ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

CREDENTIAL - BASED NODE REPLICATION DETECTION SCHEME FOR WIRELESS SENSOR NETWORK

J. Sybi Cynthia*[1], Dr. D. Shalini Punithavathani[2]
*[1]Research scholar, C.S.I. Institute of Technology, Thovalai,
[2]Principal, Government College of Engineering- Tirunelveli

Keywords: Denial of Service attack, wireless sensor network, Unassailable Randomized, Efficient and Distributed Protocol, Ardent Randomized, Efficient and Distributed Protocol.

ABSTRACT
A gathering of hubs that are improved into an agreeable network is called as the wireless sensor network. Accordingly, wireless sensor networks (WSNs) are inclined to a wide assortment of physical attacks. In this paper, we consider a run of the mill risk known as hub replication attack or clone hub attack, where an enemy makes its own minimal effort sensor hubs called clone hubs and misguides the network to recognize them as honest to goodness hubs. Recognizing the hub replication attack has turned into a basic examination subject in sensor network security, and planning identification plans against this attack includes distinctive undermining issues and difficulties, a self-mending, randomized and appropriated convention to recognize hub replication attacks were Ardent Randomized, Efficient and Distributed Protocol (ARED). Systematically demonstrated that our protocol has somewhat higher overhead yet accomplishes amazing changes in malevolent hub identification likelihood and therefore equitably adjusted among the hubs.

INTRODUCTION
A major dispute in pervasive environments is prevention in clone attacks. Information against misdeeds like change or theft must be protected due to security of the emerging WSNs in pervasive applications is a crucial problem. The short-range wireless communication techniques were used for collecting data by small wearable or implantable sensors and communication for pervasive applications in WSN emerging as a new technology [1]. A major unsolved concern on the security and privacy protection of the data collected from a WSN during storing inside or transmitting outside and challenges stringent resource constraints of WSN devices and the high demand for security/privacy and practicality/ usability [23].

At fixed intervals of time Unassailable Randomized, Efficient and Distributed Protocol (URED) executes routinely. There are two steps in every run of the protocol. In the first step among all the nodes the random value rand is shared [3]. Within network distributed mechanisms, centralized mechanism of random value was broadcast. A secure verifiable leader election mechanism for instance was elected a leader among the nodes. Then random value was chosen and broadcast by the leader.In the second step, geographic location and its claim id was broadcast locally and digitally signed by each node. Receive_Message procedure was executed when the neighbors receive the local broadcast. A set of g is greater than 1 pseudo randomly selected network locations receives the claim which is send by each of the neighbors. Since this kind of solution does not extent well, the URED protocol does not send the claim to the specific node id. The node id not present in the network that was sent by the claim would be lost and without updating all the nodes after the first network deployment cannot be used as witnesses. When a specific node is used as the message destination, URED protocol can be easily adapted to work [24]. The alogrithm of secure randomized efficient and distributed protocol is depicted [2-4].

The wireless sensor network communication system architecture is explained in Figure 1. Largely sensor nodes are deployed may cover a huge area, that expose them to attackers may capture and reprogram the individual nodes [7-8]. A huge area may be covered by largely deployed sensor nodes exposing to attackers in which capturing and reprogramming of individual nodes are possible. The attacker induce the network to accept malicious nodes as legitimate ones by using his own formula of attacking. Some of the possible threats to the security of the sensor networks are extraction of private sensed data, falsification of original data, DoS and hacking of collected network readings [5]. A challenging research issues in WSNs are security issues, development of new supporting technologies and security principles [25].

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

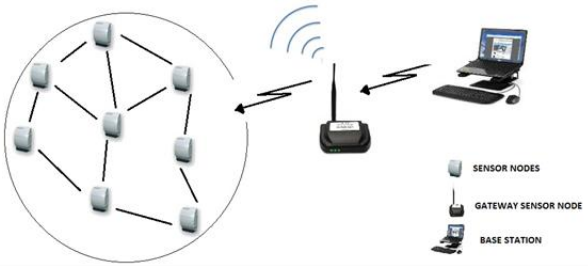

Figure 1. Wireless Sensor Network Communication System Architecture

UNASSAILABLE RANDOMIZED, EFFICIENT AND DISTRIBUTED PROTOCOL

A major dispute in pervasive environments is prevention in clone attacks. Information against misdeeds like change or theft must be protected due to security of the emerging WSNs in pervasive applications is a crucial problem. The short-range wireless communication techniques were used for collecting data by small wearable or implantable sensors and communication for pervasive applications in WSN emerging as a new technology [12-14]. A major unsolved concern on the security and privacy protection of the data collected from a WSN during storing inside or transmitting outside and challenges stringent resource constraints of WSN devices and the high demand for security/privacy and practicality/ usability [6]. At fixed intervals of time URED protocol executes routinely. There are two steps in every run of the protocol. In the first step among all the nodes the random value rand is shared. Within network distributed mechanisms, centralized mechanism of random value was broadcast. A secure verifiable leader election mechanism for instance was elected a leader among the nodes. Then random value was chosen and broadcast by the leader [15].

