A STUDY OF CLONE DETECTING TECHNIQUES IN STATIONARY AND MOBILE WIRELESS SENSOR NETWORK

R.Priyadharshni

PG Scholar/CSE
Anna University Regional centre, Madurai
Email:priyadharshni23@gmail.com

R.Selva Bharathi

PG Scholar/CSE
Anna University Regional centre, Madurai
Email:selin.rathna@gmail.com

Mr.S.Ramesh

Faculty/CSE,
Anna University Regional centre, Madurai
Email: rameshcse@autmdu.ac.in

***Abstract*—Mobile Wireless sensor network (MWSN) is one of the recently emerging areas in which mobility of sensor nodes play a major role. Sensor nodes are allowed to move freely and are allowed to communicate with each other without a need for fixed infrastructure. Sensor nodes are not equipped with tamper resistant hardware which arises many security challenges. Some of threats are clone attack, Wormhole attack, Sybil attack etc. The attack concentrated in this paper is Clone attack. Here, adversary subverts the network by just introducing replicas of previously compromised nodes. We have some traditional approaches to detect cloned nodes in stationary sensor nodes. The mobility of sensor nodes increases the challenges faced while detecting clone attacks. Recent research work leads to design of many protocols to detect clone in MWSN with low storage overhead, low computation overhead and increased probability of detection. This paper studies various techniques for detection of clones in mobile and stationary environment. It also summarizes various parameters to evaluate the detection probability of techniques discussed.**

***Keywords*— Mobile wireless sensor network, clone attack, detection, performance comparison**

I. INTRODUCTION:

Wireless sensor network[1] consist of one or more remote sinks and sensors equipped with sensing devices, actuators to track the environment, temperature, pressure etc. Sensor nodes in wireless environment are resource scarce and are deployed in unattended environment to report about the region of interest. So, we have to use limited energy for computations like tracking to work for longer span of time. To increase the flexibility and capability of sensor nodes we introduce mobility in Sensor nodes.

Mobile Wireless sensor network consist of sensor nodes that are movable in a network. Mobility is achieved in sensor nodes by equipping it with mobilizers for changing their location or sensor are made to move via wheel, robots or vehicles. Recent researchers prove that Mobile wireless sensor network outperform than the stationary sensor networks [2]. Some of the advantages are

1. Lifetime of sensor nodes increases using mobile sensor networks.
2. Reduces energy consumption during communication.
3. MWSN has better channel capacity compared to the stationary sensor networks.

Even though there are several advantages, sensors are kept unattended for long time and they are not equipped with tamper resistant hardware. This arises many types of attacks in MWSN. One of the most dangerous attacks is clone attack. In this attack the adversary node will eavesdrop to a node in a network to get the information's like Identifier, key etc. Once it gets the information from the compromised node it will deploy the replicas of compromised node in the network.

The cloned node has all the credentials of compromised node, so they are considered as legitimate nodes by all other nodes. This will initiate many insider attacks in network and will be difficult to detect. It is not necessary for the adversary to compromise more number of nodes. It is enough to compromise the single node to subvert the behaviour of a network. Many protocols have been proposed to detect the clone attack in stationary sensor networks. But they don't hold in mobile environments which will be explained in later sections.

In this paper, we propose a study of different detection protocols for clone attack. This paper explains the basic detection of clones based on centralized and distributed approach on stationary sensor networks and reasons for not holding in mobile environments. Rest of the paper, discuss about the protocols for the detection of clone in mobile environment.

