Central-node Based Clone Detection in Mobile Wireless Sensor Networks

J. ANTHONIRAJ

Department of Computer Science, M.I.E.T Arts and Science College, Trichy-620 007, Tamil nadu, India,
antonyrajmiet@gmail.com

Abstract. Clone Attack is the very dangerous attack of all the active attacks of Wireless Sensor Network. In this attack, the adversary capture a sensor node from the network with help of that adversary can create any number clone nodes. Clone nodes are controlled by the adversary, which has all the secret keys. So that clone attack is most harmful threat which is very difficult to detect. In mobile sensor network, the nodes move from one location to another regularly. So it is a complicated task to find the clone nodes which exist in the mobile sensor networks. The proposed Central-node Based Clone Detection(CBCD) protocol detect the clone nodes in efficient manner and within minimum detection time compared with existing EDD and XED protocols. The advantage of proposed CBCD protocol include 1) High clone detection ratio; 2) Minimum communication overhead; 3) Minimum End-to-End delay; 4) Minimum latency time; 5) High throughput so on.

Keywords: Clone Attack, Node deployment, Cluster, Zigbee, Clone detection.

(Received January 1st 2021 / Accepted May 22nd 2021)

1 Introduction

Wireless Sensor Network (WSN) is a distributed independent sensor nodes that are connected together so as to observe different types of environmental or physical conditions. The basic components of a wireless sensor node are processing unit with small amount of memory, sensing unit with sensors, transmission unit with transceivers and a power unit made with batteries. All the wireless sensor nodes are directly linked with the central node called as Base Station. The main applications of Wireless Sensor Network are wild life monitoring, medical applications, traffic control, machine health monitoring, agricultural applications, home automation, military applications and so on[1]. A sensor network is build with a huge number of sensor nodes that are thickly organized in the sensor field. In Wireless Static Sensor Network sensor nodes does not change their position after deployment. In Wireless Mobile Sensor Network nodes change their positions frequently after deployment. Sensor nodes which are installed within the sensor field are always vulnerable to the various attacks done by the adversary. The different causes for the attack are lack of hardware support, minimum computational ability, small amount of memory and storage space, inadequate power resources, lack of security in the wireless communication channels. The various WSN attacks are jamming, tampering, collision, exhausting, wormhole attack, sinkhole attack, flooding, de-synchronization, false data attack, overwhelm attack, sybil attack, clone attack [21, 25]. In Clone attack, an attacker physically holds any one of the sensor node from the sensor network. The captured sensor node remains missing from the network for a particular period of time. In that period attacker removes all the keys of the sensor node. After that the attacker creates clone nodes from the captured sensor nodes. These clone nodes are deployed in the sensor field like other sensor nodes. The clone attack is a very dangerous attack and it will damage entire sensor network within short period of time.

The clone nodes are very similar to the real nodes, so it is very difficult to identify the clone nodes. There

are many clone attack detection protocols to detect the clone nodes in the static WSN. But only very few clone detection protocols are available in mobile WSN. In this work I represent a new detection protocol to find the clone nodes in the mobile Wireless Sensor Network. All the existing clone nodes may be identified in a minimum time span by this protocol.

The literature survey of existing clone detection protocols in wireless mobile sensor network are discussed briefly in section 2. The section 3 represent the proposed system in that, I describe node deployment, network architecture, global positioning system, random way point model, communication standard, routing protocol, key management, encryption method and adversary model. The proposed CBCD protocol description is represent in the section 4. The performance evaluation of the protocol and its results are described in the section 5. The section 6 describes the concluding remarks.