In the second step, geographic location and its claim id was broadcast locally and digitally signed by each node [11]. RECEIVE_MESSAGE procedure was executed when the neighbors receive the local broadcast. A set of $g \geq 1$ pseudo randomly selected network locations receives the claim which is send by each of the neighbors. Since this kind of solution does not scope well, the URED protocol does not send the claim to the specific node id. The node id not present in the network that was sent by the claim would be lost and without updating all the nodes after the first network deployment cannot be used as witnesses. When a specific node is used as the message destination, URED protocol can be easily adapted to work. The alogrithm of secure randomized efficient and distributed protocol is depicted [8-10].

PROPOSED- ARDENT RANDOMIZED, EFFICIENT AND DISTRIBUTED PROTOCOL

The extension work of Unassailable Randomized, Efficient and Distributed Protocol (URED) method is the Pro-active prevention of node replication attack. It blocks the entry of the clone or malicious node completely into a network. But URED protocol method identifies and isolates the replicated node after entering into the network. To detect node replication attacks in WSNs, an effective and efficient Pro-active method was proposed. Normally the adversary stays away from the network of BS but will stay within the accessible range to reach any of the nodes in the group network. Through the multi hop mechanism, the adversary tries to contact the authentic nodes to reach the BS. And hence adversary initially contacts the nodes normally in the outer ring or on the edge of the network. Even though it has proper keying material but without proper verification mechanism the nodes in the network will not directly pass any data forwarded by any other malicious or trusted nodes which is present inside or outside the network.

In a network through peer to peer or multi hop mechanism, whenever a node tries to communicate with another node after initialization of the network, the initially contacted node always checks the id and corresponding location of the contacitng nodes are available in the allowable list of its own. It will then allow further communication in the network after verification of the id and location of the contacting node. If contacting nodes id and location not available in the list then it chooses a witness node randomly from the network and request for claim information. It will then updates in its own list and allows the contacting nodes for communication, if the claim information matches with the contacting node. It will permanently blocks the node for communication if there finds mismatch and send information to nearby nodes as contacting node is malicious [16-17]. Thus improves the network stability and also ensures interrupt free communications between the nodes.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

Approach of Node Capture

- Nodes are static, it means location is fixed.
- Constant location node is referred as X and Y coordinates.
- In network initialization period, replication is not possible and all fixed number nodes are trusted.
- But after certain period of time, the network can be physically captured by any one of the node which is said to be cloned.
- In the network, cloned nodes are introduced when the network enabled by the administrator.
- Restart of the network is done by any one of the following reasons
    - After shutdown or failure, network resumes.
    - A depleted or drained battery.
    - For maintenance purpose, the administrator shuts down then network.
    - Due to physical damage on any one or few nodes, the administrator may update or replaces the nodes.
- DoS attacks voluntarily jammed by the intruder in the network for certain period and replicated nodes are introduced into the network. During network is running, it directly introduces the cloned nodes by pushing node inside it.
- Definitely all the nodes either physically or logically checked in the network by counting the number of nodes when it restarts the network. It is assumed that if the initial count is 'n' and it may be after some time by count be 'n+x" , there may be some nodes added by it into the network with right authentication information.At initial count, 'n' is the number of nodes.Number of nodes added additionally into the network is 'x'.Sometimes difficult or not possible for networks of very large number of sensor nodes and for sparsely located in the environmental monitoring systems [18].

Structure Model

Figure 2. shows a sample WSN group. It consists of id and location information shown inside of 8 nodes. Nodes with id as 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', with their corresponding location as '1 to 1', '1 to 2','1 to 3','1 to 4','1 to 5','1 to 6','1 to 7','1 to 8'. The communication gets initiated immediately after these nodes are deployed. Initially, all nodes broadcast their claim message (ID and location) to the neighboring nodes and all the nodes get updated with minimum information through these broadcasts periodically. Figure 1 shows the node 'b' in location '1-2' has the information about the nodes 'e', 'c','a','h' and node 'f' after the initial deployment or the first run at time 't' and the claim message gets updated over a period of time. All nodes present in the network gets updated and have a list of information on its own.

