International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 7 | ISSN : 2456-3307

Combining the Concept of Abstraction, RAWL and Network Division to Detect Clone Node in Distributed WSN

M. Thirunavukkarasan*[1], Dr. S. A. Sahaaya Arul Mary[2]
[1]Research Scholar, Department of Computer Science and Engineering, Manonmaniam Sundaranar University, Tamil Nadu, India
[2]Professor & Head, Department of Computer Science and Engineering, Saranathan College of Engineering, Tamil Nadu, India

ABSTRACT

Wireless Sensor Networks (WSNs) are defenseless to clone assaults as they are conveyed in threatening and unattended environments. Likewise because of the absence of physical alter obstruction, an enemy can without much of a stretch catch and bargain sensor hubs and in the wake of imitating them, he embeds subjective number of clones into arrange. Thus the foe is capable to mount a wide assortment of interior assaults. A few arrangements have been proposed in the writing for the identification of these clones from which witness hub based circulated arrangements have indicated tasteful outcomes. Irregular Walk (RAWL) is one of the witness hub based circulated systems in which witness hubs are haphazardly chosen by starting a few irregular strolls all through the system. In spite of the fact that RAWL has accomplished high security of witness hubs however in achieving high recognition likelihood RAWL experiences high correspondence and memory overhead. In this paper I have taken three concepts abstraction which says that user cannot access any internal programming or cannot even order the node to do perform any task whereas user is allowed to select from a series of task only which will be predefined. In this case user will be node itself. Random Walk (RAWL) is one of the witness node based distributed techniques in which witness nodes are randomly selected by initiating several random walks throughout the network. Although RAWL has achieved high security of witness nodes but is not perfect. We use network division technique to divide the entire network is divided into different areas.

Keywords : Wireless Sensor Networks, Security, Clone Node Attack, Node Replication Attack, Random Walk, Network Division, Abstraction.

I. INTRODUCTION

Wireless Sensor Network (WSN) is a gathering of sensor hubs with detecting abilities, restricted assets and progressed organize models with a wide assortment of utilizations [1-2]. WSNs are frequently sent in cruel, threatening and unattended environments. These sensor hubs need alter obstruction equipment and they are inclined to numerous assaults. Here, we especially center around more hurtful assault which is known as clone connect or hub replication assault. In this assault an enemy physically catches at least one sensor hubs and trade off all its mystery certifications. He/she at that point makes reproductions of the traded off hubs and secretly send them at vital positions of the system. A foe can use these clones to dispatch numerous insider assaults and malignant exercises like he can dispatch a dark opening, wormhole assault or lunch specific sending assault and DoS assault, infuse false information, screen and catch noteworthy bit of movement, malign and affront other end honest to

goodness hubs [3-4]. Furnishing the sensor hubs with an alter resistant hardware is a straightforward answer for manage clone hub assaults, yet this arrangement isn't engaging due to two principle reasons; initially, it is the cost, as it extremely costly to shield each sensor hub in the system with a sealed equipment, and second, a specialist assailant can in any case sidestep alter obstruction.

Along these lines there is a need to create programming based countermeasures for the discovery of clone hubs as all at present accessible conventions for validation and secure correspondence enable them to be a piece of system [5-8]. In the writing, two kinds of programming based solutions have been proposed for the discovery of hub replication assault in static WSNs to be specific brought together and disseminated. In unified arrangements the discovery procedure depends on a base station [9-10] or on the other hand helped focal specialist (i.e. base station, bunch head and so on) [14-15]. In conveyed arrangements the identification procedure is conveyed out by all sensor hubs in the system without the contribution of any focal expert. Some disseminated approaches proposed to recognize clone assaults [12-13, 16] have utilized claimer-columnist witness system (additionally called witness hub based procedures) in which the claimer hub locally communicates its area guarantee to its neighbors and each neighbor fills in as a correspondent hub whose obligation is to delineate claimer id to at least one witness hubs. The brought together arrangements have accomplished high clone identification rates however they all experience the ill effects of single point of disappointment and high correspondence costs. Because of these shortcomings the consideration of scientists is occupied towards circulated arrangements. The primary problem with the existing witness hub based approaches is the choice and dispersion of witness hubs i.e. either the witness hub choice is deterministic or the circulation of witness hubs over the system is non-uniform(for every cycle of the convention).