2 Related Work

The Fast Detection method proposed by Ho et al.[9] to find the clone nodes in the sensor network using the sequential hypothesis testing concept. The mobile sensor location and node moves its old location to new location. When it reaches to the new location the neighbors request signed claim. The signed claim contains its location and time information. The neighbors forward the received claim to the base station. The speed of the two received claims is computed by the base station one after another. The base station performs the SPRT in order to find clone nodes. The node replication attacks are detected by New protocol in Mobile Wireless Sensor Networks was proposed by Den et al.[6]. In this protocol, sensor nodes establish pair-wise key for their secure communication between them. The bloom filter collects the total number of pair-wise of the each sensor node. The server of the sensor network calculates the threshold value. The available pair-wise keys in the network go ahead of the threshold value, the node is identified as clone node.

The eXtremely Efficient Detection (XED) protocol was recommended by Yu et al.[2] to deal with the clone node detection in mobile sensor networks. If two nodes exist in the same communication range, each node creates a random number and exchanges it with another node. For some instance the above nodes meet each other the existing random numbers swap between them. If the random number does not match with the existing number, the node is identified as a clone node. Neighbor Based Detection Scheme which is suggested by Ko et al.[15] to sense the clone nodes in Mobile sensor networks. In this protocol, each time the node moves from one location to another it should submit the rejoin request to its new neighbor nodes in order to rejoin the network. The neighbor node one who receives the rejoin request will check the signature and onward to the destination node. The legitimacy of the signature and ID in the neighbor table was verified by the receiving node. The report can be received by the base station from the receiving node.

The Efficient and Distributed Detection scheme was proposed by Yu et al.[33]. In this protocol, sensor node moves according to the random way point. The sensor node selects a location in the network for its movement. Then it moves to the destination point in the sensor network. There it stays inactive for a random amount of time. After that the node moves according to the previous method. During the movement it identifies the clone nodes. Deng et al.[5] has recommended mobility-assisted node replication detection protocol called as Unary Time Location Storage and Exchange protocol. In this protocol, each node initialized with a unique tracking set. Any node in the network is a witness of each node in that tracking set. The node sends a request for asking the neighbor to send a location claim. Many witness nodes receives the location claims in that witness node accepts two time locations for the same ID identified as clone node. Lou et al.[17] created a new protocol to find the clone nodes in the sensor network that is called as Single Hop Detection protocol. The basic idea behind this protocol is the sensor node does not appear in more than one location in different neighborhood community. The one-hop neighbor node list can be used to identify the neighborhood community of a node. All the nodes available in the sensor network correspond with their neighbor nodes. Wang et al.[30] proposed a Patrol Detection for Replica Attack. Each and every zone can be visited by patroller in order to transmit its claim message. Then the immobile nodes will converse with a mobile patroller. The patrol node will find out the clone nodes.

3 Proposed System

To detect clone nodes in Mobile Sensor Network, Central-node Based Clone Detection protocol is proposed. CBCD protocol detects the clone nodes in minimum clone detection time and detects all deployed clone nodes of sensor network. It also uses minimum communication cost than other existing protocols. Various methods that can be used to implement this protocol are described below.

3.1 Node Deployment

In the uniform random deployment, the sensor nodes are randomly deployed in the sensor field without prior knowledge of optimal placement. In this implementation sensor nodes are deployed in the geographical area located at Anna University, Chennai that are shown in the Figure 1.

The deployment of the sensor nodes can be done randomly at any position of the sensor network field .All the WSN applications use the uniform random deployment because it is easy to implement and cost effective [35, 13, 7, 20, 10].