WSN group is depicted in Figure 3. This group has 9 nodes with their ID and location information as shown inside the node. Nodes with Id a Nodes with id as 's', 't', 'u', 'v', 'w', 'x', 'y', 'z', with their corresponding location as '1-1', '1-2','1-3','1-4','1-5','1-6','1-7','1-8' and for cloned node 'a' with location as '1-9'. This cloned node enter into the network is introduced by an adversary with same existing ID 'a' in location '1-1'. The accessible range of the cloned node of 's' in location '1-9' is the node 'y' in location'1-7' and thus it enters and reaches the base station through this node 'y' by multi hop.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

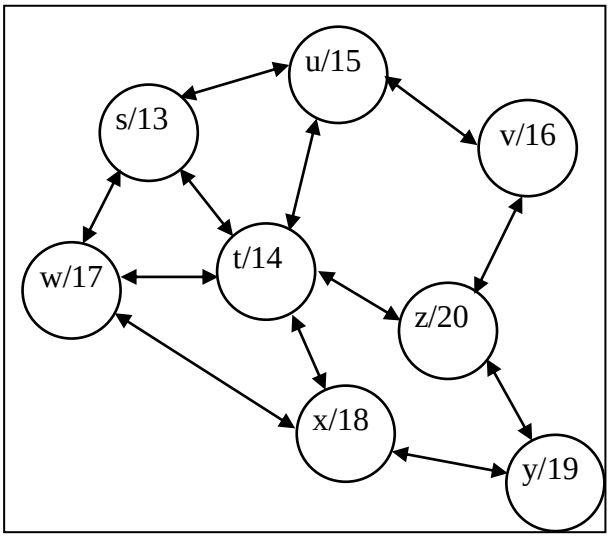

Figure 2. Nodes that are trusted along with their ID and also Location Information

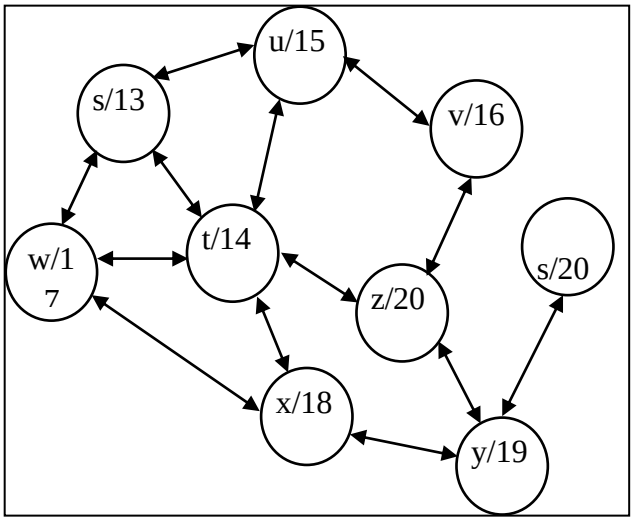

Figure 3. Nodes that are trusted along clone nodes

Until the incoherent location arises, the cloned node was allowed into the network by the proposed protocol-URED. The communication of the suspected nodes becomes blocking mode and it also raises the revocation process by the root node, when any one of the node's location mismatches in the network. The suspected nodes are nothing but that has same ID with inconsistent location and the root node is a witness node as mentioned in LSM protocol [19].

If any of the nodes in the network is tried to contact by any node from outside the network, the preliminary checking procedure is raised by the initially contaccted node. The ID and location of the entering node is initially checked by this procedure. If it is available and there is a match, the node will be allowed to participate in the network communications [20-22]. If there is a mismatch, some of the nodes in the network will be randomly chosen as witness nodes and request for claim information about the suspicious node.It is assumed that $\sqrt{n}$ nodes will be selected as witnesses from the available nodes of "n" in the network.If the answer to the queryis provided by the witness nodes,the suspecting node verifies and updates in its information table. Thus, at the initial level of contact itself the malicious or cloned node is denied entry.

The intruder can be recognized once it moves into the sensing coverage disk of any sensors. When the intruder starts form a point of the network boundary, given an intrusion distance ID≥0, the corresponding intrusion

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

detection area ID_A is almost an oblong area. A rectangular area is included by this area with length L and width 2r, and a half disk with radius r, attached to it.

$$ID_A = 2 * L * r_s + \frac{\pi r_x^2}{2} \quad (1)$$

The intruder detected if and only if, there exist at least one sensor within this area ID_A. The corresponding intrusion detection area is given in equation 2 when the intruder starts from a random point in the network domain.

$$ID_A = 2 * L * r_s + \pi r_s^2 \quad (2)$$

$$S_0 = \frac{\pi r_s^2}{2} \quad (3)$$

First, the detection probability was considered on its immediate detection by an intruder once it enters the network domain. It means, an intrusion distance ID=0 and its corresponding intrusion detection area is given in Equation 3.