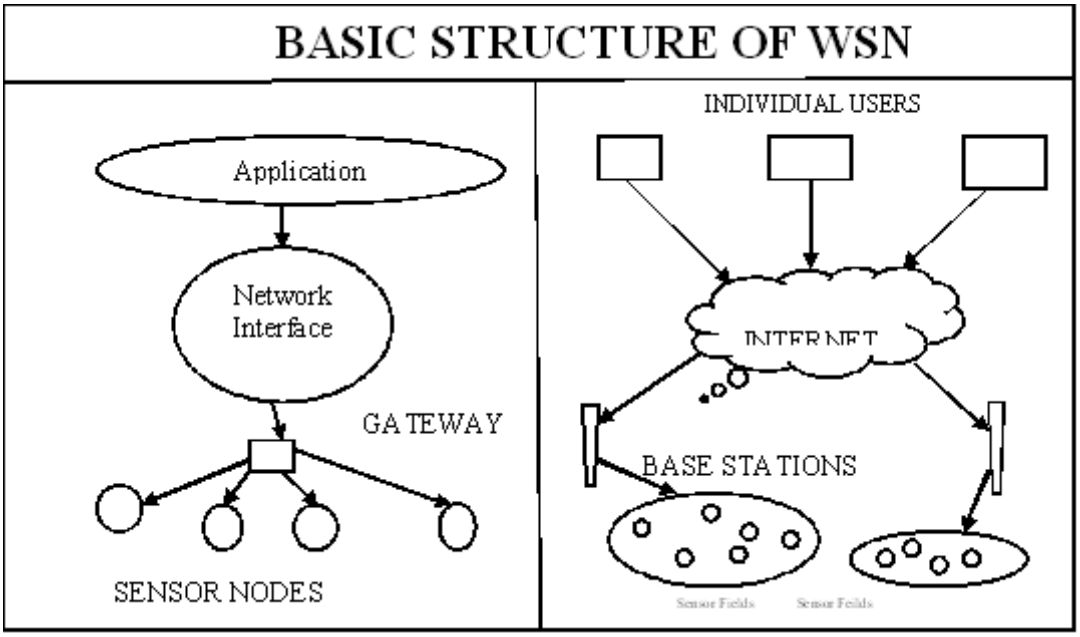


Figure 1

Including the current endeavors done as such far meaning to recognize clones in static WSNs, RAWL [12] is by all accounts the most ideal approach. This is on account of RAWL takes care of the issues of different witness hub based procedures by choosing witness hubs arbitrarily and afterward starting a few

arbitrary strolls all through the system. Other than accomplishing sensible security of witnesses RAWL has still some vital imperfections. Right off the bat, RAWL exchanges off expenses brought about for correspondence and memory to accomplish higher likelihood of recognizing clones and more grounded security of witnesses. Also, RAWL guarantees accomplishing witness hub convergence by starting more arbitrary strolls with longer walk steps. Thirdly, RAWL requests more journalists for starting arbitrary strolls that can forward the area claim to arbitrarily chosen hubs which all at that point start irregular strolls the hubs on the passing way additionally turn into the witnesses.

The network division WSNs which blends the division of the system into territories with an arbitrary walk called RAND (random stroll with arrange division). It depends on claimer-journalist witness structure and comprises of two stages. In the to start with stage called organize setup stage, the whole network is partitioned into various leveled levels by utilizing heuristic based calculation and afterward at least one levels define a particular area. Every hub in the system has a place with a specific level and region. In the second stage which is called copy recognition stage, the claimer hub sends a marked area claim to its one bounce neighbors. At least one neighbors (columnist hubs) forward the claim to haphazardly chosen hubs in any blend Of haphazardly chose territories (we will portray the points of interest of are-as determination in segment III.C) with some likelihood. These randomly chose hubs will turn into the witness hubs which at that point start an irregular stroll inside the every zone. All the passed hubs are chosen as witness hubs and will store the area guarantee. On the off chance that there are clones in the system they will forward the area guarantee in comparative way and if any witness hub receives diverse area claims for a same hub, a contention is recognized lastly a clone hub will be denied. The outcomes demonstrate that our proposed convention beats the current solution RAWL by decreasing the correspondence and memory costs with high likelihood of recognition.

