iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 3 **Issue:** IV **Month of publication:** April 2015

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

Volume 3 Issue IV, April 2015
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Performance Metrics and Analysis for Node Clone Detection Schemes in Wireless Sensor Networks

K.Vijayalakshmi[1], Dr.P.Marikkannu[2]
[1]*Anna University, Regional Centre-Coimbatore*
[2]*Assistant Professor, Department of Information Technology, Anna University, Regional Centre-Coimbatore*

Abstract: ***Wireless sensor networks are now-a-days rapidly developing in the field of science and technology. And it promises to have a large number of applications in next generation networks (NGN). The wireless sensor networks can be easily attacked from various sides and one of the serious attacks faced by the wireless sensor networks is the node clone attack. The node clone attack acts as the basic method to mount a huge insider attack. The cloned nodes must be detected in order to minimize the damages caused by them to the network. To protect the network from the clone attacks is to prevent an adversary from extracting the secret key materials from the captured node. Thus, various protocols were proposed to detect the cloned nodes in the network. To detect the cloned nodes from the network two existing protocols were addressed named as RM (randomized multicast) and XED (extremely efficient detection). In RM, each node broadcasts a location claim to its one-hop neighbors. Then, each neighbor selects randomly witness nodes within its communication range and forwards the location claim with a probability to the nodes closest to chosen locations by using geographic routing. At least one witness node is likely to receive conflicting location claims according to birthday paradox when replicated nodes exist in the network. The key idea of XED is to detect clones by providing the random numbers to the other nodes and asking for random number while meeting the node again. Thus, the cloned nodes will be detected by using the above mentioned protocols.***

I. INTRODUCTION

Wireless sensor network is a collection of sensors with limited resources that combined together to achieve a common goal. The sensors will communicate with each other over wireless channels. The wireless sensors will be often placed in an environment where nodes can be easily captured and compromised.

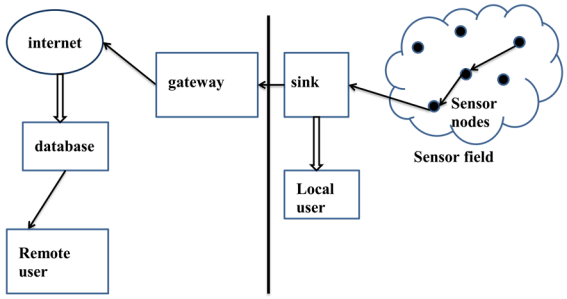


Fig 1. Wireless sensor network

The fig 1. shows the various components of a wireless sensor network like a sink, gateway, sensor nodes, etc

Since wireless sensor networks are placed in hostile environments, it is challenging to provide efficient security mechanisms for WSNs.

II. NODE REPLICATION ATTACKS

Sensor networks are often deployed in a hostile environment to perform critical missions, and the sensor networks are unattended.

The sensor nodes are normally unequipped with tamper-resistant hardware. This gives a situation where the adversary can capture compromise one sensor node, produce many replicas of the captured having the same identity (ID) and place these replicas back into strategic positions in the network for further malicious activities. This is a so-called *node replication attack*. Since the replicated nodes are the clones of the captured nodes, the replicas can be considered as legitimate members of the network and detecting those nodes are difficult. From the security point of view, the node clone attack is very harmful to networks, because replicas have secret keys and credentials and thus launching many insider attacks.

Causes of node replication attacks:

A. the replicated node contains the same identity as the legitimate member, creates an extensive harm to the network
B. various attacks will be Created by extracting the secret credentials of the captured node
C. monitoring operations will be corrupted by injecting the false data
D. denial of service attacks will also be initiated
E. detecting the replication is complicated makes authentication difficult

Wireless sensor network can be either stationary or mobile. In static wireless sensor networks (SWSNs), the sensor nodes are stationary or static and after deployment sensor nodes positions will not be changed.

III. CLONE DETECTION TECHNIQUES

After compromising a sensor node, a clone attack can be launched by replicating the captured nodes and injecting them sporadically over the networks such that the adversary can enlarge the compromised areas by employing the clones.