The node detection theorems are explained below:

Theorem 1: The probability, $p_1[ID=0]$ that the immediate detection is done by an intruder once it enters the network with node density λ and identical sensing range r, can be given by Equation 4.

$$P_1[ID = 0] = 1 - e^{-\lambda \frac{\pi r_s^2}{2}} \quad (4)$$

Proof : Node density λ in a uniformly distributed WSN, the sensor's probability 'm' located within the area 'S' follows the Poisson distribution given in Equation 5.

$$P\ (m, S) = \frac{(S\lambda)^m}{m!} e^{S\lambda} \quad (5)$$

Thus, the probability of the number of sensors in the intrusion detection area immediately can be expressed as

$$S_0 = \frac{\pi r_s^2}{2}$$

$$p\left[0, \frac{\pi r_s^2}{2}\right] = e^{-\lambda \frac{\pi r_s^2}{2}} \quad (6)$$

Then, the complement of $p\left[0, \frac{\pi r_s^2}{2}\right]$ is

$$S_0 = \frac{\pi r_s^2}{2}$$

in this case, detection is done by the intruder once it approaches the intrusion distance D=0 in the network. And thus, the intrusion immediate detection probability by the network once it enters the WSN is expressed in Equation 7.

$$p_1[D = 0] = 1 - P\left(0, \frac{\pi r_s^2}{2}\right)$$

$$p_1[D = 0] = 1 - e^{-\lambda \frac{\pi r_s^2}{2}} \quad (7)$$

The node density and sensing range determines the result of immediate detection probability $p_1[D=0]$. When the node density and sensing ranges increases then $p_1[D=0]$ improves. The WSN deployment cost is increased by immediate detection based on large sensing range or high node density. Thus the detection probability is considered as relaxed condition in the WSN when it allows the intruder to travel some distance.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

Algorithm- Ardent Randomized, Efficient And Distributed Protocol
The algorithm of ARED Protocol is shown in Algorithm I. This algorithm show how to prevent the entry of the duplication node.

Algorithm I

Rand Receive Broadcasted Rand();
Set time-out ;
a Neighbors Of (a) :< ID_a Neighbors of (a), Is Claim (ID_a,L_a,T_a))>;
While Δ not …and Receive Message(M) do begin
For (i=0;i<n;i++)
If (node ID [i] == nodeID[i+1])
Block Data From (i);
Block Data From (i+1);
For (t=m;t>=0;t--)
Trusted Node Y=Node
At(Time [t-1]);
ID_y=Node ID at (Time[t-1]);
T_y = Time [t-1];
L_y = Location(Trusted Node Y at (Time t-1]));
end;
if Is Not Coherent(L_y, L_X)
Iteration 1: Rand Witness (ID_X, l_x, l_y, Signed Claim $_x$, Signed Claim$_y$)
WitnessNode1
Iteration 2: Response(Signed Claim $_x$, Signed Claim$_y$) Access Point
Iteration 3:(Rand Witness (ID_X, l_x, l_y, Signed Claim $_x$, Signed Claim$_y$)
&!Witness Node1)...Witness Node2
if (Claim(Witness Node1)= Claim (Witness Node2)))
Extract Claim Value ();
if ((ID Claim = = ID_y) && (L Claim = = L_y))
Grant Access(Claim(WitnessNode1)) and discard other node;
Else
Goto Iteration 1:
end;
clear MEM;

Analysis done on Ardent Randomized, Efficient And Distributed Protocol (ARED)
A new challenge task in WSN is designing protocols due to the resource constraints of these typical networks. A protocol is needed to reduce the overhead. On average even if it shows small reasonable overhead, it experiences much higher overhead in small subset of the nodes. The buffer of these nodes overflows due to the limited capacity of the node's memory since it concentrates high memory overhead on a small number of nodes. Duirng overflow, the node could drop packets or stops protocol's function inorder to make free of memory. It is very necessary to know about the knowledge of impact on this scenario of these detection protocol capabilities.

The ARED protocol is an improved and efficient protocol which concentrates on the improvement of memory and communication overhead when compared with URED protocol and classical Randomized, Efficient and Distributed Protocol. In each execution in URED Protocol, the protocol selects the random witnesses and verifies the claims. But in ARED protocol, it verifies only the information received with information available in its table in respect to their ID and location inforamation and then passes it to the other nodes. It calls for witnesses if the information received is new and it request for claim message and if both matches then the new message passes and added to its information table. The verifying node will be blocked if the matching fails. Each node has information about all other nodes present in the network after certain period. And during this

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

stage, information received at the entry point itself will be blocked when it mismatch with the available information. Consequently, no delay occurs during information passing.

The Table 1 shows the Randomized, Efficient and Distributed protocol's asymptotic notation overhead for one protocol run in the first row and it reports average overhead for a network of 1000 nodes with 31 neighbors per node (on average). A node that turns out to be much higher than the average is experienced the maximum overhead in the third row. Table 2. Shows the Notations.