Abstraction this is a concept where we prevent the user from interfering in the internal algorithms or the internal programming of a system we can achieve this by making everything controlled by the processor itself and handing over some functions to choose from to the user. The same concept can be implemented in WSN networks where the task performed by a node can be listed by the programmer at the starting itself. The software written for a note should be compatible with the random walk and the division network concept also which will provide complete combination of these three techniques. The programmer current node can program only the Limited task which will be only communicating to the neighboring nodes . Whenever And node is selected for the clone on detection process by random walk procedure the node will check itself whether all the functions which is been listed is working properly or not the report will be checked by the neighboring nodes also if some conflicts ignored will be declared as compromise and will be deleted from the network until and unless it is repaired and put back into the service by the administrator.

II. RELATED WORK

In recent years, various witness hub based plans have been proposed for the identification of hub replication assault in remote sensor systems. In this segment we have portrayed some latest witness hub based methods and furthermore identify their noteworthy downsides. B.Parno et al. [11] were the in the first place to propose appropriated two disseminated calculations Randomized Multicast (RM) and Line-Selected Multicast (LSM). RM circulates area cases to an arbitrarily chose set of witness hubs and every hub communicates an area

claim to its one-bounce neighbors which additionally forward the area assert with a likelihood to the hubs nearest to the picked areas by utilizing geographic directing. No less than one witness hub is probably going to receive clashing area claims as per birthday conundrum at the point when imitated hubs exist in the system. LSM diminishes the correspondence expenses and increment the likelihood of identification by misusing the steering topology of the system to choose mind nesses for a hub's area and uses geometric likelihood to distinguish recreated hubs. This appears like haphazardly drawing a line over the system and the convergence of two lines becomes the confirmation hub of accepting clashing area claims. In both RM and LSM the issue lies in the determination of witness hubs (i.e. Probabilities) and furthermore it isn't generally genuine that area cases of clone hubs are gotten to the same witness hub. Also, LSM experiences uneven distribution of witnesses hubs as dominant part of witness hubs are chosen from the focal point of the system, the vitality of these hubs is exhausted soon along these lines they turn into the purpose of intrigue for the enemy.

Zhu et al. [12] have proposed two circulated conventions called Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC). In the two conventions the entire sensor organizes in partitioned into cells to shape a geographic framework. In SDC every hub's ID is particularly mapped to one of the cells in the matrix. Amid discovery methodology, every hub communicates a area claim to its neighbors. At that point each neighbor advances the area guarantee with likelihood to a novel cell by executing a geographic hash work. Once any hub in the destination cell gets the area assert, it surges the area guarantee to the whole cell. Every hub in the goal cell stores the area assert with likelihood. Consequently, the clone hubs will be distinguished with a specific likelihood since the area cases of clone hubs will be sent to a similar cell. Like SDC, in the P-MPC plot, a geographic hash work is employed to delineate personality to the different deterministic cells with different probabilities. Whatever remains of technique is like SDC. For all intents and purposes both of these strategies rely on the cautious choice of a cell measure on the grounds that if the cell estimate is as well extensive they bring about high correspondence cost and if measure is as well little, it will be simple for an enemy to trounce them by trading off all hubs in the deterministic little cells. An important issue with SDC is that so as to diminish the expansive cast overhead it requires to execute the flooding just when the in the first place duplicate of a hub's area guarantee touches base at the cell and the following duplicates are overlooked. In doing this, the hub in the cell that initially gets the area guarantee can't recognize between cases of unique hub and imitation hub.

Y.Zeng et al [14] have proposed two conventions Random Walk (RAWL) and Table-helped Random Walk (TRAWL). In RAWL every hub communicates a marked area claim to neighboring hubs which probabilistically advances the claim to some arbitrarily chose hubs. At that point each haphazardly chose hub communicates something specific containing the claim to begin an irregular stroll in the system, and the passed hubs are chosen as mildness hubs and will store the claim. In the event that any witness receives different area claims for a same hub ID, it can utilize these cases to renounce the repeated hub. TRAWL depends on RAWL and includes a follow table at every hub to decrease memory cost. The RAWL needs more arbitrary strolls and irregular walk ventures for accomplishing high recognition likelihood that prompts higher correspondence and memory cost which is more than twice correspondence overhead of LSM. The creators decrease the memory cost by proposing TRAWL yet the correspondence cost still exists. Alternate strategies for the recognition hub replication assault in static and portable sensor system can be found in more points of interest [15,

16, 17].Like this more and more ideas were proposed for the detection and rectification of clone hubs in wireless sensor networks.

III. DRAWBACKS OF EXISTING PROTOCOLS

Every system is having its own particular quality and shortcomings.