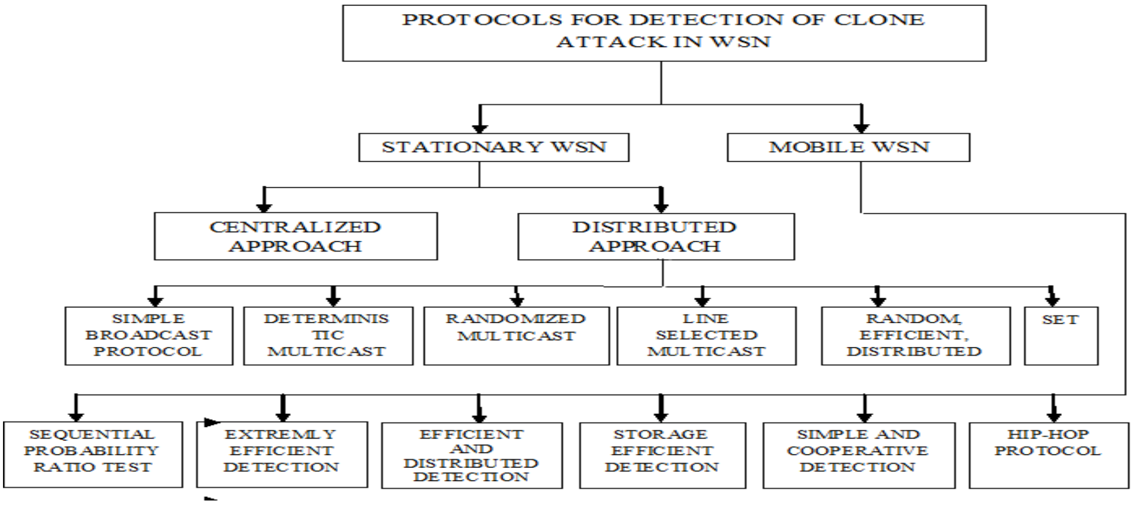
PROTOCOLS FOR DETECTION OF CLONE ATTACK IN WSN
STATIONARY WSN
MOBILE WSN
CENTRALIZED APPROACH
DISTRIBUTED APPROACH
SIMPLE BROADCAST PROTOCOL
DETERMINISTIC MULTICAST
RANDOMIZED MULTICAST
LINE SELECTED MULTICAST
RANDOM, EFFICIENT, DISTRIBUTED
SET
SEQUENTIAL PROBABILITY RATIO TEST
EXTREMLY EFFICIENT DETECTION
EFFICIENT AND DISTRIBUTED DETECTION
STORAGE EFFICIENT DETECTION
SIMPLE AND COOPERATIVE DETECTION
HIP-HOP PROTOCOL

Fig 1: Overview of clone detecting techniques.

II. DETECTION APPROCHES FOR STATIONARY WSN

Clone attacks in wireless sensor networks will initiate many insiders attack like wormhole or black hole attack by changing the code of the compromised node and replicating it in various part of network. The detection of clone is based on the location claims and it is discussed below. There are two different approaches in detecting a clone in detection of clone in Stationary WSN. They are

1. Centralized approach
2. Distributed approach

2.1 *Centralized approach:*

In this approach[19][20], we have a base station (BS) or a remote sink and this initiates the protocol for detection of clone. All the sensor nodes of the network will report the BS about their location information. And the BS will compare the location claims it has received for finding conflicts. If there exist, two nodes with different location claims then BS will broadcast the revoke message for the entire network.

The drawbacks [3] of this approach are

- If the BS is drained out of energy, then detection can't be preceded. This will make detection protocol to fail. This is referred as single point failure.
- If the adversary compromises the BS, then the clones will not be detected.
- The nodes closest to the BS will have a high routing load. Based on this, if the adversary targets these highly loaded nodes then the detection will fail.
- The BS waits for all sensors to report and then analyse them to find the conflicting claims. Then floods the network which increases the storage and computation overhead at BS.

2.2 *Distributed Approach:*

This approach doesn't depend on Base station. The detection of clone is distributed among the sensor nodes in network. The drawbacks of the previous approach are overcome by this distributed approach. There are different protocols that are discussed below under this category.

A) Node-to network broadcasting

In this protocol [5][18], each node in network will broadcast an authenticated message to flood the network with its location claim. Assume that every node receives the broadcast. Every node stores the location claim in the local storage. If it receives a conflicting claim, revokes the offending node. Considering the efficiency, sensor node has to store the location claim of d neighbours. Each node has to send its location claim to all n nodes in network. Thus the total communication cost is O (n^2). Even though, the protocol is simple it will justifiable only in small networks. If scalability increases, the communication cost will be too costly.

B) Deterministic Multicast (DM)

To reduce the communication overhead incurred in the previous detection strategy, we share the location claim only to a pre determined subset of nodes referred as witness nodes. When a node broadcast its claim to its neighbours it will forward it to witness node alone. If the adversary replicates a node [5][20], the witness will receive to conflicting location claims for same node ID. This conflicting claim acts as an evidence to trigger the revocation procedure.

This method reduces the number of messages broadcasted than the previous technique. The drawback is, the adversary can find out the witness node easily and compromise it. This will reduce the detection probability.

C) Random Multicast (RM)

This technique [5][19] overcomes the cons in previous technique by selecting the witness randomly using probability model. Each node signs and broadcast the location claim to its neighbours. This claim in turn forwarded to the randomly selected witness node. The adversary doesn’t know the witness node in prior. So, detection probability is not affected. Every neighbour sends the location claim to O (√n) randomly chosen witness, then exploiting birthday paradox, at least one node will receive the location claim to detect the clones.