Table 1. Overheads that are present in Randomized, Efficient and Distributed Protocol (n=1000, r=0.1, g=1)

	Memory Occupancy	Sent Messages	Received Messages	Signature Check
Asymptotic	O(wn.pn.dn)	O(wn.pn.dn.√n)	O(wn.pn.dn.√n)	O(wn.pn.dn)
Average (p=0.1)	1.2	12.06	68	1.87
Max (p=0.1)	15	220	250	3.6
Average (p=0.05)	0.98	10.16	39.0	1.37
Max (p=0.05)	8	69	86	20

Table 2. Notations

Notation	Significance
N	Number of nodes in the network
ID	The identity of node i
Dn	Average degree of each node
Wn	Number of witness nodes
W	Witness node nearby edge or vertices of the sample space
PK_i, SK_i	The public key and private key of node i
Pn	Probability a neighbor will replicate location information
H(M)	Hash of M
l_α	Location node α Claims to occupy
S	Sample Space
A	'A' may be an event

1.1 Detection probability of the malicious node

During a sequence of iterations, the clone detection probability was investigated in this section. Assume that an intruder cloned a node and the subset of 'w' randomly selected other nodes are already controlled by it without implementation mechanism of preventing from packet dropping and thus malicious nodes stop forwarding the claim. Also assume a cloned node 'a' and 'a^1' is one of a's clone node which is randomly deployed within the network area. And assume that from each neighborhood exactly one claim message is sent and doesnot occur routing failure. Both claims are sent through path of length $l = c\sqrt{n}$ nodes.

The nodes on the two paths (first one departing from the honest node 'a' and the cloned node 'a^1' is the second node) are involved by two protocols in the detection process. And the corrupted forwarding node simply drops the received location claim. The probability of atleast one malicious node present in two paths (P_t)is expressed in Equaiton 8.

$$Pt = 1 - \frac{\binom{n-w}{21}}{\binom{n}{21}} \quad (8)$$

For single iteration using the Ardent Randomized, Efficient and Distributed Protocol (ARED) protocol, the probability of not detected attack is exactly in Equation 4. Assume by analyzing a sequence of iterations, all

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

iterations are probabilistically independent. The Equation 9 expresses the probability of undetected attack (P_u)after 'i[th]' Ardent Randomized, Efficient and Distributed Protocol (ARED) protocol iteration.

$$Pu = \left(1 - \frac{\binom{n-w}{21}}{\binom{n}{21}}\right)^{i} \quad (9)$$

RM and LSM analysis were different. The attack is detected only with the probability (when 'a' and 'a[1]' intersects each on a network node) even then all nodes are honest. In Parno et al 2005 analysis, the probabilityPi proposed in Equation 10

$$Pi = \frac{1}{3}\left(1 - \frac{35}{12\pi^2}\right) \quad (10)$$

However, the above probability refers to geometric line intersection in LSM was observed. Then it is an optimistic upper bound since no failure in the routing assumption. In fact, two intersecting paths (geometrically) do not have a node in common. Geometrically, no two intersecting paths have a node in common. In single protocol iteration, 'EA' be the event that the attack is not detected and two disjoint events are considered for Ardent Randomized, Efficient and Distributed Protocol (ARED). It is possible for the malicious node to be prevented by clone detection when there is a path present before the witness.

Let us define:
Event E_h : All the forwarding nodes in the network before the possible witness nodes are honest.
Event E_m: Atleast one malicious node forwarding before the possible witness.
Now, E_h and E_m form a partition of the probability space and it is given in Equation 11.

$$P[EA] = P[EA|[E_h]P[E_h] + P[EA|[E_m]P[E_m] \quad (11)$$

Where $Pr[U|[E_h]$ is the probability of undetected attack when there are no malicious nodes in the paths.

$$Pr[U|[Eh] = 1 - \frac{1}{3}\left(1 - \frac{35}{12\pi^2}\right) = \frac{1}{3}\left(2 + \frac{35}{12\pi^2}\right) \quad (12)$$

Assume that $P[U|E_m] = 1$ since it may discard the claim and stop the detection by the malicious node before the witness. The probability of the malicious nodes appear before the witness is $P[E_m] = 1\text{-}P[E_h]$. The witness is in the middle of the paths and therefore on average, the probability estimations is expressed in Equation 12.

$$P[E_m] = 1 - \frac{\binom{n-w}{1}}{\binom{n}{1}} \quad (13)$$

Putting it altogether, compute P(U) and which is given in Equation (13)

$$P[U] = 1 - \frac{\binom{n-w}{1}}{\binom{n}{1}}\left(\frac{35}{36\pi^2} - \frac{1}{3}\right) \quad (14)$$

After i[th] Ardent Randomized, Efficient and Distributed Protocol (ARED) protocol iterations that the probability not detected is given in Equation (14).

$$P[RA] = 1 + \frac{\binom{n-w}{1}}{\binom{n}{1}}\left(\frac{35}{36\pi^2} - \frac{1}{3}\right) \quad (15)$$

SIMULATION RESULT

Consider that a unit square of deployment area has a fixed number of n = 1000 nodes in the following simulations and the communication radius between these are r = 0.1m, set g =1 and p =0.1 for both Unassailable Randomized, Efficient and Distributed Protocol (URED) and Ardent Randomized, Efficient and Distributed Protocol (ARED) protocols. On an average same number of location claims are send per node by the protocols. Assume that the nodes are uniformly distributed at random location in the network. The neighbor closest node to destination is the relay node to simulate the same geographic routing protocol. When there is no node closest to destination then the routing will be stopped and the current node will be a witness node. The network with no

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

convex area deployment in the sensor creats a problem of 'dead ends' places while the destination is still far and no node closer to destination for the message to proceed.