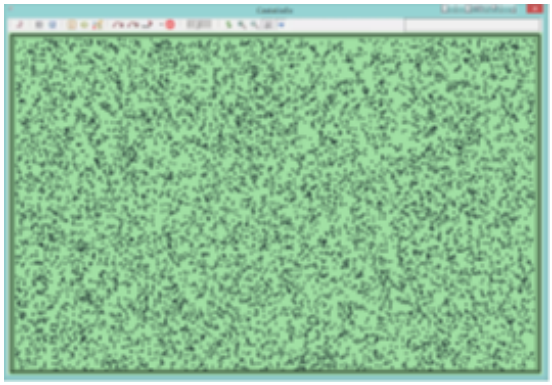

Figure 1: Deployment of 10,000 sensor nodes

3.2 Network Architecture

The Cluster based hierarchical architecture is used in the proposed system. In that, a group of sensor nodes form a cluster, each cluster has a cluster head. Nodes of the network onward the data to the Cluster head. Similar way all the Heads of the cluster onward the data to the central node called as Base station. The Cluster head also exchange the data with its members and base station exchange data with its Cluster heads. The Cluster Heads have more computational capability and large memory space than sensor nodes [23, 4]. In this implementation, all the nodes are deployed in the hierarchical architecture, in that approximately 100 to 500 clusters are formed from the sensor nodes and each cluster has approximately 3 to 50 sensor nodes. The cluster formation of the sensor nodes are shown in the Figure 2. The Legacy algorithm can be used to select the Cluster head of the cluster.

3.3 Global Positioning System (GPS)

The position of the senor node in the sensor network can be identified by the Global Positioning System. In static wireless sensor network sensor nodes are established in

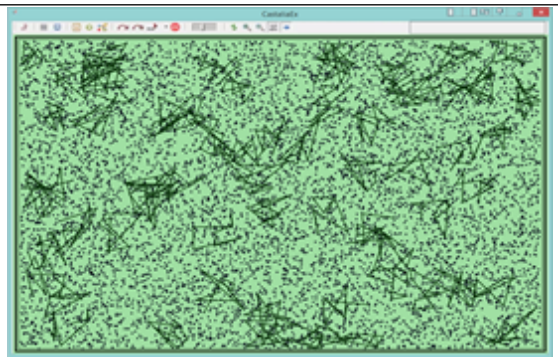

Figure 2: Cluster formation in the Sensor network

the fixed position and cannot alter their position after deployment.

But sensor nodes in the Mobile Sensor Network change their position frequently after deployment [31, 11, 26, 29]. So that establishing localization in the Mobile Sensor Network is a very difficult process. The deployment details of Sensor nodes are given in the Table 1.

Table 1: Deployment Details of Sensor Nodes

Node Id	Latitude	Longitude	Node Type
392	13.014772'N	80.269001'E	Cluster Head
516	13.014644'N	80.259570'E	Node
662	13.012319'N	80.266910'E	Node
388	13.011237'N	80.257172'E	Node
859	13.012197'N	80.220434'E	Node
84	13.013973'N	80.207394'E	Node
356	13.010808'N	80.216980'E	Node
862	13.010017'N	80.259142'E	Node
797	13.011823'N	80.283377'E	Node
2	13.016620'N	80.268276'E	Node

3.4 Random Way Point Model

The Random Way Point model can be used for mobility of sensor nodes in the sensor field. In this method, each node known its geographic position and randomly selects a destination point in the network area.It moves towards the destination point, after reaching the point, the node remains static for a random time.

3.5 Communication Standard

The proposed system uses IEEE 802.15.4 LR-WPAN Zigbee technology for sensor node communication. It is a network which interconnects devices to convey information over short distance among a private group. It

connects a large range of devices into a single network. It supports approximately 65,000 devices on one network. It operates globally in 2.4 GHz band of frequency and 27 channels available with a 20 kpbs transmission bandwidth [28, 8], [27], [19], [24].

3.6 Routing Protocol

For providing the data transfer among the sensor nodes GPSR protocol can be used. In this protocol all the nodes find the geographical position of destination node before transmission. The shortest path between the source and destination can be identified with the help of the location information and the data packets are transmitted in that path[12].

3.7 Key Management

The key exchange between the sensor nodes can be done by Diffee-Helman public key management[22]. In this method, the sender and receiver not known to each other and share a secret key between them through insecure communication channel. The Base station contains the two keys(public and private) before deployment. The Base station sends these keys to the Cluster Head and the sensor nodes. [14, 18, 23].

3.8 Encryption Method

Encryption during the data communication between sensor nodes can be done by Elliptic Curve Cryptography (ECC) Algorithm can be used for encryption. It provides light weight public key cryptography for the Wireless Sensor Network and generates keys through the properties of the elliptic curve equation. In this method, the data encryption can be done by public key and the data decryption can be done by private key [16].