1. Hub to Network Broadcasts does not require a focal base station to identify hub clone [9]. In spite of the fact that 100 % identification is given accepting communicate achieves each hub, every hub is in charge of location prompting high correspondence over-burden.

2. To beat this, Deterministic Multicast [9] is utilized where area guarantee is sent to some subset of hubs called witness hubs. Be that as it may, the Function used to delineate hub id to the arrangement of witness hub is deterministic in this manner an enemy can likewise decide the witness hubs. Hence an enemy needs to trade off just the witness hubs to perform assaults making it far-fetched to utilize.

3. As a change of DM, RM and LSM were proposed. Both RM and LSM are firmly identified with the no of witnesses. Bigger the no of witnesses more correspondence is required while bring down the no of witnesses gives less odds of identification of clones. Again LSM experiences swarmed focus issue where focal zone is utilized all the more much of the time utilize then the fringe of the system prompting exhaustion of hubs vitality dwelling in focus. Again convergence may not occur on a genuine regular hub offering ascend to Cross over issue.

4. RED convention was proposed to circulate the witnesses pseudo arbitrarily utilizing a pseudorandom work [10]. A confided in outsider is required to convey the irregular variable which may not generally be accessible.

5. In SDC [11], the primary downside is the hub in the cell that initially gets the area asserts can't separate between cases of unique and cloned hub.

6. In RDE, If a system topology is twisted to such an extent that no real way to accomplish line transmission exclusively, the RDE winds up unacceptable.

Table 1. Summary Of Methods

S.No	METHOD	ADVANTAGE	DISADVANTAGE
1	N2NB	More efficient than centralized approach	High communication overload
2	DM	Communication overhead is reduced to some extent.	Less security is provided
3	RM	Witness nodes are randomly Selected	Lower detection probability
4	LSM	Reduced the communication overhead caused by RM.	Suffers from uneven distribution of witness nodes
5	RED	Pseudorandom selection of witness nodes leading to uniform witness distribution.	Trusted third party is needed.
6	SDC and P-MPC	More efficient then LSM	Dependant on cell size. If too large high communication overhead, if too small, node compromise can occur easily
7	RDE	Good memory overhead	If a network topology is distorted such that no way to achieve line transmission, the RDE becomes unsuitable

IV. PROPOSED WORK

The random walk technique and the network division technique have already been introduced together for the detection of a clone note in a WSN. But we improved the proposed technique called abstraction with two process to increase the performance of the existing algorithm and also reducing the cost of manufacturing of node. Because this technique will also help to reduce the memory requirements in a node and the network congestion in a WSN. The above two mention problems are the most major problem in a WSN. The process of abstraction will work in a fashion such that every node present in the WSN will be provided with a list of functions which unknown is allowed to perform any other functions apart from that list cannot be performed by the node.

We will first divide the entire network into different parts with the help of network division technique this indeed will help us to increase the performance of the random walk selection of node with a lot. Then with the help of random walks we will check a node whether it is cloned or not. When we got a confirmation that the selected node is clone node then we will see that number of functions which is being performed by that node. We will check also with the neighboring nodes is all the functions done by the node is the approved the network or not and no extra function is seen before the previous check, then the node is said to be not compromised. If any one of the function fails due to any course the node is required to terminated from the WSN. If it is seen any new function has been added then also the node will be treated as compromised and is required to terminate from the WSN. After the detection of the clone node the authorities need to personally reset the node and re-enter it into the WSN.

V. RESULTS AND PROOF

Algorithm 1 Clone Detecting protocol

Initialize： The hops of each sensor node to the sink are built through the flooding protocol;

Exchange the relational information with neighbors;

Stage A: building witness

1: $Xa \leftarrow$ Encrypt(IDa , la)

2: k = PseudoRand(IDa , la , h)

3: Random walk ε1 hops to node b, i ← b. hop, b'=b ;

4: while i≠ k do

5: if i < k then

6: b′ ← NextNodeOnMaxHop(b′), i ← i + 1;

7: else

8: b′ ← NextNodeOnLeastHop(b′), i ← i – 1;

9: end if;

10: end while;

11: node b' Random walk ε2 hops to node b′′, where each node's hop count is the same as the route path; i ← 1

12:while i < ⌈Ψ/r⌉ do

13: Let b′′record Xa;

14: b′′ ← NextNodeOnSameHop(b′′), i ← i + 1;