The performance of the ARED protocol is analyzed for various simulation parameters and result is listed in the Table 3.

Table 3. performance of the Ardent Randomized, Efficient and Distributed Protocol (ARED) protocol

	Memory Occupancy	Sent Messages	Received Messages	Signature Check
Asymptotic	O(g.p)	O(g.p√n)	O(g.p√n)	O(g.p)
Average (p=0.1)	0.21	3.16	6.1	1.57
Max (p=0.1)	25	220	250	58
Average (p=0.05)	0.15	1.58	3.05	2.11
Max (p=0.05)	7	76	89	22

With the help of crossbow motes and motewieview software the protocol was tested in real time. There are five environmental sensing nodes were taken for an experiment and any one of that node was physically captured and cloned. The nodes with IDs 612, 622, 632, 642 and 652 were considered and its communication initiated between the coordinator and with those nodes. After capturing the necessary information, the node542 was captured and made as clone of node 5325 through reprogramming. And thus clone node introduced into the network to perform malicious activities by the adversary for further communication. And this proposed Ardent Randomized, Efficient and Distributed Protocol (ARED) will not allow any cloned node to enter into the network.

Performance Characteristics

The Ardent Randomized, Efficient and Distributed Protocol (ARED) protocol's performance is analyzed with penalty factor against different parameters viz. pruned count, throughput and node density.

Storage Overhead

The nodes report the number of messages that it required to store for URED and ARED protocols. It shows the percentage of nodes that needs to store that the number of messages for a fixed n-value of messages in the memory. The values in 1000 simulations give the result by averaging. In our proposed protocol, some nodes may store as many as 100 messages. This ARED protocol need 1.4 percent of the nodes to store more than 40 messages, 3 percent of nodes store a number of messages between 20 and 39, and 18 percent of the nodes to store a number of messages between 10 and 20. To store less than 8 messages around 40 percent of the nodes are required. A negligible percentage of the nodes of 0.001 percent require more than 10 messages to store for Unassailable Randomized, Efficient and Distributed Protocol (URED). To store more than 4 messages it needs 0.2 percent and store number of messages between 2 and 4 for less than 8 percent.

There is a need of storing only one or two messages for 40 percent of the nodes while 20 percent of the nodes never need any messages at all for storing. Finally, in Unassailable Randomized, Efficient and Distributed Protocol (URED) it is observed that only 0.2 percent of the nodes never require storing any message. And hence ARED protocol when compared to URED protocol needs higher number of messages for storing. This make out clear concern that every node in a claim path is a possible witness in ARED protocol and therefore it is to be stored each and every claim that the witness relays. In URED protocol, only in first run the randomly selected nodes to be the witnesses and thus it requires only the destination to be stored the claims.

To overcome the energy overhead of URED and ARED protocols, the communication and computation are considered. This includes the operation of public key cryptography, signature generation and signature verification. A node battery of 323,000 mJ,15.103 mJ for sending a packet, 7.167 mJ for receiving a packet and 44.0 mJ for both signature generation and verification. Thus the operation of a node depends upon its battery. It results different patterns of node energy exhaustion of different energy overheads for two given protocols.. In ARED protocol, 20 percent of nodes and in URED protocol, 8 percent of nodes are exhausted after 100 iterations of the protocols. For ARED protocol and URED protocol, 32 percent and only 21 percent of exhausted nodes are shown after 150 iterations. Finally, after 200 iteration run, half of the nodes of the network are

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

exhausted in ARED protocol and only 31 percent for URED protocol and detection capabilities are still remarkable.
In these two protocols most of the exhausted nodes are in the center. In the presence of uniform traffic, the nodes in the center involve more in routing the messages in the network. In case of ARED protocol, mostly all the nodes in the center are exhausted except a few isolated ones and the overhead transferred to semi central areas. Various distributions of node exhaustion imply different clone attack detection probability.

