11] Conti, Mauro, Roberto Di Pietro and Angelo Spognardi. "Clone Wars: Distributed Detection of Clone Attacks in Mobile WSNs", *Journal of Computer and System Sciences*, Vol. 80, No. 3, pp. 654-669, 2014.

[12] Wenliang Du, Jing Deng, Yunghsiang S. Han, Shigang Chen and Pramod K. Varshney, "A Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge", *Proceedings of 23rd Annual Joint Conference of the IEEE Computer and Communications Societies*, Vol. 1, pp. 586-597, 2004.

[13] Donggang Liu, Peng Ning and Wenliang Du, "Group-Based Key Predistribution for Wireless Sensor Networks", *ACM Transactions on Sensor Networks*, Vol. 4, No. 2, pp. 1-11, 2008.

[14] Wenliang Du, Lei Fang and P. Ningi, "LAD: Localization Anomaly Detection for Wireless Sensor Networks", *Proceedings of 19th IEEE International Parallel and Distributed Processing Symposium*, pp. 1-15, 2005.

[15] Wenliang Du, Ronghua Wang and Peng Ning, "An Efficient Scheme for Authenticating Public Keys in Sensor Networks", *Proceedings of 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*, pp. 58-67, 2005.

[16] Rik Sarkar, Xianjin Zhu and Jie Gao, "Double Rulings for Information Brokerage in Sensor Networks", *IEEE/ACM Transactions on Networking*, Vol. 17, No. 6, pp. 1902-1915, 2009.