15:end while;

Stage B: clone detection

1: Random walk x1 hops to node a′; a′. tag = true 3

2: node a′ routing reverse sink to a′′′ with broadcast Xa;

3: while a′. hop ≠ 2 do

4: a′ ← NextNodeOnLeastHop(a′); Broadcast Xa;

5: end while;

6: ∂ ←The hops need for routing to build the next clone route

7: a′. tag = false

8: routing ∂ hops to node c with same-hop routing;

9: c. tag = true, c route reverse to sink;

10: for each clone detection route reverse to the sink ;
11: c′ ← NextNodeOnMaxHop(c′); Broadcast Xa;
12: if c′. tag = true then
13: compute ∂ using formula 9;
14: if $\partial \neq 0$ then
15: along both left- and right-hand directions, same-hop ∂ routing hop to nodes c″, c‴;
16: c′. tag = false;
17: nodes c″, c‴ route reverse to the sink;
18: end if;
19: end if;
20: end for;
21: for each node S that hears Xa do
22: if (, la) of $S \neq$ (IDa , la) in Xa then
23: trigger the revocation procedure;
24: end if
25: end for

THEOREM 1:

In the Network Division protocol, considering following equation, the lifetime ratio of the LSCD protocol to that of the RED (or LSM) protocol is

$$\varphi=h\,2+gpd\sqrt{(d+1)}h\,\lambda''/(h\,2+1+\lambda'')$$

PROOF:

Assume that $\lambda'=\lambda''=1$. According to [2], [8], it has been proven that the number of clone detection packets under the RED (or LSM) protocol is $gpd\sqrt{n}$ because the nodal degree is d; then, $\pi r2\rho=d+1$, and the total number of nodes in the network is $n=\pi(h\,r)2\rho$. Because $\pi(h\,r)2\rho/\pi r2\rho=h\,2$, $n=h\,2(d+1)$. Thus, $gpd\sqrt{n}=gpd\sqrt{(d+1)}h$. There are λ'' clone detections in each data collection round, and thus, there are $gpd\sqrt{(d+1)}h\,\lambda''$ clone detection packets because the amount of data in the first ring is maximized as $h\,2$. Therefore, the maximum load of the RED and LSM protocols is $h\,2+gpd\sqrt{(d+1)}h\,\lambda''$. In the LSCD protocol, the maximum load at the first ring is $h\,2+1+\lambda''$, among which 1 is the witness route construction load and λ'' is the clone detection load. Thus, the theorem is proved.

THEOREM:2

Storage Overhead:

The average nodal storage requirement is

$$\Phi=(\lceil\psi/r\rceil\hbar 2)/(\hbar\,2-1)$$

In the LSCD protocol, the stored route length for each nodal witness is ψ, and it is stored $\lceil\psi/r\rceil$ times. There are $n=(\pi(h\,r)2\rho)$ nodes in total, and thus, the total storage is $n\lceil\psi/r\rceil$ because the first ring generates the witness. These witness storage requires are undertaken by $n-\pi r2\rho$ nodes. Therefore, the storage needed by each node is $(\pi\hbar\,2r2\rho\lceil\psi/r\rceil)/(\pi\hbar\,2r2\rho-\pi r2\rho)$.

THEOREM:3

Clone Detection probability

Given that the selected witnesses of node a are trustful, if there exists a clone of node a', the cloned node can always be detected.

PROOF:

As observed from the LSCD protocol, the witness of node a must be stored in an arc with length Ψ, and the distance between any two detection routes must be smaller than Ψ. Thus, during clone detection, the detection route that contains node a's (ID, location) must encounter the witness of node a, and this reveals to the witness that nodes a and a' have the same ID but are at different locations. Thus, the cloned node can always be detected.

THEOREM:4

Considering that node a in the detection route stores $2j$ current routes, when a routes to ring i, the condition for new detection route construction and same-hop routing for these new routes is as follows:

$\partial=0$, if $2j\geq(2\pi ir)/\Psi$
$\partial=(2\pi ir)/(2j+1)$, else

PROOF:

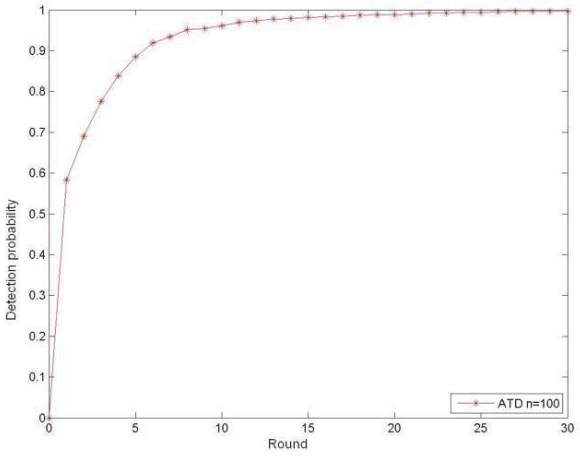
Obviously, if $2j \geq (2\pi ir)/\Psi$, then the distance of any two detection routes is smaller than Ψ. Therefore, no additional detection routes are needed, and $\partial=0$; otherwise, additional detection routes are needed. According to the LSCD protocol, there are $2j$ routes. With the distance of any two routes as $(2\pi ir)/2j$, the newly created routes will be placed in the middle of the original routes, and the number of routes is doubled. Therefore, the length of the same ring route is $\partial=(2\pi ir)/(2j+1)$.

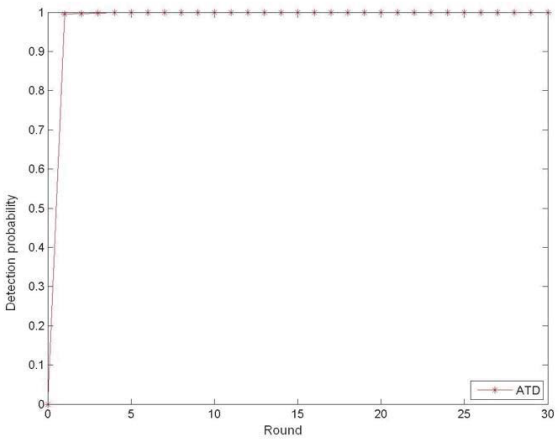
SIMULATION AND DISCUSSION:

We simulated the proposed mobile replica detection scheme in a mobile sensor network. Inspired by [9], we focused on the detection performance of the simulated scheme. A modified Random Waypoint model is used as the mobility model. Nodes are unaware of their velocities and directions, but have a known maximum velocity Vmax. Instead of choosing a certain speed for the destinations, nodes randomly vary their speed at each movement. The pause time is set to 0, so the node starts for the next destination immediately after one round of trip. We assume that the default value of communication range R is set to 42 units and all the nodes are uniformly deployed in a 800*800 square area. The default value of the maximum velocity is set to 36 units/s. The default value of the count of the nodes N is set to 1000.

Under the standard condition, we performed the simulations considering the length of history log h = 10 and setting the number of the replicated nodes: c=l. When the node is collusion with deceiving location in the network, because the local and global detection are added to the location of the verification, it is easy to find malicious nodes cheat on location, as shown in the figures. The probability of isolated nodes is increasing when node density to reduce in network, the possibility of communication among nodes is reduced, then the detection rate of ATD scheme has been affected. However, as shown in the figures, after a certain rounds of detection, ATD can still achieve higher detection rate. ATD scheme for low-speed network node position deception can maintain a higher detection rate, as shown in the figures.

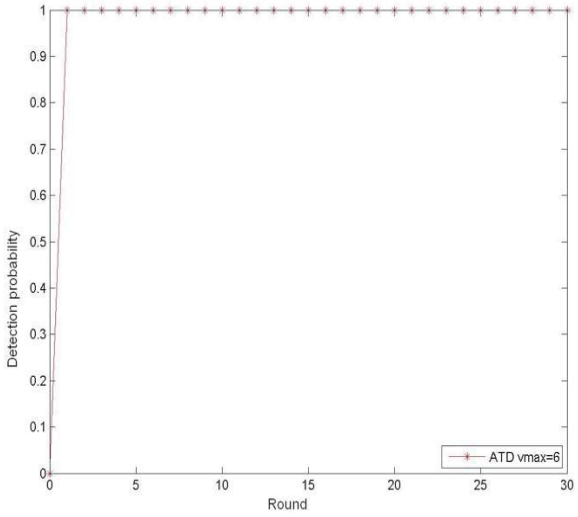
There's no influence on the density of nodes in the network while the length of history log shorten, therefore, no effect on the probability of location cheating nodes. To sum up, for the detection of the position of the nodes of deception, ATD is only concerned with the density of nodes in the network, when a neighbor of nodes exists, ATD will be able to quickly identify the location deception node.