The selection criteria of clone detection schemes were based on,

A. device types
B. detection methodologies
C. deployment strategies
D. detection ranges
E. according to their mobility, sensor nodes are divided in to static and mobile sensors
F. the detection schemes were classified based on centralized and distributed schemes
G. deployment strategies were classified based on random uniform deployment and grid deployment strategies
H. according to clone detection locations, whole area and local area detection schemes

Classification of existing clone detection schemes based on following criteria,

A. Device type : static sensor versus mobile sensor
B. Detection method : centralized detection versus distributed detection
C. Deployment strategy: random uniform deployment versus grid deployment
D. Detection range : whole area detection versus local area detection

Clone detection schemes for static wireless sensor networks:

A. Static, centralized, random uniform and whole(SCRW)
B. Static, distributed, random uniform and whole(SDRW)
C. Static, distributed, grid and whole(SDGW)
D. Static, distributed, grid and local(SDGL)

IV. RELATED WORKS

Attacks are categorized in to active and passive attacks [1] and also internal attacks and external attacks[9]. Passive attacks can be grouped into eavesdropping, node malfunctioning, node tampering destruction and traffic analysis types. Active attacks can be grouped into Denial-of-Service (DoS), jamming, hole attacks (black hole, wormhole, sinkhole, etc.), flooding and Sybil types. The existing clone detection schemes and selection criteria for clone detection schemes with regard to device types, detection methodologies, deployment strategies, and detection ranges were proposed in [2]. And also the adversary model and clone detection scenario was proposed. the localized algorithms to prevent the network from the clone attacks and advantages of these localized algorithms are discussed in [3] which includes, 1) localized detection 2) efficiency and effectiveness 3) network-wide

synchronization avoidance and 4) network-wide revocation avoidance .according to the above discussed classification of clone detection schemes two algorithms were proposed in [4] and they are XED(extremely efficient detection),EDD(efficient distributed detection).and in [6],DHT(distributed hash table) and RDE(randomly directed exploration) and one more protocol called RED(randomized efficient distribution)was proposed in[10].XED algorithm have storage overhead of O(n). EDD algorithm's detection time increases based on the number of neighbor nodes and is showed in [5] two more efficient distributed protocols for detecting node replication attacks were proposed in [8] and they are Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cells (P-MPC).

V. SYSTEM MODEL

A. *Network Model*

Assume that the sensor network consists of sensor nodes with IDs {1…n}. The communication is assumed to be symmetric. In addition, each node is assumed to periodically broadcast a beacon containing its ID to its neighbors. This is usually required in various applications, for example, object tracking. The time is divided into time intervals, each of which has the same length. Nonetheless, the time among sensor nodes does not need to be synchronized. The sensor nodes have mobility and move according to the Random Way Point (RWP) model, which is commonly used in modeling the mobility of *ad hoc* and sensor networks. Each node is assumed to be able to be aware of its geographic position.

B. *Security Model*

In our methods, sensor nodes are not tamper-resistant. In other words, the corresponding security credentials can be accessed after sensor nodes are physically compromised. Sensor nodes could be compromised by the adversary immediately after sensor deployment. The adversary has all of the legitimate credentials from the compromised nodes. After that, the adversary deploys two or more nodes with the same IDs i.e., replicas, into the network. Replicas can communicate and collude with each other in order to avoid replica detection in EDD. For example, replicas can share their credentials and can selectively be silent for a certain time if required after the collusion. Owing to the use of the digital signature function, the replicas cannot create a new ID or disguise themselves as the nodes being not compromised before, because it is too difficult for the adversary to have the corresponding security credentials. Since the focus of this paper is on the node replication attack, despite many security issues on sensor networks such as key management, replay attack, wormhole attack, Sybil attack, secure query, etc., we assume that they can be well handled.

VI. THE CLONE DETECTION METHODS

The two proposed methods for node clone detection are XED (extremely efficient detection) and RM (randomized multicast)

A. *XED (extremely efficient detection):*

The idea behind XED is motivated by the observation that, if a sensor node meets another sensor node at an earlier time and sends a random number to at that time, then, when and meet again, can ascertain whether this is the node met before by requesting the random number. Note that, in XED, it is assumed that the replicas cannot collude with each other. In addition all of the exchanged messages should be signed unless specifically noted.