This method increases the communication cost. Each node is sending the claim to O (√n) destinations and this increases the total communication cost to O (n). If adversary finds the probability model for finding witness node, then it will compromise those witnesses and clones go undetected.

D) Line Selected Multicast (LSM)

LSM protocol [2] [5] makes use of routing topology for the detection of clones in network. Here, each node signs the location claim and forwards it to the neighbours. On receiving the claim, it is forwarded to the destination chosen as witness. The forwarding nodes also save the location claim and checks for the same ID in its local storage. If conflicts present, then it is broadcasted to the entire network. So, the forwarding node also acts as the witness node.

This increases the detection probability compared to the RM. It needs only O (√n) hops for each node. This will increase the computational overhead by getting signed and verified by each relay nodes.

E) SET protocol

SET protocol [4] is proposed to detect clones in network. It has five components for detection process and they are listed below. First step is to form an exclusive subset maximal independent set (ESMIS) which forms the exclusive subsets in distributed environment. Second, is to ensure security in the subsets construction with compromised nodes. Third, is to form multiple tree based subset computation for the detection of clone and number of trees constructed in network is represented as T. In this approach, each leaf node in tree will check and verify the conflicts. If conflicting location claim arises, it will be informed to the parent node and that node will in turn check, verify and inform to its parent node and this goes on till it reach the root node. But if a clone node is present nearby the root, it may allow the clone to go undetected.

This drawback is handled by forming multiple roots on every exclusive subset. It reduces the computational overhead because it uses only basic computations like union and intersection. Total message sent in entire network is O (n).

F) Real time detection

Detecting the clone in real time [14] is done by forming fingerprints based on the neighbours through superimposed s-disjunct code. It has two steps. First, generate fingerprint of length $\log_2 M$ where M is the number of neighbouring nodes to form fingerprint. Second, detect clones in network. Each node store its own and neighbours fingerprint. For each message sent, add the fingerprints and this can be verified by legitimate neighbours (w). Along, with this normal message transfer also happens and this is denoted as num. If a clone is deployed in other networks this can be identified by the fingerprint which will be different from the original node.

In this protocol, it collects the preloaded codeword’s from d neighbours and computes the social fingerprints. It also increases the memory overhead by sending the fingerprint along with regular messages.

G) SET protocol

SET protocol [4] is proposed to detect clones in network. It has five components for detection process and they are listed below. First step is to form an exclusive subset maximal independent set (ESMIS) which forms the exclusive subsets in distributed environment. Second, is to ensure security in the subsets construction with compromised nodes. Third, is to form multiple tree based subset computation for the detection of clone and number of trees constructed in network is represented as T. In this approach, each leaf node in tree will check and verify the conflicts. If conflicting location claim arises, it will be informed to the parent node and that node will in turn check, verify and inform to its parent node and this goes on till it reach the root node. But if a clone node is present nearby the root, it may allow the clone to go undetected.

This drawback is handled by forming multiple roots on every exclusive subset. It reduces the computational overhead because it uses only basic computations like union and intersection. Total message sent in entire network is O (n).

H) Real time detection

Detecting the clone in real time [14] is done by forming fingerprints based on the neighbours through superimposed s-disjunct code. It has two steps. First, generate fingerprint of length $\log_2 M$ where M is the number of neighbouring nodes to form fingerprint. Second, detect clones in network. Each node store its own and neighbours fingerprint. For each message sent, add the fingerprints and this can be verified by legitimate neighbours (w). Along, with this normal message transfer also happens and this is denoted as num. If a clone is deployed in other networks this can be identified by the fingerprint which will be different from the original node.

In this protocol, it collects the preloaded codeword’s from d neighbours and computes the social fingerprints. It also increases the memory overhead by sending the fingerprint along with regular messages.

I) Hybrid detection

Hybrid detection [16] is the merging of both centralized and distributed protocols. Large networks are divided into sectors. Each sector has a central node, where each node in sector has to send ID and check it. Central node acts as server to identify the clones. Server node requests the node to send the ID to any node in its sector. That node will return its cryptic information. Server node will cross check the reply by asking the neighbour nodes to verify its correctness.

In this detection protocol, division into sectors increase the difficulty in processing. This in turn increases the computational overhead for detection of node replication.