3.9 Adversary Model

Adversary is an entity that attempts to cause harm to the network. First it captures any number of sensor nodes from the network. It can create clones by using cryptographic information. It cannot create a new ID for a clone and establish secure links with their neighbors. It will protect its clones from being detected by detection protocols. Deployment of 50 clones in the sensor field is shown in the Figure 3.

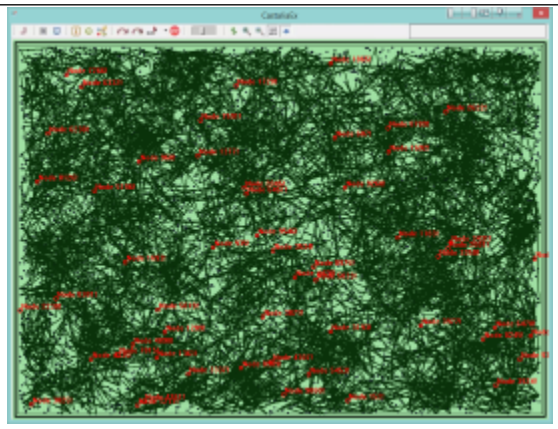

Figure 3: Deployment of Clones in the Sensor network

4 Central-Node Based Clone Detection

The Sensor network is divided into clusters. In mobile wireless sensor networks, sensor node changes its location after deployment. The sensor node moves from one location to another within the cluster. The sensor node also moves from one cluster to another [34, 3]. The entire operation of Central-Node Based Clone Detection is based on the central node (base station) of the network.

4.1 Key Distribution

Before deployment node-ID, location and keys of the nodes and clusters are stored in the base station. The public and private keys are distributed by the base station to the and private keys are distributed by the base station to the cluster heads and sensor nodes.

4.2 Location Information Collection

Each sensor node gathers the position information from all its neighbor nodes and stores the collected information in the neighbor table. The node calculates the finger print with Boolean summation of all its neighbor nodes.

4.3 Node Movement Within The Cluster

The sensor node changes its position from one place to another within the cluster. Before movement, the node informs its neighbor nodes to remove the location information from its neighbor table. After removing the location information from the neighbor table, the neighbor node sends the acknowledgement to the node. After getting the remove-acknowledgement from all neighbor nodes, node goes for the movement.

After that, node makes a request with its cluster head to give the possible locations for its movement. The cluster head verify the node is clone node or not. If it is not a clone node the cluster head sends various locations for its movement. The node chooses any one location for its movement and informs the location details to the cluster head before movement.

The node moves to the new location within the cluster. Then it seeks the readmission from the cluster head for its regular process in the cluster. Cluster head verifies the given node information with the existing information in the cluster table. If the given information matches with existing, the node is accepted. After that the cluster head verifies if it is exists in its old location or not. If it is not available in its old location, then readmission is accepted otherwise it is identified as the clone node.

4.4 Node Movement To Other Cluster

The node moves from its location to some other of other cluster. Before movement, remove its location information in its neighbor nodes. The node sends a request message to the cluster to receive possible locations for its movement.

The Head of the cluster accepts all the requests and forwarded them to the central node called as Base station. The base station contacts with other cluster head and receive the possible locations and return them to the requested cluster head. The node chooses any one of the location and informs the location to the cluster head.

The node moves to the new cluster and seeks the readmission from the new cluster head. The cluster head verifies the node information with help of the base station. Suppose the node already exist in its old location then it is identified as the clone node otherwise readmission accepted.

5 Simulation Results And Performance Evaluation

The proposed CBCD protocol is implemented and tested with Castalia 3.2 simulator that runs on omNet++ platform. This is a standard simulation tool used by many research scholars for their implementation. This tool is suitable one for static and mobile nodes [32]. The experiment has been carried out with the 10,000 sensor nodes deployed in 50m communication range.