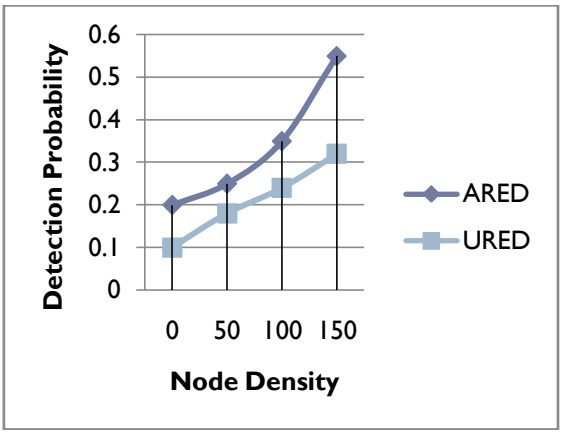

Figure 4. Detection probability ratio

The Figure 4 shows the detection probability for different protocols that has been observed. The graph plotted for the detection probability of 200 runs. This shows that the RED has the probability of 0.35 and the URED has the probability of 0.25.

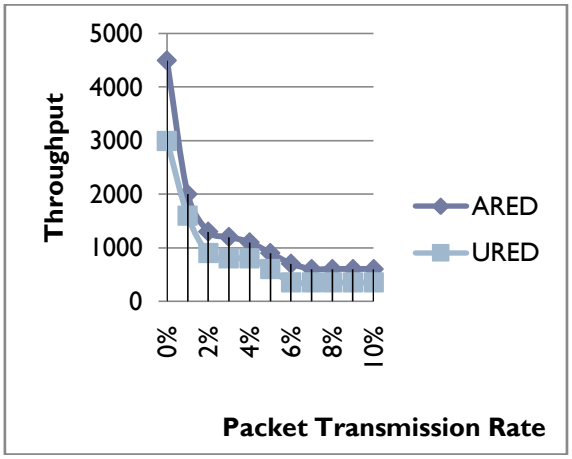

Figure 5. Packet loss verses Throughput

For the first 200 runs the detection probability was plotted. The plotted values were computed by averaging the result for 1000 network deployments. Evaluation is done by each single deployment for URED and ARED protocols. When compared with all iterations, the ARED protocol shows better detection probability than Unassailable Randomized, Efficient and Distributed Protocol (URED). Probability detection is about 0.89 for upto 30th iteration in ARED protocol and 0.97 for URED protocol. At least five witness nodes were designed for ARED. Figure 5 shows the packet loss verses throughput. Figure 6 shows prudent count verses Energy consumption.

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

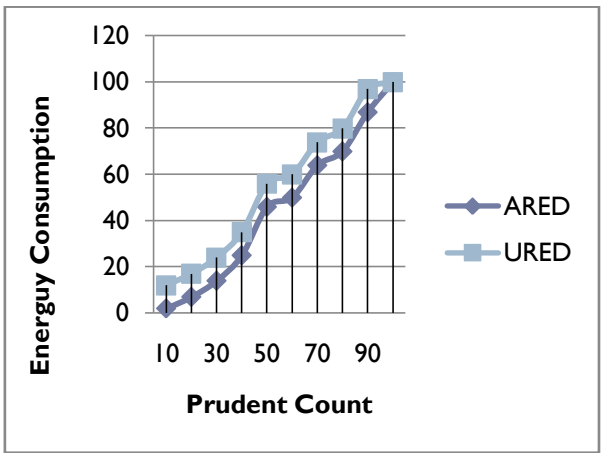

Figure 6. Prudent count verses Energy consumption

The parameters are set at least three witnesses for URED and thus the detection probability of ARED will be similar to the detection probability of URED but with higher overhead. To make fair comparison from a performance standpoint the parameters has been set similarly for an each iteration of ARED and URED. The detection probability is 0.99 and 0.89 for ARED and URED for the first 10 protocol runs when nodes are not compromised.

CONCLUSION

A distributed detection of node replicas has been justified by a few basic requirement of an ideal protocol. A measure of the quality such as resilience to smart attack was satisfied. On observation, protocol with less overhead is not enough but also evenly distributed among nodes both in computation and memory is necessary. Further, a new threat model and self-healing, randomized, efficient and distributed protocol to detect node replication attacks were suggested by our ARED and analytically achieves remarkable improvements in malicious node detection probability and thus almost evenly balanced among the nodes. Lastly, the analysis shows that ARED are more resilient in its detection capabilities than URED in the presence of compromised nodes. The detection probability increases consequently in all iterations. And on at tenth iteration for URED protocol is 0.89 and for ARED is 0.99. Finally, concluded that overheads in ARED protocol are negligible even in critical application when compared with URED protocol.