III. DETECTION OF CLONES IN MOBILE WSN

Detecting the clones in mobile wireless sensor networks increases the difficulty to a higher extent. All the detection techniques discussed above are not suitable for this environment. This is because; the main concept for all the detection techniques is based on the geographic location of sensor nodes. But the nodes that are equipped with mobility, move anywhere in the network.

Nodes have the possibility of being in two different locations within the same protocol run. This will be taken as clone in all the stationary WSN. So, many researchers have proposed protocols for MWSN with different detection probability, energy consumption and memory usage. The proposed techniques are discussed and analysed in detail.

3.1 *Sequential Probability Ratio Test (SPRT)*

In SPRT [10] [17], every time the sensor moves to the new location it signs the claim (location and time) and sends it to its neighbours and to the Base station (BS). BS computes the speed based on the probability ratio test and compares it with the observed speed. If the observed speed is beyond the computed maximum speed then the node is considered to be clone. In this technique, each sensor on average receives b claims. So, each node checks b signature checks. The probability that claim is forwarded to BS is p. The BS verifies b*p*N signature where N is total number of sensor nodes.

The worst case of this technique is generation of false negatives and false positives. False negatives states that, if max speed is considered to me small then a normal node can be considered as clone (falsely). False positives is the vice versa of the previous one. The detection of clone is based on base station and the maximum speed deployed. If the BS fails, detection of clone fails (Single point failure).

3.2 *Extremely Efficient Detection Protocol (XED)*

XED [9][15][17] is based on the concept of Remember and Challenge. It argues that, it doesn’t need to be aware of location information. If two nodes meet each other for the first time they exchange a random number and store it in table. E(x) is the expected number of moves in network by a sensor. On the occasion of meeting for the second time or more, it request for the previous exchange number saved in table. If both have the same number then we decide as no clone otherwise clone is detected.

Two important factors in this technique are

1. Detection is possible only if the nodes have already met each other.
2. Probability that the genuine node is fooled.

This reduces the communication overhead to O (1). The flaw in this technique is false negatives. I.e. an adversary can say that the legitimate node have a wrong number. There is no security mechanism employed to check this situation.

3.3 *Simple and Co-operative Distributed Detection (SDD & CDD)*

SDD [11][17] proposes the idea that each node ‘a’ should keep track of nodes in subset T_a. Consider a node b Є $T_{a,}$ if comes in communication range of ‘a’ then it stores the time‘t’ and set the time that expire after ‘λ’ seconds. If time expires, node ‘a’ floods an alarm to the network to revoke ‘b’. If the time out expires, the network is flooded with an alarm to revoke ‘b’.

When node ‘a’ meets node ‘b’ for the first time, it checks whether it is supposed to trace ‘b’. If b Є $T_{a,}$ ‘a’ will update the information about ‘b’ and resets alarm for node. The Receive procedure will check whether the message is ALARM. If so, it will check the time when it has last received before the Maximum Interval Time (MIT). Then counter is reset to 1. Otherwise, increment count by 1. This is to reduce number of False Positives generated.

The flaws in this technique are to maintain and transfer number of parameters like λ, MIT for each node in network. This increases the computation and storage overhead. Number of ALARM’s for each node is in O(T_a).

CDD [11][17] is proposed to improve Node replication detection using node co-operation. In this technique, consider two nodes ‘a’ and ‘b’. They exchange the information when they meet each other which are common to both nodes and it is represented as Ta∩Tb. If there is a node ‘c’, which is tracked by both nodes a, b they compare the last time they meet the node ‘c’. Assume, node ‘b’ meet node ‘c’ in time t_2 and node ‘a’ meet node ‘c’ in time t_1. Let $t_1 < t_2$, node ‘a’ will update the time with the more recent value.

T_a - Subset of nodes traced by node ‘a’.

T_b- Subset of nodes traced by node ‘b’.

The drawbacks of this technique are maintaining time synchronization between the two nodes. This also creates drift error and skews errors.

3.4 *Efficient and Distributed Detection (EDD)*

EDD [8][15][17] proposes that it determines the threshold for number of meeting between the two nodes in a given time T with higher probability. Replica of node is detected if the node encounter the other node with higher number than the threshold. This setting up of threshold can be done in two ways. One is through offline (Planning before deployment) or in online (In each and every step).

This increases the storage overhead to higher extent. This technique is suitable in sensors if and only if a separate memory module is inserted. Computational overhead is increased in online mode, due to the prior planning before deployment. This technique arises to false positives if threshold is set to low. If threshold is high, this give raise to false negatives. Security is given in the protocol by Selective Silence. Storage overhead incurred can be reduced by the alternative technique named as SEDD. It proposes that each node monitors only the subset of nodes called monitor set.

3.5 *History Information Exchange protocol and Optimized version (HIP & HOP)*

HIP [1] is implemented mainly based on the exchange of information to all the neighbours (d) we meet. Consider there are two clone nodes (c, c') in two different locations. Say, the node ‘a’ meets node ‘c’ and ‘b’ meets ‘c'’. They exchange the location claim (ID, loc, protocol run) with each other. If the nodes ‘a’ and ‘b’ meet each other, they predict that the nodes of same ID is in different location at the same protocol run which means that there exist a clone.

HOP [1] is the optimized version of HIP. In HIP, only the direct neighbours exchange their information. But in HOP, neighbour set of two nodes also exchange their information. Consider for example, node‘d’ has node ‘a’ and ‘b’ in its neighbour set, then they exchange the information and find out the clones even though they are not direct neighbours.

The important factors that play a major role are,

1. Radius of communication (r)
2. Size of the history log (h)

If the clone is not detected within ‘h’ runs of protocol then the detection probability decreases to the greater extent. Because the logs are overwritten after ‘h’ runs.

IV.COMPARISON

Detection Method	Detection Probability	Computation Overhead	Storage Overhead	Communication Overhead

Centralized Approach	Poor	High	O(d) (each node)
			O(n.d) (at BS)
				$O(n\sqrt{n})$

Node to Network Broadcasting	Low	Comparably Low	O(n) (each node)	$O(n^2)$
DM	Comparably High	Average	O(g)	O(g ln g)
RM	Good	Low	$O(\sqrt{n})$	$O(\sqrt{n}.p.g)$ msg/node
LSM	Good	Comparably High	$O(\sqrt{n})$	$O(n\sqrt{n})$
RED	High	Low	O(g.p.d)	$O(g.p.d. \sqrt{n})$
SET protocol	High	High	O(N/T) (at root)	O(N)
Real Time Detection	Good	High	$O(d)+\max(M,w,\log_2 M)$	$O(num. \sqrt{n})$
Hybrid Detection	Poor	High	No Storage	Mobile: Increases for every move
SPRT	Poor	Low	O(N)	$O(b*p*N*\sqrt{n})$
XED	Average	Low	d.E(X)	O(1)
EDD	Average	Online: High Offline: Comparably Low	O(N)	O(1)
SEDD	Average	Online: High Offline: Comparably Low	O(€)	O(1)
SDD & CDD	Low	High	$O(T_a)$	O(1)
HIP & HOP	High	$O(d^3h)$	$O(d^2h + hd)$	$O(d^2h)$

TABLE I Performance Comparison of Clone Detection Techniques

V CONCLUSION

From this survey, we have discussed about various technique to detect the clone attacks in WSN and MWSN. The detection of attack is based on various approaches like centralized and distributed detection. Finally, from the above comparison (Table I) we conclude that the HIP-HOP technique [1] is the best approach to detect clones in MWSN. There are major problems to be noticed on detecting clones in mobile environment. First, every node is in mobile. Basically, all clone detecting techniques are based on geographical area. But in mobile environment, nodes move and have different geographic area at different time. Second, a node is employed to trace the movement of set of nodes. This will consume energy and this is the major drawback in WSN environment. Considering all these factors, HIP-HOP is more efficient in detecting clone attacks in mobile WSN. In future, some of the issues prevailing in this technique can be opened up as new research areas.

REFERENCES

[1] M.conti, R.Di pietro, A.spongnardi, “Clone wars : Distributed detection of clone attacks in mobile WSNs,” *Journal of Computer and System Sciences* (***Elsevier Publications***), In press.

[2] M.Conti, R.DiPietro, L.V.Mancini, A.Mei, “Requirements and open issues in distributed detection of node identity replicas in WSN” , in : *SMC’06, 2006, pp.1468–1473*.

[3] I.F.Akyildiz, W.Su, Y.Sankarasubramaniam, E.Cayirci, “Wireless sensor networks: a survey” , *Int.J.Comput.Telecommun.Netw*. 38 (4) (2002) 393–422.

[4] H.Choi, S.Zhu, T.F.LaPorta, “SET : Detecting node clones in sensor networks” , *in:SecureComm’07, 2007, pp.341–350.*

[5] B.Parno, A.Perrig, V.D.Gligor, “Distributed detection of node replication attacks in sensor networks” , *in:S&P’05, 2005, pp.49–63.*

[6] M.Conti, R.DiPietro, L.V.Mancini, A.Mei, “A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks”, *in:MobiHoc’07, 2007, pp.80–89.*

[7] M.Conti, R.DiPietro, L.Mancini, A.Mei, “Distributed detection of clone attacks in wireless sensor networks”, *IEEETrans. Dependable Secure Comput.8(2011) 685–698.*

[8] B.Zhu, V.G.K.Addada, S.Setia, S.Jajodia, S.Roy, “Efficient distributed detection of node replication attacks in sensor networks”, in*:ACSAC’07, 2007, pp.257–266.*

[9] C.M.Yu, C.S.Lu, S.Y.Kuo, “Mobile sensor network resilient against node replication attacks (poster*)”, in:SECON’08, 2008, pp.597–599.*

[10] J.W.Ho, M.K.Wright, S.K.Das, “Fast detection of replica node attacks in mobile sensor networks using sequential analysis*”, in:INFOCOM2009, 2009, pp.1773–1781.*

[11] M.Conti, R.DiPietro, L.V.Mancini, “Emergent Properties: Detection of the Node-capture Attack in Mobile Wireless Sensor Networks” in: *WiSec’08, 2008, pp.214-219.*

[12] Shahzad , Sajjad Madani, “Distributed Efficient Multi Hop Clustering Protocol for Mobile Sensor Networks” in: *The International Arab Journal of Information Technology, Vol. 8, No. 3, July 2011, pp.302-309.*

[13] L. Eschenauer and V. D. Gligor. “ A key-management scheme for distributed sensor networks”. In *Proceedings of the 9th ACM Conference on Computer and Communications Security (CCS ’02), pages 41–47, 2002.*

[14] Kai Xing , Fang Liu , Xiuzhen Cheng , David H.C. Du. “Real-time Detection of Clone Attacks in Wireless Sensor Networks” . In: *The 28th International Conference on Distributed Computing Systems, 3-10, 2008.*

[15] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu , “Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks”. In: *IEEE Transactions On Information Forensics And Security*, Vol. 8, No. 5, May 2013.

[16] B.Gowtham, S.Sharmila, “Location Traced Hybrid Detection of Node Replication Attack in Mobile Wireless Sensor Network”. In: *International Journal of Computer Applications (0975 – 8887) on Information Processing and Remote Computing* – IPRC, August 2012.

[17] M.H Ansari, V. TabatabaVakily, “Classification and Aanalysis of clone attack detection procedures in mobile wireless sensor networks”. In : *International Journal of Scientific and Research Publications*, Volume 2, Issue 11, ISSN 2250-3153, November 2012.

[18] C. Geetha, Dr.M. Ramakrishnan, “ Detection Of Clone Attacks In Wsns – A Survey”. In : *Asian Journal of Computer and Information Systems (ISSN: 2321 – 5658),* Volume 01– Issue 01, June 2013.

[19] V. Ram Prabha, P . Latha, “An Overview of Replica Node Detection Wireless Sensor Networks”. In *: International Conference on Recent Trends in Computational Methods, Communication and Controls,Proceedings Published in International Journal of Computer Applications(IJCA)*, ICON3C 2012.

[20] Dr. G. Padmavathi , D.Shanmugapriya, “A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks ”. In: *International Journal of Computer Science and Information Security,Vol.4 No. 1&2,2009.*

AUTHORS PROFILE

Priyadharshni R, is doing post graduate in regional centre, Anna university, Madurai. She received her bachelor of engineering from M.A.M college of engineering affiliated by Anna university, Chennai in 2010. Her area of interest are clone attacks, sensor networking, mobility of nodes.

Selva Bharathi R, is doing post graduate in regional centre, Anna university, Madurai. She received her M.Sc Computer science from Periar Maniyammai college of technology for women, Thanjavur in 2011. Her area of interest are sensor networking, Data Aggregation Techniques.

S. Ramesh, Faculty in the Department of Computer Science and Engineering at Anna University Regional Centre, Madurai. Currently pursuing his Ph.D under faculty of Information and Communication Engineering. Completed his B.Tech in Information Technology at Adhiyamman Engineering College, India. Pursued his Master Degree in Information Technology at Anna University, Coimbatore, India. His research interests include Wireless Communication, Network Security, and Optimization Techniques.