Specifically, the XED scheme is composed of two steps: an offline step and an online step. The former is executed before sensor deployment while the latter is executed by each node after deployment.

Offline Step. A security parameter and a cryptographic hash function ***H(.)***are stored in each node. Additionally, two arrays, ***Lr(u)*** and ***Ls(u)***, of length , which keep the received random numbers and the materials used to check the legitimacy of received random numbers, respectively, along with a set ***B(u)*** representing the nodes having been blacklisted by , are stored in each node ***u*** .***Lr(u)*** and ***Ls(u)*** are initialized to be zero-vectors. ***B(u)*** is initialized to be empty.

Online Step. If encounters for the first time, randomly generates ***α € [1,2b-1]*** computes ***H(α),*** sends ***H(α)*** to ***v*** , and stores ***Ls(u)*****[v]=α** . Note that ***u*** knows that it encounters for the first time if ***Ls(u)*****[v]=0**.

When ***u*** encounters ***v***, it first checks if is in the blacklist ***B(u)***. If so, this means that ***v*** is considered a replica by ***u*** and ***u*** refuses to communicate with ***v***. If not, the following procedures are followed. They exchange the random numbers ***Lr(u)[v]*** and ***Lr(v)[u]***. From the viewpoint of node ***u***, after the reception of the random number ***Lr(v)[u]*** sent by ***v***, ***u*** checks if ***Lr(v)[u]*** the random number is ***u*** sent to ***v*** last time. This can be accomplished by verifying ***H(Ls(u)[v])=Lr(v)[u]*** if holds. Node ***v*** is added into ***B(u)*** if the

verification fails. Otherwise, the same procedure, including randomly generating a new ***α***, computing ***H(α),*** sending ***H(α)*** to ***v***, and replacing the old

Lr(u)[v] with a new ***Lr(u)[v]=α***, is performed. For the replica that does not possess the correct random number, due to the one way property of the cryptographic hash function, the probability of successful verification is only ***1h2b -1***. The same procedure applies for node ***v.*** Note that ***B(u)***'s could be different for different nodes. This can be attributed to the fact that each node detects the replica by itself and will detect the replica at different time. Nonetheless, we can guarantee that the replica will be blacklisted by all nodes eventually.

B. RM (Randomized Multicast):

In a WSN using the RM clone detection algorithm, upon receiving a location claim, a node randomly chooses a set of g nodes to act as witnesses. A clone ˜ni of node ni will therefore be detected if and only if one of ˜ni's neighbors randomly selects the same witness as one of ni's neighbors. This event has probability,

$$\mathbb{P}_{RM}[\tilde{n}_i \text{ detected}] = 1 - \prod_{i=1}^{\gamma-1}\left(1 - i\frac{pdg}{N}\right)^{pdg}$$ ...eqn.1

In equation 1, p denotes the probability that a neighbor forwards the location claim to the set of witness nodes, d the average number of neighbors, g the number of witnesses, the number of clones of one captured node and N the total number of nodes in a WSN. Using this approach, cloned nodes will be detected with high probability when $pdg \approx \sqrt{N}$.

C. Protocol description:

The protocol has each node broadcast its location claim, along with a signature authenticating the claim. Each of the node's neighbors probabilistically forwards the claim to a randomly selected set of witness nodes. If any witness receives two different location claims for the same node ID, it can revoke the replicated node. The birthday paradox ensures that we detect replication with high probability using a relatively limited number of witnesses.