Detection probability for changeable parameter n=100

Detection probability under the standard condition when the parameter is H=lO,v=36,c=l,R=42



Detection probability for changeable parameter h=6

VI. CONCLUSION

This paper introduces node clone attack, the importance of clone detection and the existing techniques for detection of node clones present in the network. Centralized techniques suffer from single point of failure while local detection is limited to a nodes neighborhood. Hence the Network Division techniques are appropriate to detect the replicas in the network. In network witness based distributed techniques, selection of witness node is done in such a way to cover larger areas to find any clones present in the network. However it is necessary that the communication and storage requirement to detect the node clones should be less in order to apply in resource constraint network like WSN.

VII. ACKNOLEDGMENT

I would like to thank my guide **Dr. S.A. Sahaaya Arul Mary** who guided me solve this problem in a proper manner. I extend my thanks to student Akash Kumar for supporting me. Also I want to thank my family and friends for their support.

VIII. REFERENCES

[1]. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "Wireless Sensor Networks: A Survey", International Journal of Computer and Telecomm. Networking, 38(4): 393-422, 2002.

[2]. W. Z. Khan, Y. Xiang, M. Y. Aalsalem and Q. Arshad, "Mobile Phone Sensing Systems: A Survey," IEEE Communications Surveys & Tutorials, 15(1): 402-427, 2013.

[3]. C. Karlof, D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures", In Proceedings of 1st IEEE international workshop on sensor network protocols and applications, May 2003.

[4]. A. Wood, J. A. Stankovic, "Denial of Service in Sensor Networks,"IEEE Computer, 3(10):54-62, October 2002.

[5]. S. Zhu, S. Setia, and S. Jajodia, "LEAP: efficient security mechanisms for large-scale distributed sensor networks," In Proceedings of the 10th ACM Conference On Computer and Communications Security (CCS-03), pp. 62–72, 2003.

[6]. C. Karlof, N. Sastry, and D. Wagner, "TinySec: a link layer security architecture for wireless sensor networks," ," In Proceedings of the 2nd ACM Conference Embedded Networked Sensor Systems (SenSys -04),2004, pp. 162–175.

[7]. A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen , D. E. Culler. "SPINS: security protocols for sensor networks.", Wireless Networks, (8): 521–34, 2002.

[8]. C. Hartung, J. Balasalle and R. Han, "Node Compromise in Sensor Networks: The Need for Secure Systems", Technical Report Technical Report CU-CS-988-04, Department of Computer Science, University of Colorado at Boulder, 2004.

[9]. H. Choi, S. Zhu, and T. F. L. Porta, "SET: detecting node clones in sensor networks," in Proceedings of the 3rd International

Conference on Security and Privacy in Communication Networks (SecureComm '07),2007, pp. 341–350.

[10]. 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 Transactions on Systems, Man, and Cybernetics, Part C: Applications and Reviews, 37(6): 1246-1258, 2007.

[11]. B. Parno, A. Perrig and V. Gligor. "Distributed detection of node replication attacks in sensor networks", In Proceedings of the IEEE Symposium on Security and Privacy (S&P), 2005.

[12]. B. Zhu, S. Setia, S. Jajodia, S. Roy, and L.Wang, "Localizedmulticast: efficient and distributed replica detection in large-scale sensor networks," IEEE Transactions on Mobile Computing, 9(7): 913–926,2010.

[13]. M. Conti, R. Di Pietro, L. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Transactions on Dependable and Secure Computing, 8(5): 685–698, 2011.

[14]. Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random walk based approach to detect clone attacks in wireless sensor networks," IEEE Journal on Selected Areas in Communications, 28(5): 677–691, 2010.

[15]. W. Z. Khan, M. Y. Aalsalem, N. M. Saad, and Y. Xiang, "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey," International Journal of Distributed Sensor Networks, vol. 2013, Article ID 149023, 22 pages, 2013.

[16]. W. T. Zhu, J. Zhou, R. H. Deng, and F. Bao, "Detecting Node Replication Attacks in Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, 35(3): 1022–1034, 2012.

[17]. W. Z. Khan, N. M. Saad and M. Y. Aalsalem, " Scrutinizing Well known Countermeasures against Clone Node Attack in Mobile Wireless Sensor Networks", International Journal of Grid and Utility Computing (IJGUC), 4(2): 119-127, 2013.