REFERENCES

1. *Aalsalem, M. Y., Khan, W. Z., Saad, N. M., Hossain, M. S., Atiquzzaman, M., & Khan, M. K. (2016). A New Random Walk for Replica Detection in WSNs. PloS one, 11(7), e0158072.*
2. *Augustine, J., Pandurangan, G., Robinson, P., Roche, S., & Upfal, E. (2015, October). Enabling robust and efficient distributed computation in dynamic peer-to-peer networks. In Foundations of Computer Science (FOCS), 2015 IEEE 56th Annual Symposium on (pp. 350-369). IEEE.*
3. *Bhoite, M. S. A., Jalindar, C. S., Hanumant, G. V., SA, S., & Scholar, U. G. (2016). Low Priced And Efficient Energy Replica Detection In WSN.International Journal of Engineering Science, 4155.*
4. *Bokare, M., & Ralegaonkar, A. (2012). Wireless Sensor Network.International Journal of Computer Engineering Science (IJCES), 2(3).*
5. *Conti, M. (2016). Clone Detection. In Secure Wireless Sensor Networks (pp. 75-100). Springer New York.*
6. *Conti, M., Di Pietro, R., & Spognardi, A. (2014). Clone wars: Distributed detection of clone attacks in mobile WSNs. Journal of Computer and System Sciences, 80(3), 654-669.*
7. *Elkin, M., & Neiman, O. (2016). On Efficient Distributed Construction of Near Optimal Routing Schemes. arXiv preprint arXiv:1602.02293.*
8. *John, J. S., Kayalvizhi, R., & Vaidehi, V. (2014). Cluster Based Mechanism for Clone Detection in WSN. Wireless Communication, 6(4), 134-139.*
9. *Khan, W. Z., Aalsalem, M. Y., Saad, M. N. B. M., & Xiang, Y. (2013). Detection and mitigation of node replication attacks in wireless sensor networks: a survey. International Journal of Distributed Sensor Networks,2013.*

ISSN 2349-6193
Impact Factor: 2.805

IJESMR
International Journal OF Engineering Sciences & Management Research

10. *Khan, W. Z., Hossain, M. S., Aalsalem, M. Y., Saad, N. M., & Atiquzzaman, M. (2016). A cost analysis framework for claimer reporter witness based clone detection schemes in WSNs. Journal of Network and Computer Applications, 63, 68-85.*
11. *Lee, Y. S., & Chung, S. H. (2016). An efficient distributed scheduling algorithm for mobility support in IEEE 802.15. 4e DSME-based industrial wireless sensor networks. International Journal of Distributed Sensor Networks, 2016, 1.*
12. *Maheswari, P. U., & Kumar, P. G. (2015). Distributed defense mechanism for clone attacks based on gravitational search algorithm (GSA) in WSN.Tehnički glasnik, 9(4), 370-380.*
13. *Manickavasagam, V., & Padmanabhan, J. (2016). A mobility optimized SPRT based distributed security solution for replica node detection in mobile sensor networks. Ad Hoc Networks, 37, 140-152.*
14. *Mishra, A. K., & Turuk, A. K. (2016). A comparative analysis of node replica detection schemes in wireless sensor networks. Journal of Network and Computer Applications, 61, 21-32.*
15. *Mishra, P., & Gupta, G. (2016). Detection of Node Replication Attacks in MSN Using EDD Algorithms.*
16. *Pandurangan, G., Robinson, P., & Scquizzato, M. (2016, July). Fast distributed algorithms for connectivity and MST in large graphs. InProceedings of the 28th ACM Symposium on Parallelism in Algorithms and Architectures (pp. 429-438). ACM.*
17. *Rodrigues, J. J., & Neves, P. A. (2010). A survey on IP-based wireless sensor network solutions. International Journal of Communication Systems,23(8), 963-981.*
18. *Radley, S. (2013). Transitional Survey ON IPv4-IPv6. International Journal on Information Sciences & Computing, 7(1).*
19. *Sindhuja, L. S., & Padmavathi, G. (2016). Replica Node Detection Using Enhanced Single Hop Detection with Clonal Selection Algorithm in Mobile Wireless Sensor Networks. Journal of Computer Networks and Communications, 2016.*
20. *Suryadevara, N. K., & Mukhopadhyay, S. C. (2012). Wireless sensor network based home monitoring system for wellness determination of elderly. IEEE Sensors Journal, 12(6), 1965-1972.*
21. *Tsai, S. C., Tseng, Y. H., & Chang, T. H. (2016). Communication-efficient distributed demand response: A randomized admm approach.*
22. *Vinayagamoorthy, M., & Ramesh, V. (2016). Secure And Energy Efficient Transmission For Cluster-Based Wireless Adhoc Networks.*
23. *Xu, K., Hassanein, H., Takahara, G., & Wang, Q. (2010). Relay node deployment strategies in heterogeneous wireless sensor networks. IEEE Transactions on Mobile Computing, 9(2), 145-159.*
24. *Yu, D., Hua, Q. S., Wang, Y., Tan, H., & Lau, F. C. (2016). Distributed multiple-message broadcast in wireless ad hoc networks under the SINR model. Theoretical Computer Science, 610, 182-191.*
25. *Zhang, J., & Varadharajan, V. (2010). Wireless sensor network key management survey and taxonomy. Journal of Network and Computer Applications, 33(2), 63-75.*