More formally, each node α broadcasts a location claim to its neighbors β1,β2…βd. The location claim has the format IDα,lα,{h(IDα,lα)}kα. where lα represents α's location (e.g., geographic coordinates (x, y)). Upon hearing this announcement, each neighbor, βi, verifies α's signature and the plausibility of lα(for example, if each node knows its own position and has some knowledge of the maximum propagation radius of the communication layer, then it can loosely bound α's set of potential locations). Then, with probability p, each neighbor selects g random locations within the network and uses geographic routing to forward α's claim to the nodes closest to the chosen locations .Since we have assumed the nodes are distributed randomly, this should produce a random selection from the nodes in the network. The probability of selecting the same node more than once is generally negligible. Collectively, the nodes chosen by the neighbors constitute the witnesses for α. Each witness that receives a location claim first verifies the signature. Then, it checks the ID against all of the location claims it has received thus far. If it ever receives two different locations claims for the same node ID, then it has detected a node replication attack, and these two location claims serve as evidence to revoke the node. It blacklists α from further communication by immediately flooding the network with the pair of conflicting location claims, lα and lα'. Each node receiving this pair can independently verify the signatures and agree with the revocation decision. Thus, the sensor network both detects and defeats the node replication attack in a fully distributed manner. Furthermore, the randomization prevents the adversary from predicting which node will detect the replication.

VII. PERFORMANCE EVALUATION

Five performance metrics are used in this evaluation:

A. Detection Accuracy

Detection accuracy is used to represent the false positive ratio and false negative ratio of the underlying detection algorithm, which are the ratios of falsely considering a genuine node as a replica and falsely considering a replica a genuine node, respectively.

B. Detection Time

Detection time is evaluated according to the average time (or, equivalently, the number of moves) required for a genuine sensor node to add the replica's ID into.

C. Storage Overhead

Storage overhead is counted in terms of the number of records required to be stored in each node. Here, the *records* differ in different algorithms. For example, a record is a tuple containing an ID, time, location, and signature in while a record involves only an ID, location, and signature in. If the storage overhead is counted in terms of the number of *bits*, a multiplicative factor O(log n) is obviously needed due to the space for IDs. Nonetheless, for fair comparison, we do not use such bit-based storage estimation.

• *Computation Overhead*—Computation overhead accounts for the number of operations required for each node to be executed per move.

•*Communication Overhead*—Communication overhead accounts for the number of records required for each node to be transmitted. Similarly, it can be considered in terms of the number of bits, but we do not use such a kind of estimation.

VIII. COMPARISON

Table 1, shows the comparison between communication cost and memory for various clone detection protocols

Protocol Name	Communication Cost	Memory
Preliminary Approach	O(n)	O(n)
SET	O(n)	O(d)
SPRT	O(n)	O(d)
Deterministic Multicast	O(g ln g√n / d)	O(g)
RED	O(r √n)	O(r)
Randomized Multicast	O(n²)	O(√n)
Line-Selected Multicast(LSM)	O(n√n)	O(√n)
SDC	O(r_f√n)+O(s)	g
P-MPC	O(r_f√n)+O(s)	g
XED	O(1)	
EDD	O(1)/O(n)	O(N)
UTLSE & MTLSD	O(n)	O(√n)

Table 1: comparison between various protocols

IX. RESULTS

A. XED

XED is one of the centralized techniques and its advantages are communication cost is constant, location information is not required to detect cloned nodes

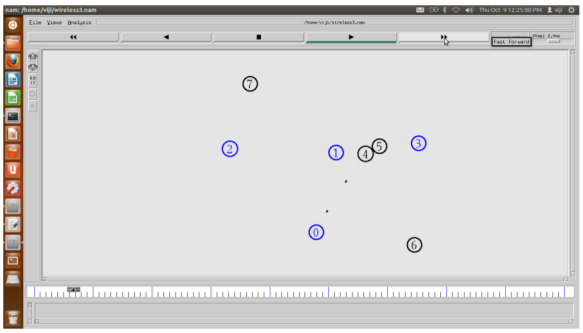


Fig 2. Communication between nodes and cloned nodes

The figure 2, shows the packet transmission between the nodes and cloned nodes. The node 0 is sending the packet and node 4 is receiving the packet and vice versa.

