Journal of Theoretical and Applied Information Technology
10th June 2014. Vol. 64 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

SWBC - SECURITY IN WIRELESS SENSOR NETWORKS BY BROADCASTING LOCATION CLAIMS

S.MEENATCHI[1], C.NAVANEETHAN[2],N.SIVAKUMAR[3], P.THANAPAL[4], J.PRABHU[5]
[#1#2#5]Assistant Professor (Senior)/SITE School,[#3#4]Assistant Professor(SG)
School of Information Technology & Engineering, VIT University, Vellore.
E-mail: [1]meenatchi.s@vit.ac.in, [2]navaneethan.c@vit.ac.in, [3]nsivakumar@vit.ac.in, [4]thanapal.p@vit.ac.in, [5]j.prabhu@vit.ac.in

ABSTRACT

Secure data transfer in Wireless Sensor Networks (WSN) is a challenge, as there are always chances for intruders to form a clone node to interrupt data packets. The proposed system Security in Wireless Sensor Networks by Broadcasting Location Claims (SWBC) engages with Area Based Clustering Detection (ABCD).ABCD divides the WSN into sub areas by implementing division of angle equally and nodes in the sub area elects a Witness node by using maximum neighbour nodes approach. Witness nodes are selected near to the central node to the transmission within the range. Witness nodes gets the location claims of the source node and central node manages the witness nodes where both central node and witness node identifies the intruder by broadcasting the location claims to all the nodes. By simulation SWBC gives the best security compared to the existing techniques like RED, and LSM. Simulation results enhance lifespan of WSNs, decreases the data traffic, detection of intruder before replication of data packets.

Keywords: *SWBC, WSN, ABCD, Broadcast*

1. INTRODUCTION

Wireless sensor network (WSN) is a highly distributed network of small size, light weighted wireless nodes. In wireless sensor networks, sensor nodes will be deployed in large numbers as shown in fig.[1]. The wireless sensor network is used to monitor the environments. In many applications wireless sensor networks are used in the applications like constant monitoring, military surveillance, flood detection, and in habitat exploration of animals. General working structure of wireless sensor networks are shown in fig.1. The main work of wireless sensor nodes are a) data gathering b) data transmission c) processing data subsystem d) energy supply subsystem. The main usage of wireless sensor networks is to transfer data in a secured manner. But the security is incompatible due to attackers (Clone node).There may be many types of attacks during data transfer like Node replication attacks, Sybil attacks, selective forwarding attacks, rushing and wormhole attacks. This kind of attacks will deploy the network topology, path of data transfer, structure of networks by making an adversary node. In order to reduce the attacks we go for algorithms. But in usage of algorithms there will be much more wastages of memory, computation, and time complexity occurs. There are some security requirements of wireless sensor nodes they are A) the nodes should ever last till the transmission. B) The data packets should be in confident manner. C) The nodes should communicate with each other) Unity should be there during whole transmission of data. By using [1] clustering detection is obtained to detect the node replication attacks by using this method we can also secure broadcasting in satellite without no interception. By [2] we have done study to detect node replication attacks by line mannerism. This method will collide with its witness node(w) to protect from attacks in line manner. It will be in line manner one end the node will be there and at another node witness node will be there so the method is Line Selected Multicast. In [3] this method we discuss RED(Randomised Efficient and Detection) to detect various attacks by fixing time variables and to detect we use a rand method to find the attacks. In [4] we discuss about a method called RSDA(Reputation-based Secure Data Aggregation) in this each node is assign with a keys in a geographic locations. In [9] graph planar routing method is used

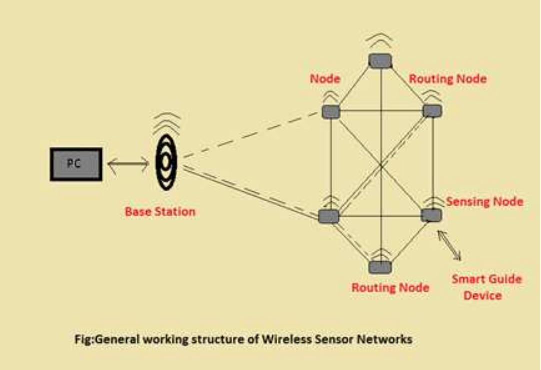


Fig.1 General Working Of Wireless Sensor Networks.