5.1 Clone Detection Ratio

The detection ratio refers to the detection of clones in limited time period.

In the available total clone nodes, how many clone nodes are correctly found is called clone detection ratio.

The proposed protocol many times achieves 100% clone detection ratio compares with existing XED and EDD protocols that are given in the Table 2 and Figure 4.

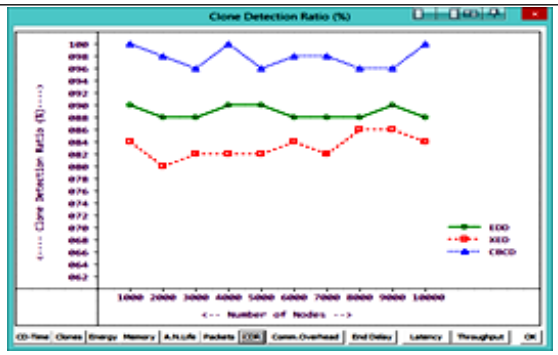

Figure 4: Clone Detection Ratio

Table 2: Clone Detection Ratio

NODES	EDD	XED	CBCD
1000	90	84	100
2000	88	80	98
3000	88	82	96
4000	90	82	100
5000	90	82	96
6000	88	84	98
7000	88	82	98
8000	88	86	96
9000	90	86	96
10000	88	84	100

5.2 Communication Overhead

The communication rate also has plays a vital role in the node performance. The communication overhead of proposed CBCD protocol is compared with existing EDD and XED protocols that are shown in the Table 3 and Figure 5.

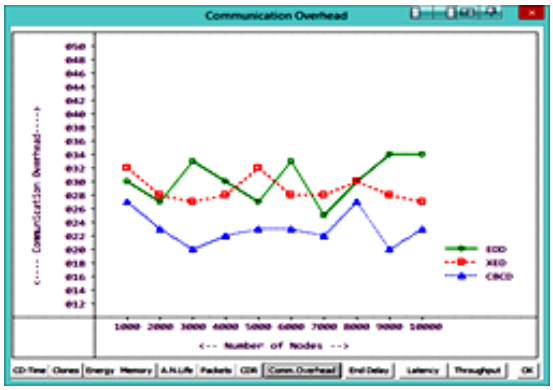

Figure 5: Communication Overhead

The higher communication rates are translated into the ability to achieve the higher effective sampling rates and the lower network power consumption. The sensor

Table 3: Communication Overhead

NODES	EDD	XED	CBCD
1000	30	32	27
2000	27	28	23
3000	33	27	20
4000	30	28	22
5000	27	32	23
6000	33	28	23
7000	25	28	22
8000	30	30	27
9000	34	28	20
10000	34	27	23

Table 4: End-to-End Delay

NODES	EDD	XED	CBCD
1000	268	369	266
2000	256	335	239
3000	282	362	266
4000	301	337	220
5000	271	346	224
6000	281	335	232
7000	292	348	237
8000	272	376	229
9000	269	361	235
10000	291	384	230

nodes send and receive the location claims between the nodes of the network. This process is called as communication overhead.

5.3 End-To- End Delay

The packets always pass through source to destination in the network for that time taken for the nodes in the network, this time is called End-to-End delay. The packet delivery is important for wireless sensor networks, and it should be reliable and scalable.

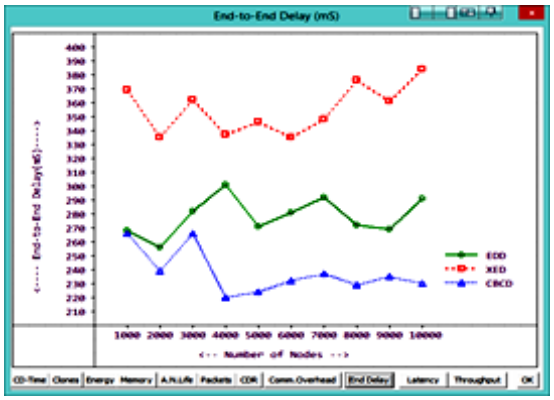

Figure 6: End-to-End delay

End-to-End delay

Transmission Delay+ Propagation Delay + Processing Delay+ Queuing delay

Transmission Delay

N/R

N- Number of bits

R- Rate of transmission

Propagation delay

d/s

d- distance

s- speed of wave propagation

Processing delay

It is the time taken by the routers to process the packet

Queuing delay Total waiting time for a packet in a queue

The proposed CBCD protocol has very minimum end-to-end delay for data transmission than existing EDD and XED protocols that are provided in the Table 4 and Figure 6.

5.4 Latency

The total amount of time taken for a packet to travel from a source to the destination of the wireless sensor network is called latency. The speed and capacity of the sensor network can be defined by the latency and bandwidth.

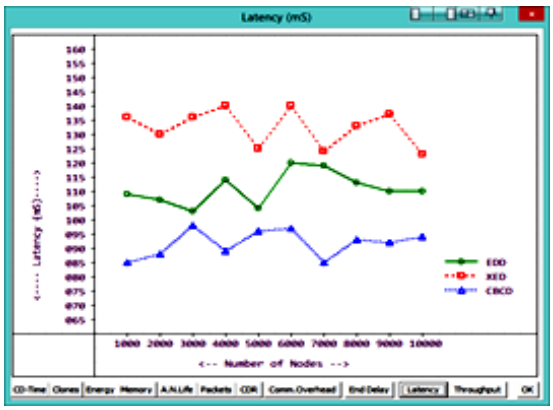

Figure 7: Latency

Latency = d / s

d- distance

s - speed of the medium

Compared with the EDD and XED protocols, the proposed CBCD protocol takes very minimum amount of

Table 5: Latency

NODES	EDD	XED	CBCD
1000	109	136	85
2000	107	130	88
3000	103	136	98
4000	114	140	89
5000	104	125	96
6000	120	140	97
7000	119	124	85
8000	113	133	93
9000	110	137	92
10000	110	123	94

Table 6: Throughput

NODES	EDD	XED	CBCD
1000	68077	56314	73190
2000	67650	57080	73639
3000	68107	56347	73336
4000	67736	56198	73168
5000	68607	56462	72626
6000	68484	56938	73407
7000	67766	57193	73132
8000	68127	56239	73428
9000	67883	56919	72493
10000	68402	56499	73325

time for a packet to travel from source to destination that are shown in the Table 5 and Figure 7.

5.5 Throughput

Total number of messages which are received successfully with a given period of time is called throughput. Issues like bandwidth, signal-to-noise ratio and hardware limitations will be effect the throughput of the network.
Throughput = FS / TR
FS - File Size
TR- Transmission Range

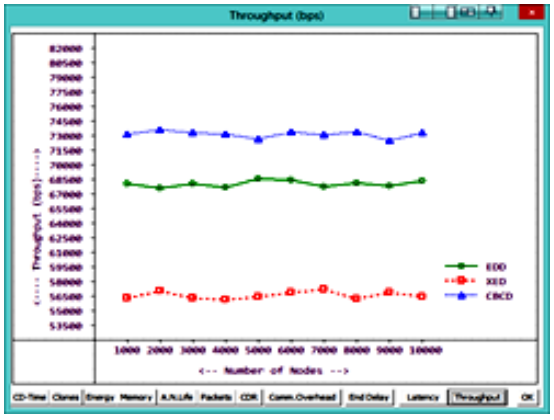

Figure 8: Throughput

The proposed CBCD protocol has the highest hroughput when compared with the existing two protocols EDD and XED that are shown in the Table 6 and Figure 8.

6 Conclusion

In this paper, I propose Central-node Based Clone Detection protocol to find the clone nodes in the wireless mobile sensor networks. This protocol does better than the existing EDD, XED mobile clone detection protocols in following aspects. i) Detect the clone nodes within a short period to avoid the damage, ii) Improve the clone detection ratio and throughput value, iii) Minimize the average memory consumption per node, iv) Minimize communication overhead and latency time, v) Improve the average number of packets transmitted or received per node, vi) The End-to-End delay time may be reduced for transmitting or receiving packets between sensor nodes.

References

[1] Akyildiz, I. F., Su, W., Sankarasubramaniam, Y., and Cayirci, E. A survey on sensor networks. *IEEE Communications magazine*, 40(8):102–114, 2002.

[2] Chia-Mu, Y., Chun-Shien, L., and Sy-Yen, K. Mobile sensor network resilient against node replication attacks. secon'08. In *5th Annual IEEE Communications Society Conference on, vol., no*, pages 597–599, 2008.

[3] Conti, M., Di Pietro, R., Mancini, L., and Mei, A. Distributed detection of clone attacks in wireless sensor networks. *IEEE transactions on dependable and secure computing*, 8(5):685–698, 2010.

[4] Das, A. K. Improving identity-based random key establishment scheme for large-scale hierarchical wireless sensor networks. *IJ Network Security*, 14(1):1–21, 2012.

[5] Deng, X., Xiong, Y., and Chen, D. Mobility-assisted detection of the replication attacks in mobile wireless sensor networks. In *2010 IEEE*

6th International Conference on Wireless and Mobile Computing, Networking and Communications, pages 225–232. IEEE, 2010.

[6] Deng, X.-M. and Xiong, Y. A new protocol for the detection of node replication attacks in mobile wireless sensor networks. *Journal of Computer Science and Technology*, 26(4):732–743, 2011.

[7] Díaz, J., Mitsche, D., and Pérez-Giménez, X. Large connectivity for dynamic random geometric graphs. *IEEE Transactions on Mobile Computing*, 8(6):821–835, 2009.

[8] Gill, K., Yang, S.-H., Yao, F., and Lu, X. A zigbee-based home automation system. *IEEE Transactions on consumer Electronics*, 55(2):422–430, 2009.

[9] Ho, J.-W., Wright, M., and Das, S. K. Fast detection of mobile replica node attacks in wireless sensor networks using sequential hypothesis testing. *IEEE transactions on mobile computing*, 10(6):767–782, 2011.

[10] Howard, A., Matarić, M. J., and Sukhatme, G. S. Mobile sensor network deployment using potential fields: A distributed, scalable solution to the area coverage problem. In *Distributed Autonomous Robotic Systems 5*, pages 299–308. Springer, 2002.

[11] Huang, C.-F. and Tseng, Y.-C. The coverage problem in a wireless sensor network. In *Proceedings of the 2nd ACM International Conference on Wireless Sensor Networks and Applications*, WSNA 03, pages 115–121, New York, NY, USA, 2003. Association for Computing Machinery.

[12] Karp, B. and Kung, H.-T. Gpsr: Greedy perimeter stateless routing for wireless networks. In *Proceedings of the 6th annual international conference on Mobile computing and networking*, pages 243–254, 2000.

[13] Kenniche, H. and Ravelomananana, V. Random geometric graphs as model of wireless sensor networks. In *2010 The 2nd international conference on computer and automation engineering (ICCAE)*, volume 4, pages 103–107. IEEE, 2010.

[14] Kesavan, V. T. and Radhakrishnan, S. Secret key cryptography based security approach for wireless sensor networks. In *2012 International Conference on Recent Advances in Computing and Software Systems*, pages 185–191. IEEE, 2012.

[15] Ko, L.-C., Chen, H.-Y., and Lin, G.-R. A neighbor-based detection scheme for wireless sensor networks against node replication attacks. In *2009 International Conference on Ultra Modern Telecommunications & Workshops*, pages 1–6. IEEE, 2009.

[16] Liu, A. and Ning, P. Tinyecc: A configurable library for elliptic curve cryptography in wireless sensor networks. In *2008 International Conference on Information Processing in Sensor Networks (ipsn 2008)*, pages 245–256. IEEE, 2008.

[17] Lou, Y., Zhang, Y., and Liu, S. Single hop detection of node clone attacks in mobile wireless sensor networks. *Procedia Engineering*, 29:2798–2803, 2012.

[18] Malan, D. J., Welsh, M., and Smith, M. D. A public-key infrastructure for key distribution in tinyos based on elliptic curve cryptography. In *2004 First Annual IEEE Communications Society Conference on Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004.*, pages 71–80. IEEE, 2004.

[19] Mihajlov, B. and Bogdanoski, M. Overview and analysis of the performances of zigbee-based wireless sensor networks. *International Journal of Computer Applications*, 29(12):28–35, 2011.

[20] Norman, J. Connectivity and coverage in hybrid wireless sensor networks using dynamic random geometric graph model. *International journal on applications of graph theory in wireless ad hoc networks and sensor networks*, 3(3):39, 2011.

[21] Padmavathi, G. and Shanmugapriya, M. D. A survey of attacks, security mechanisms and challenges in wireless sensor networks. *IJCSIS IJCSIS IJCSIS IJCSIS*, page 117, 2009.

[22] PATEL, J. S. Security in mobile wireless network with less storage overhead. *INFOCOMP: Journal of Computer Science*, 19(1), 2020.

[23] Pengcheng, Z., Yong, X., and Min, N. A hybrid key management scheme based on clustered wireless sensor networks. *Wireless Sensor Network*, 2012, 2012.

[24] Rana, Y., Nandal, V., Vats, K., and Kumar, R. Ieee 802.15. 4 based investigation and simulation evaluation of zigbee tree and mesh topology using different qos. *International Journal of Computer Science and Mobile Computing*, 6:922–932, 2014.

[25] Sharma, K., Ghose, M., et al. Wireless sensor networks: An overview on its security threats. *IJCA, Special Issue on Mobile Ad–hoc Networks MANETs*, pages 42–45, 2010.

[26] Singh, P., Tripathi, B., and Singh, N. P. Node localization in wireless sensor networks. *International journal of computer science and information technologies*, 2(6):2568–2572, 2011.

[27] Somani, N. A. and Patel, Y. Zigbee: A low power wireless technology for industrial applications. *International Journal of Control Theory and Computer Modelling (IJCTCM)*, 2(3):27–33, 2012.

[28] Srivastava, A. R. Analysis of wireless tactical networks (wtn). *INFOCOMP Journal of Computer Science*, 18(2), 2019.

[29] Wang, G., Guo, L., Duan, H., Liu, L., and Wang, H. Dynamic deployment of wireless sensor networks by biogeography based optimization algorithm. *Journal of Sensor and Actuator Networks*, 1(2):86–96, 2012.

[30] Wang, L.-M. and Shi, Y. Patrol detection for replica attacks on wireless sensor networks. *Sensors*, 11(3):2496–2504, 2011.

[31] Wellenhof, B. H., Lichtenegger, H., and Collins, J. *Global positioning system: theory and practice*. Springer, 1997.

[32] Xian, X., Shi, W., and Huang, H. Comparison of omnet++ and other simulator for wsn simulation. In *2008 3rd IEEE Conference on Industrial Electronics and Applications*, pages 1439–1443. IEEE, 2008.

[33] Yu, C.-M., Lu, C.-S., and Kuo, S.-Y. Efficient and distributed detection of node replication attacks in mobile sensor networks. In *2009 IEEE 70th Vehicular Technology Conference Fall*, pages 1–5. IEEE, 2009.

[34] Yu, C.-M., Tsou, Y.-T., Lu, C.-S., and Kuo, S.-Y. Localized algorithms for detection of node replication attacks in mobile sensor networks. *IEEE transactions on information forensics and security*, 8(5):754–768, 2013.

[35] Zhang, H. and Liu, C. A review on node deployment of wireless sensor network. *International Journal of Computer Science Issues (IJCSI)*, 9(6):378, 2012.