B. RM

RM is one of the distributed techniques. Advantages are less communication cost, less storage requirement, high detection rate

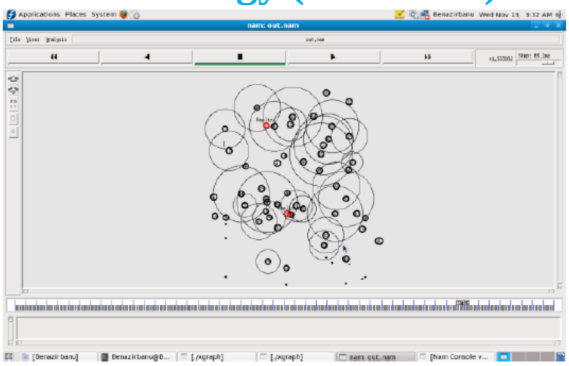


Fig 3. Detection of cloned nodes

The figure 3, consists of 50 nodes and the red color indication shows the cloned nodes and the cloned nodes are avoided from communication

X. CONCLUSIONS AND FUTURE WORK

Considering that sensors may not be equipped with tamper resistant hardware, it is crucial to provide a detection system against clone attacks. XED (extremely efficient distribution), here a node will send a random number to the another node and while meeting the node again it will ask for the same random number. If it doesn't have a random number then the node will be considered as clone.

RM scheme, nodes broadcast to neighboring nodes the location claim message signed by ID-based public key scheme then the neighbors forward such received claim message with a specified probability to randomly selected network nodes, which act as witness. According to the birthday paradox, the nodes owning the same ID would select same witness nodes with a big probability. These witness nodes eventually detect replicas successfully

The future work is to enhance the XED and RM protocol using AIS (artificial immune system) and the performance will be compared between the existing system and the enhanced system.

REFERENCES

[1] Butun I., Salvatore D., Morgera and Sankar R. (2014)," A Survey of Intrusion Detection Systems in Wireless Sensor Networks, " IEEE Communications Surveys & Tutorials, Vol. 16, No. 1

[2] Cho K., Jo M., Kwon T., Chen H. and Lee D. (2013),"Classification and Experimental Analysis for Clone Detection Approaches in Wireless Sensor Networks," IEEE Systems Journal, Vol. 7, No. 1

[3] Yu C., Tsou Y., Lu C and Kuo S. (2013), "Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks," IEEE Transactions On Information Forensics And Security, Vol. 8, No. 5

[4] Dr.M.BalaGanesh ,S.NithyaDhevi,(2013)" A Survey of Dynamic Detection of Node Replication Attack in Wireless Sensor Network,"in the proceedings of International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682 Vol.18, No.18

[5] Banu B., Angayarkanni A (2014)" Mobility Based Algorithms For Detection Of Clone Nodes In Mobile Sensor Networks,"in the proceedings of International Journal of Advanced Research in Computer Engineering & Technology (IJARCET) Volume 3 Issue 4

[6] Li Z. and Gong G.(2013)"On the Node Clone Detection in Wireless Sensor Networks," ieeehacm transactions on networking, vol. 21, no.6

[7] Anandkumar K.M. ,C. Jayakumar(2012) ,"Pro-Active Prevention of Clone Node Attacks In Wireless Sensor Networks," in the proceedings of Journal of Computer Science 8 (10): 1691-1699ISSN

[8] Geetha C,"A Review on Replica Node Detection Algorithms in Wireless Sensor Networks," in the proceedings of International Journal of Computational Engineering Research||Vol, 03||Issue,8||