In this paper we have proposed that Area-Based Clustering Detection method is the best method for preventing adversary attacks. Because in this method the entire network is integrated by a root node with it is neighbouring nodes. The root node is selected among the entire networks which have maximum number of neighbouring nodes. Each root node and neighbouring node will have their witness node and intermediate node to store their location claims. By having their own location they will transfer their locations to their root node so the root node will differentiate which are the sub-nodes and which are the adversary nodes. Here we have three different sections, in section [1] we have done our prescribed work, section[2] we have given the comparison between RED, LSM, ABCD, section and evaluated that RED, LSM, ABCD and shown that ABCD method have greater efficiency.[3] we have proposed the efficiency calculation of our RED, LSM, ABCD.

II.OBJECTIVE OF WORK:

In this section we have described about the Location Claims for wireless sensor networks and how the wireless sensor networks is prevented from adversary attacks.

2.1. RED (Randomised Efficient And Distribution):

RED[3] works on centralised broadcasting approach to find the adversary attacks in wireless sensor networks. This method is useful for broadcasting from low level region. Does not useful for high-level data transmission. The entire network divide into fixed time intervals. Entire network is divide into groups to broadcast their locations claims. The groups are divided along their ID and into its locations. If trapping occurs in the network witness node will lose its data of location claims.

Here the neighbouring node is assume to be d and nodes will assume as p. To detect a formula is used:

$$RED = (1-(1-p)^{\wedge}d)^2 \quad [Formula.1]$$

The process of detection is illustrated as below,

The entire networks is divide by its location and when conflict occurs the entire node will send its location claims to its root node. The root node will solve by the formula[1] to detect the adversary nodes. An algorithm is used to detect the trapping process.

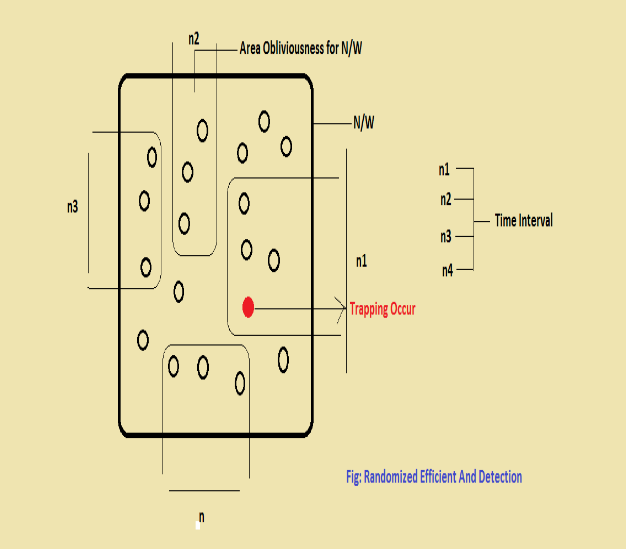

n2
Area Obliviousness for N/W
N/W
n3
n1
n1
n2
n3
n4
Time Interval
Trapping Occur
Fig: Randomized Efficient And Detection
n

Fig:2 RED Method.

2.2. Line Detection Multicast Method:

When a location claim travel from one node to another node, all the intermediate node store the location and virtually form a line across the network. If a conflicting location claim ever crosses the line, then the node at the intersection will detect the conflict as shown in fig.[3]

Location claim from node A to C travel through several intermediate nodes as well. If the intermediate nodes store the location claim then a line is effectively drawn through the network. If a duplicate location claim crosses the line, It is detected and revocation scheme is invoked.

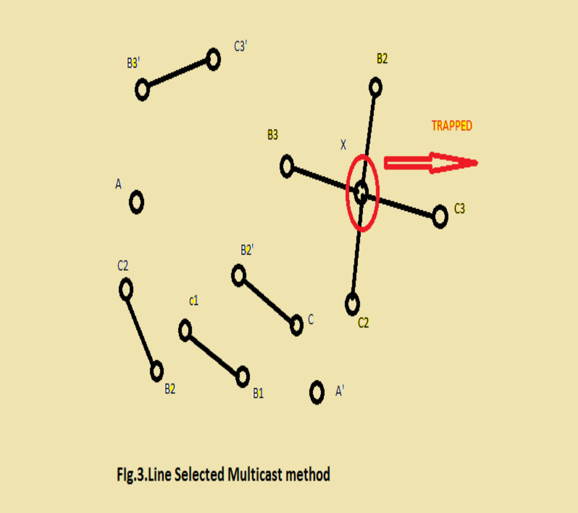


Fig.3Line Selected Multicast Method.

We only need few lines to detect duplicate location claims. Adversary has created a replica A namely as A' Neighbors' Bi and Bi' reports claim to randomly selected witnesses Ci and Ci' and then intersect at X.When A's neighbors' send out location claims to the R witnesses, each node along the root stores a copy of the location claims as well. E.g: Bi stores a copy of the location claim before sending it along the path of nodes X1,X2,X3….Xm to the witness Ci. Each Xk verifies the signature of the claim store the copy in its buffer and forward it along to Xk+1.However before forwarding, it checks if it already has stored a location claim for this node-id before. If it finds a conflict, it floods the network with both the signed location claim La and La'(unforgeable evidence) resulting in revocation of A.

2.3.Area-Based Clustering Detection:

In ABCD [1] method is working by the use of location claims. In every wireless sensor networks they will have some nodes. Each node will have some data to transfer to its own base station. Consider the fig.[4]

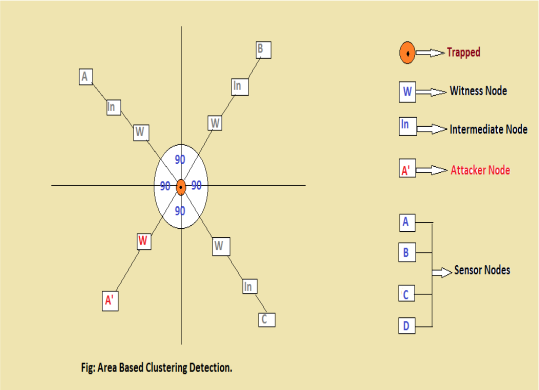


Fig.4area-Based Clustering Detection.

Here the nodes are divided into groups and sub-groups by selecting a central node on the network. The central node is divided on it maximum neighbour nodes approach. After dividing the networks it is differentiate by angles of 90˚ or 120˚ of equal sectors. The entire network area is divided equally around the central nodes to assign a witness node for each sector. The sub groups will have an intermediate node [In] and witness node[w]. The intermediate node is used for transfer of data between root node and neighbouring nodes. The witness node will store the location claims of their node and witness node will also transmit the locations to root node. The witness node is also useful to send conflict detection message. Consider attackers node be A' during data transmission to interrupt the process the adversary node will send a packet to the network. At that time the root node will sense two nodes coming with same data name. So here trapping occurs in the wireless sensor networks. The trapping is same as congestion and flooding but not the relevant process. The similarity is they interrupt the transmission of data packets.

3. OCCURRENCE OF PROBLEM AND SOLUTION FOR RESOLVING THE ATTACKS:

The A node sends it location claim data to neighbouring nodes. As we have discussed earlier witness node which stores the data of location claims sends the data to neighbouring nodes. (via. Intermediate node). Now A'(Adversary nodes or Attackers nodes) will send their data to corrupted the transmission. Now conflicting occurs in the whole network. So now witness node will pass a error syllogism message to entire network. Then witness node also cannot find where the trapping occurs and then it will collect all the data of location claims of all nodes send the entire data to root node. Now the entire location claims is collect by root node and it will sense where trapping occur and repels that adversary nodes.

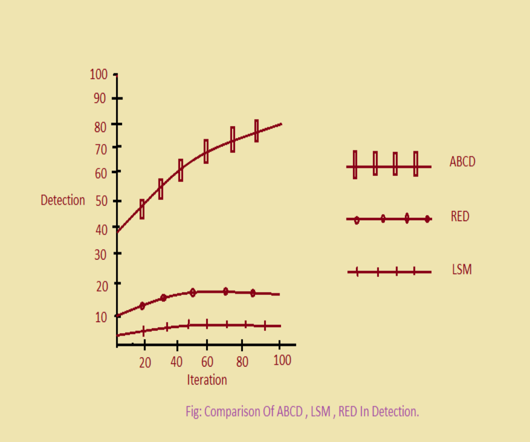
4. PERFORMANCE EVALUATION OF ABCD:

Area-Based Clustering Detection is evaluated using Qualnet6.0. These have many simulation setup to do the process. The nodes will divided into 20,40,60,80 and 100. The entire network is divided into groups and sub-groups of each 90˚. The sensor nodes will be set in 0.0004 per square meter. Each sensor node will have location claims that is consider as size of data packet and the size of data packet will 512 bits. In Qualnet it is repeated every 60 seconds this steps. By repeating this step the

entire wireless sensor networks will be benefits like:
i) The communication overhead is reduced.
ii) Successful detection of adversary attacks.
iii) Number of location claim data stored in sensor nodes is greater than the two methods
In this graph X axis represent the iterations and Y axis represent the Detection probability.

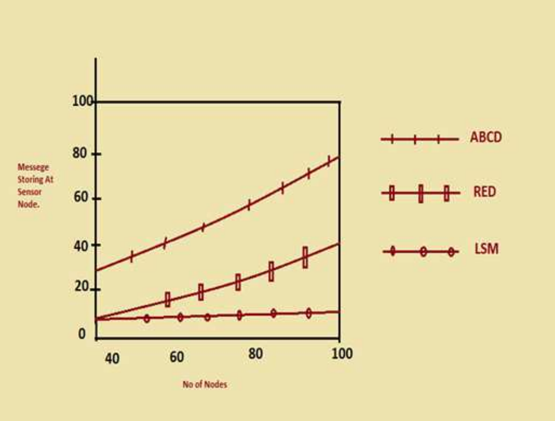
5. COMPARISON BETWEEN THE ABCD, RED, LSM:

Here we are comparing [1] [2] [3] these three methods with some properties like communication overhead, number of message stored in sensor nodes and detection of adversary attacks. For an example consider the three methods ABCD, LSM and RED working on property to show number of message stored in sensor nodes here we are illustrated with an example that is shown in graph.2) as the graph shows that after detection of clone nodes or attackers node the number of message is stored highly in ABCD(Area-Based Clustering Detection). As this example shows that ABCD method is one of the best methods to detect the adversary attacks.

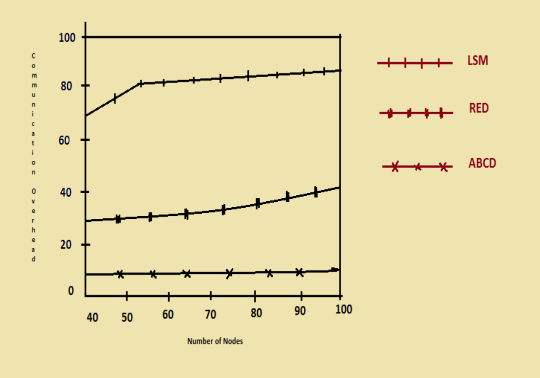


Graph 1.Detection Of Attacks Proability

Then now communication overhead is shown in graph.3) here the communication between the entire network is defined. By defining the nodes communication to communicate with each other data packets there conflict will occurs and the entire data transfer and data packets will be lost. In order to overcome this kind of problems we will simulate with communication overhead. This property also prove that ABCD method have top efficiency. As the three graph shows the properties of communication overhead, detection probability of attackers node and number of location data stored in nodes.



Graph.2.Number Of Message Stored In Sensor Nodes



Graph.3.Communication Overhead.

Now the adversary attacks detection is compared between ABCD, LSM and RED. Here every method will have its own method to detect the attackers but here we have proposed a comparison to predict the best method. As shown in graph.4 The ABCD method will have the great way to detect adversary attacks from every sides. Because it divides the entire network into sub-groups by means of angle. So it protect the data from all the directions and location. So only Area-Based Clustering Detection is called as secure broadcasting by the use of location claims (SWBC).

6. COMPARISON OF ABCD, LSM, AND RED WITH SPECIFICATIONS:

Here we are comparing the methods ABCD with LSM and RED[1] with some specifications to show that our method ABCD has more security for data transfer other than LSM and RED. This table.1 shows working method, applications, execution method, and time probability. The properties like communication overhead. Number of message stored in sensor nodes and detection probability of attackers nodes table.[1]

Table.1 Test On Different Security Claims

Specifications	Area based Clustering Detection	Line Selected Multicast	Randomised Efficient and Detection
Method	Works by dividing the entire networks into equal angles.	Nodes will have their witness node in line manner.	Detects the witness node by rand manner.
Communication Overhead (%)	10%	80%	40%
Number of message stored after detecting adversary attacks (%)	75%	10%	35%
Detection Probability	Very Good	Bad	Good (When Compared to LSM)
Losses in network when trapping occurs	No loss	N/w collapse	Loss of data packets is applicable.
Time Taken	Every 60secs (simulation is repeated)	Whenever it finds conflict only it will start the process.	Long process
Memory Computation	No use of memory	Same as ABCD no use of memory	High use of memory for computations
Steps for executing	Only simulation steps	Simulation steps	Long Algorithm
Applications	Military Surveillances	Simple data transfer	In low level broadcasting

7. EXISTING SYSTEM OF OUR WORK:

The existing system of our work is LSM(Line selected Multicast) in this method the entire network is divide into and the nodes are divided in line manner with their witness node(w). The attackers' node will also collide in line manner to attack the whole network data transmission. But by witnessing the location claims of all nodes the attacker's node will be detected but in LSM there will not be a proper manner to detect the attackers node. Because the entire network is differentiated in line manner but when conflict occurs they combine each other and send their location claims to all root nodes. The disadvantage of LSM is takes much more time and the efficiency will be around 40% to overcome and enhance the clustering nodes by witnessing node using location we proposed a method called ABCD(Area-Based Clustering Detection).

8. CONCLUSION:

Thus by comparing clustering method with another clustering method and clustering method with algorithmic method here we have proposed that ABCD is best method to provide security in wireless sensor networks. Thus the graph.4) shows that Area-Based Clustering Detection has more attacker's detection probability than Line Selected Multicast and Randomised Efficient and Detection. The Detection probability of ABCD is 80%, LSM be around 40% and for RED it will have a efficiency of 60%. Thus our ABCD method will secure network lifetime and protect from communication overhead, number of message stored in sensor nodes, and ensure the detection of attacker nodes with high probability. Our method works in simple manner does not have a long algorithm process to execute and give the result in efficient manner.

REFERENCES:

[1]. Wibhada Naruephiphat, Yusheng Ji and Chalermpol Charnsripinyo, "An Area-Based Approach for Node Replica Detection in Wireless Sensor Networks", 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications.

[2]. Bo Zhu, Sanjeev Setia, Sushil Jajodia, Sankardas Roy and Lingyu Wang, "Localized Multicast: Efficient and Distributed Replica Detection in Large-Scale Sensor Networks", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 7, JULY 2010.

[3]. Conti M, Di Pietro R, Mancini LV, Mei A. "A randomized, efficient,distributed protocol for the detection of node replication attacks in wireless sensor network". In: Proceedings of the 8th ACM international symposium on mobile Ad Hoc networking and computing (MobiHoc'07);2007. p. 80–9, September.

[4]. Hani Alzaid, Ernest Foo and Juan Gonzalez Nieto," RSDA: Reputation-based Secure Data Aggregation in Wireless Sensor Networks", Ninth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2008.

[5]. V Manjula and Dr .C. Chellappan , "The Replication Attack in wireless Sensor Networks: Analysis & Defenses" ,CCIST 2011, Communications in Computer and Information Science, Volume 132, Advances in Networks and Communications, Part II, Pages 169-178, book chapter, Springer –Verlog.

[6]. G. Indirani, Dr. K. Selvakumar and V. Sivagamasundari," Intrusion Detection and Defense Mechanism for Packet Replication Attack over MANET Using Swarm Intelligence", Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22, 2013.

[7]. Bryan Parno, Adrian Perrig and Virgil Gligor," Distributed Detection of Node Replication Attacks in Sensor Networks", Proceedings of the 2005 IEEE Symposium on Security and Privacy.

[8]. M. Conti, R. Di Pietro, L.V. Mancini, A. Mei, "Distributed Detectionof Clone Attacks in Wireless Sensor Networks" Dependable and Secure Computing, IEEE Transactions on vol. 8, Issue: 5, pp. 685 –698, 2011.

[9] H. Frey, M. Hollick, and A. Loch, "Curve-based planar graph routing with guaranteed delivery in multihop wireless networks," in Proc. of IEEE WoWMoM 2012, 2012.

[10]. J. Dinger and H. Hartenstein, "Defending the Sybil attack in P2P networks: Taxonomy, challenges, and a proposal for self-registration," in ARES '06: Proc. of the 1st Int'l Conf. on Availability, Reliability and Security, 2006, pp. 756–763.

[11]Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu and Sy-Yen Kuo,"Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks" IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 5, MAY 2013.

[12]. M. Conti, R. D. Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," IEEE Trans. Depend. Secure Comput, vol. 8, no. 5, pp. 685–698, Sep/Oct. 2012.

[13] C.-M. Yu, Y.-T. Tsou, C.-S. Lu, and S.-Y. Kuo, "Practical and secure multidimensional query framework in tiered sensor networks," IEEE Trans. Inf. Forensics Security, vol. 6, no. 2, pp. 241–255, Jun. 2011.

[14] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "Localized multicast: Efficient and distributed replica detection in large-scale sensor networks," IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913–926, Jul. 2010.

[15] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," IEEE J. Sel. Areas Commun., vol. 28, no. 5, pp. 677–691, Jun. 2010.

[16] A. Le and A. Markopoulou, "On detecting pollution attacks in intersession network coding," in Proc. 2012 IEEE INFOCOM.

[17] A. Le and A. Markopoulou, "Locating Byzantine attackers in intra session network coding using spacemac," in Proc. 2010 International Symposium on Network Coding.