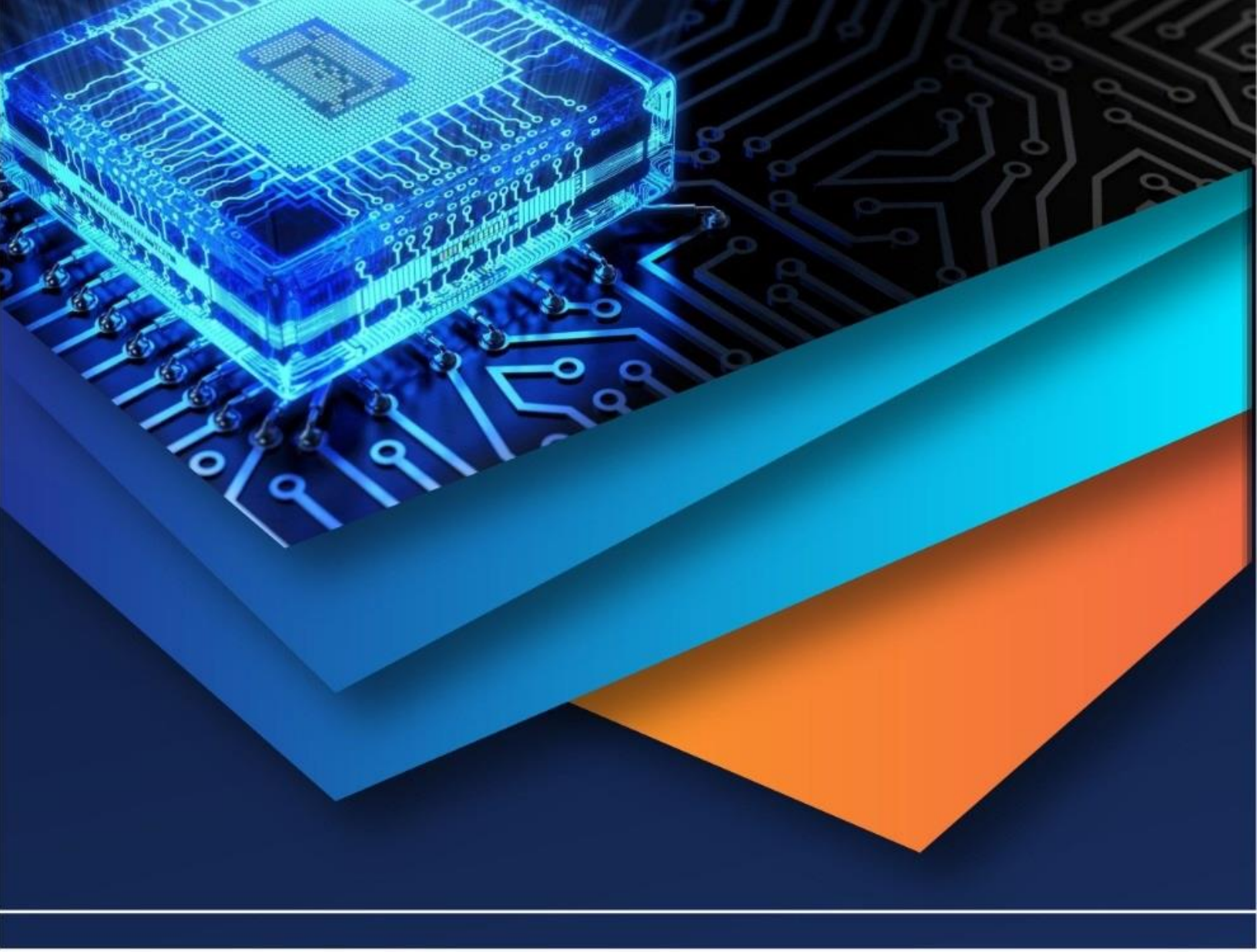
[9] Raju M et al(2014), "An Approach in Detection of Replication Node in Wireless Sensor Networks: A Survey," in the proceedings of International Journal of Computer Science and Information Technologies, Vol. 5 (1), 192-196

Volume 3 Issue IV, April 2015
ISSN: 2321-9653

AUTHORS BIOGRAPHY

VIJAYALAKSHMI KRISHNASAMY has completed her bachelor's degree in engineering in electrical and electronics from info institute of engineering, Coimbatore
Tamilnadu, India (2011) and presently pursuing master of engineering in the department of mobile and pervasive computing under the board of information and communication engineering in Anna university regional centre, Coimbatore, tamilnadu, India. Her research interests are pervasive computing, wireless sensor networks.

Dr.P. MARIKKANNU received his Ph.D (Information and Communication Engineering) from Anna University Chennai and Masters (Master of Technology) in Information Technology from College of Engineering, Guindy, Anna University, Chennai. He is working as an Assistant Professor in the Department of Information Technology, Anna University Regional Centre, Coimbatore. He has published many research articles in various Journals. His research interests include Agent-Based Intelligent Systems, Network Security, Data Mining, Cloud Computing and Distributed Computing. Dr.P.Marikkannu is a life member of ISTE.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY