International Journal of Engineering & Technology, 7 (1.2) (2018) 27-32

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

On node reproduction attack in wireless sensor networks

P. Harini *

Professor & HOD, Department of Computer Science and Engineering St. Ann's College of Engineering & Technology, Chirala
**Corresponding author E-mail: mukiriratnaraju001@gmail.com*

Abstract

WSNs (Wireless Sensor Networks) comprise a large number of small, inexpensive, low power and memory constrained sensing devices (called sensor nodes) that are densely deployed to measure a given physical phenomenon. Since WSNs are commonly deployed in a hostile and unattended environment, it is easy for an adversary to physically capture one or more legitimate sensor nodes, re-program and redeploy them in the network. As a result, the adversary becomes able to deploy several identical copies of physically captured nodes in the network in order to perform illegitimate activities. This type of attack is referred to as Node Replication Attack or Clone Node Attack. By launching node replication attack, an adversary can easily get control on the network which consequently is the biggest threat to confidentiality, integrity and availability of data and services. Thus, detection and prevention of node replication attack in WSNs has become an active area of research and to date more than two dozen schemes have been proposed, which address this issue. In this paper, we present a comprehensive review, classification and comparative analysis of twenty five of these schemes which help to detect and/or prevent node replication attack in WSNs.

Keywords: *Wireless Sensor Networks Security; Node Replication; Clone Node Attack.*

1. Introduction

WSNs comprises of set of isolated programmed sorting out sensor hubs with ungainly assets. A sensor hub is typically contains one or more sensors, RF handset, a microcontroller (for performing processing), one or more recollections, a vitality source and actuator. WSNs have many intriguing and coming up applications including military (e.g. war zone administration, checking of gear), environmental control and study (e.g. surge and fire identification), human services, activity control framework, shrewd home/office environments, intuitive amusements and toys, and so forth. In any case, utilization of wireless channel, use in disagreeable, physically perilous and not went to environments have made security of WSNs imperative and testing theme. A portion of the privacy hazards include active and passive eaves dropping, MiTM (Man-in-the-Middle)attack, selective forwarding attack, sinkhole assault, wormholes assault, sybil assault, hub subversion, HELLO surge assault, sniffing assault, dark gap assault, false hub assault, DoS (Denial of Service) assault, and hub generation assault [1]. The concentration of this paper is node reproduction attack, which is also referred as hub cloning assault. In this assault an enemy first physically apprehension at least one right node(s) of the WSN, makes clone hubs of the fear node(s) by duplicating their ID (s), and after that convey them in the system. When enemy prevails with regards to propelling hub multiplication assault, it is conceivable to dispatch numerous progressively a few other dynamic and inactive assaults, for example, interruption, parcel change, Denial of Service assault and particular sending, and so forth [1]. As of late hub multiplication attack has got vital consideration from scientists and more than dozen of plans and conventions [2-29] have been proposed for versatility against hub propagation assault in static and additionally portable WSNs. In this paper, I have analyzed both sorts of techniques and have additionally partitioned and compared them in terms of communication cost, memory cost and type of procedure they use.

The rest of this paper is organized as follows. Section2 is about the thought process and commitment, which depicts the basis, need and the full main contribution of this work. Section3 presents the Coordination and working plan of the methodology proposed to date addressing the issue of node reproduction attack. In section 4, a point by point temporary examination of the greater part of the talked about schemes is presented, and finally section5 concludes the paper.

2. Motive and contribution

A mid a few decades an broad work has been done to recognize and distinguish and moderate the hub reproduction assaults in static as well as mobile WSNs. In order to provide the state-of-the-craftsmanship on hub reproduction assault many research papers [2-4], [26-27] have also been published, each of which has its own problems. For example in [2], Singh, et. Al .have talked about protocols for dealing with hub replication assault just in static WSNs, while in [3], Ansari, et. al. have surveyed node replication resiliency techniques available for portable WSNs as it were. In [4], creators have presented a examination on disseminated protocols tending to the issue of hub replication assault, yet it doesn't give information on incorporated models. To the best of my insight, none of the said reviews have given broad order of the hub reproduction assaults found and anticipation procedures for both static and in addition versatile WSNs and all the above studies are likewise missing probabilistic examination of these models. In this paper, I have filled the hole left by various investigations and show the depiction and arrangement of the 25 models and protocols that have been proposed for found and controlled of node reproduction attacking both static as well as versatile WSNs. Further, a temporary investigation of the grouped models and proto-

cols is additionally done. In addition, this paper also includes probabilistic analysis of 11 protocols. Compactly, this paper will be a guide for those beginner scientists who needs to work for the recognition and counteractive action of hub reproduction assault in WSNs and in addition this paper will be helpful for WSNs application engineers to pick the most appropriate protocol for their application(s) so as to facilitate the vertex reproduction assault.

3. Coordination of node reproduction attacks detection and prevention schemes

Figs. 1-2 demonstrate the coordination of the plans proposed to date for distinguishing, recognizing and relieving hub reproduction assaults in WSNs. These can be ordered into two expansive models: Node reproduction strength plans for static WSNs and for portable WSNs separately. In static sense, WSNs hubs are bolted and they are assumed not to change their area; though in portable WSNs hubs continue adjusting their area. They utilize specially appointed topology where whenever any hub can be included or expelled, and the structure of the system is continue increasing. Encourage grouping is done in each of the above determined sorts as: circulated and incorporated models separately. Conveyed and brought together plans are additionally delegated area ward and area free plans. Brought together plans are straightforward and are first answer for control the hub reproduction assaults. These models thickly rely upon BS (Base Station), which is considered as a capable focal hub. All the information is put away at BS and it is its activity for basic leadership and distinguishing imitated hubs. While disseminated strategies does not rely upon single focal manage or hub. Rather recreated hubs are detected either by neighbor hubs, by haphazardly selected nodes (i.e. witness hubs), or by joined exertion of each point in the system. The plan area subordinate, makes utilization of the physical area of hubs for taking choice about recreated hubs. While area autonomous plans finds recreated hubs without utilizing hubs area data. Each of the subcategory is furthermore separated as restricted plan or entire conveyed plot. The confined models are exceptional type of conveyed frameworks where duplicated vertex are found with join battle of just a single expectation neighbor hubs of resulting hub. While in entire conveyed plots any union of hubs inside a system finds the copy hubs. In consequent subsections start having a place with each of the previously mentioned types are depicted quickly taken after by the relative examination and discussion.

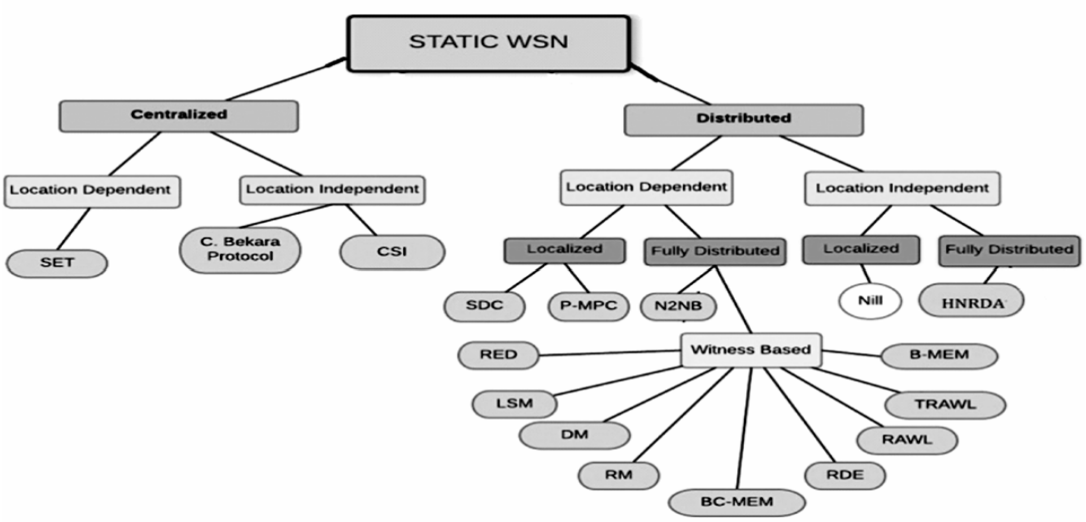

Fig. 1: Arrangement of Node Replication Attack Resiliency Schemes in Static Wsns.

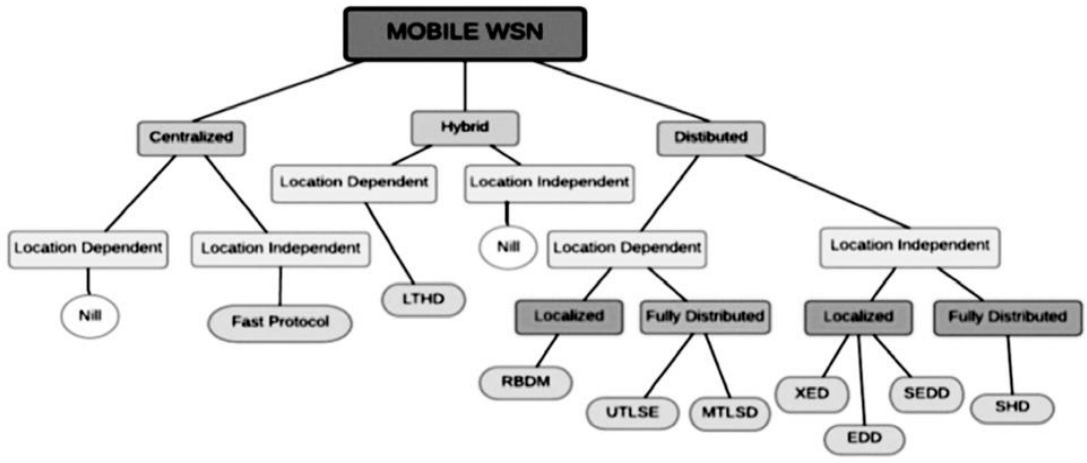

Fig. 2: Arrangement of Node Replication Attack Resiliency Schemes in Mobile Wsns.

3.1. Centralized techniques for detecting node reproduction attacks in static WSNs

SET [5] makes utilization of gathering operations to diminish correspondence issues. It legitimately classifies framework into non-covering sub-locales, hubs in sub-districts shapes selective subsets called groups. Each bunch is comprised of head and part hubs. The sum total of what hubs have been alloted with steady ids. Bunch heads first club list of hub ids in area and sends them to establish of sub-tree in type of subset. Root at that point send their reports to BS and BS recognizes hub reproduction assault by discovering crossing point of any two got reports of sub-trees. The

model proposed by Bekaraet, al. [6] utilizes gather based organization of hubs. Every hub has exceptional ID and it has a place with special age.

The fundamental thought of this protocol is that, when a hub is sent it must have a place with recently conveyed age. Every real hub know the present age. In this manner, when an enemy makes clones of the vertex, cloned vertex have same age id as the first vertex, which causes age conflict to happen and subsequently clone is recognized. In [7], CSI (Compressed Sensing-Based Clone Identification), every hub in the system communicates á (settled number of detected information) to its one expectation neighbor hubs.

Sensor hubs are joined and forward the gotten detected number from their successor hubs along the aggregate tree utilizing compacted detecting based information gathering systems to the Base Station. Base Station at that point reclaimed the steady detected perusing from resultant tree. As per CSI technique node with sensor reading greater than á is cloned one, in light of the fact that correct hub can report a number once.

3.2. Distributed techniques for identifying node reproduction attacks in static WSNs

In [8], N2NB (Node to Network Broadcasting) protocol each node stores location information of all its neighbors and every hub in WSN recordings an approved message along with its localized information after stable time in term. In the event that collector hub gets various area guarantees for one hub it calls a disavowal technique against the sender hub. This procedure is rehashed by each hub in the system that rejects the imitated hub from the system. DM (Deterministic Multicast) protocol is proposed by Parno, et. al. [8], which is an authorized based approach. In DM protocol claimer hub communicates its area information to journalist hub (neighbor hubs) and columnist hub advances the cases to approved hub. Authorized node stores area alongside id. Along these lines, when enemy copies the hub, approved hub gets two distinctive area claims for same hub id and distinguishes the problem (attack). In [8] LSM (Line Select Multicast) protocol, a unique key is used to create digitally signed location-claims for each hub. Hubs at that point send their area cases to chose witnesses. All delegate hubs between sources to goal likewise stores area claim and server the purpose of additional guarantee. Each intermediary node before sending case to next expectation in way coordinates it with as of now put away claims. Two unique cases with same id points to replicated node. After replica detection, a denial move is made against copy hub. RM (Randomize Multicast) [9] protocol is like LSM. The main distinction is, in LSM all middle person hubs, between sender hub and witness hub, are likewise considered as witness and spares area guarantee. While in RM all witnesses are chosen haphazardly. This randomized determination of witnesses make witnesses unpredictable for adversary. RED (Randomized Efficient Distributed) [10-11] protocol works in two steps. In first stage BS communicates an irregular esteem, rand, to every hub in network. In second step, called detection stage, nodes communicate their carefully marked cases to neighbor hubs. Witness hubs are then chosen by neighbor hubs. At the point when witness gets area guarantee it checks whether it is first time getting area assert for this ID, if yes then it stores the claim in separate memory. Then, when next time claim from same node ID is received, witness hubs contrast the got claim and as of now put away area claims, in the event that it discovers two diverse area claim sit invokes revocation method. In RAWL (RAndomWaLk) [12], a hub begins numerous arbitrary strolls in the system and afterward select hubs it has experienced as witness hubs. RAWL protocol has four stages. Initially, hubs communicate their marked area assert. Second, the hub's neighbors forward area claim to some randomly selected nodes. In third step, randomly chosen hubs send the message to begin arbitrary walk, the message contains area assert. In fourth step, if conflicting claims for same ID are received, witness will summon disavowal. TRAWL (Table-Assisted RAndomWaLk) [12] is a variation of RAWL protocol. It works similar to RAWL protocol except that it includes a trace table at each node for recording location claim entries. RDE (Randomly Directed Exploration)[13]protocol is a witness node-based technique. In RDE protocol, during detection phase, nodes broadcast their claim message containing neighbor list to randomly selected neighbors. Previous claim transmission forms a direction, and then the intermediate node tries to follow that direction to forward the message. This protocol is quite simple and consumes less storage during detection. In [14] Znaidi, et. al. have proposed a HNRDA (Hierarchical Node Replication Detection Algorithm), which uses cluster based approach[15]and bloom search to detect replicated nodes in the network. LM (Localized Multicast) [16] protocol randomly selects witness nodes from the nodes located in limited geographic region called cell. The LM approach maps node's ID to one or more cells, and uses randomization within the cells to increase the protection and security of the scheme. This randomization also increases the probability of detecting duplicated nodes. LM approach has two variants called SDC (Single Deterministic Cell) and P-MPC (Parallel Multiple Probabilistic Cells).In [17], Zhang,et.al. Have proposed two variants of memory efficient protocols: (1) B-MEM (Memory Efficient Multicasting Bloom) filters, which uses Bloom filters (memory efficient data structure) and (2) BC-MEM (Memory Efficient MulticastusingBloom filters and Cell) protocol. Note that the detailed description of some of the schemes [14-17] is not presented here due to the paper space limits.

3.3. Centralized techniques for detecting node replication attacks for mobile WSNs

Ho, et. al. [18] have proposed a centralized technique, called Fast Detection of Replica Node Attack in Mobile Sensor networks, which is based on SPRT (Sequential Probability Ratio Test) [19]. This scheme makes use of hub speed and hubs area information. Protocol is formed on fact that the legitimate node should never move at speeds more than the framework arranged most extreme speed. Hence, the legitimate sensor nodes are allowed to move upto speed of maximum system-configured speed. At the other hand, traded off hubs could move at speed more than system-configured speed. If such nodes are founded there is probability of existence of replicated hubs.

3.4. Distributed techniques for detecting node replication attacks for mobile WSNs

In [20-21], creators have proposed a circulated procedure – called XED (Extremely Efficient Detection) for the arrangement of hub replication assaults for portable WSNs. Since determination of witness hub includes high correspondence and vitality overheads, XED does not influence utilization of witness-based to approach. Rather, it utilizes challenge-and-recollect methodology to recognize hub replication attack. Each sensor node has random number generator and has a remarkable ID relegated. At the point when two hubs come in each other's correspondence run, they create irregular numbers and trade them. Traded numbers are then put away in their memory table alongside neighbor's hub ID got arbitrary number and produced irregular number. At the point when the two hubs meet again they again produce and trade RN (Random Numbers). As of now, hubs first pursuit memory table to check accessibility of neighbor hub, if discovered, hubs request to send already traded RN. In the event that sent number matches with the number as of now put away in memory table, hub is checked as verified hub and beforehand produced and got RN are supplanted with currently generated and received RN. In other case, hub is considered as copy hub and a disavowal message for duplicated hub is broadcasted EDD (Efficient Distributed Detection) [20-23] scheme has two stages (disconnected advance and online advance). The disconnected advance is performed before organization of sensor hubs. It manages figuring of interim length and edge of the two hubs met in a specific interim. The online advance is performed by every hub per move. It manages trading

and looking at the messages of various hubs and identifies hub replication assault. Since EDD conspire has high memory overheads, SEDD (Storage-Efficient EDD) [23] has been proposed. SEDD plot works similarly as EDD, however as opposed to breaking down and putting away messages of all hubs of the system, every hub just investigations a subset of the system hubs, called screen set, in a particular time interim. By embracing this approach memory overhead is fundamentally lessened. SHD (Single-Hop Detection) [24], makes utilization of personality based open key framework where every hub stores remarkable private key and an ace open key. The protocol is separated into fc (unique finger impression claim) and unique mark check stages. In fc stage, every hub signs its neighbor hub list. Marked neighbor list is unique mark guarantee fc of its present neighborhood group. fc is then sent to one expectation neighbors. Neighbors in the wake of accepting case confirm unique mark assert and locally store fc. In second stage, when two hubs meet with each other, they trades their witness hub records and perform crossing point. In the event that convergence of the two records is non-unfilled, the two hubs check for fc strife. The two fc with a similar ID and private key guaranteeing two diverse neighborhood groups prompts hub replication. Xiaoming, et. al. [25] have proposed two versatility helped, circulated and area based protocols for distinguishing replicated hubs in portable WSN. The two protocols are UTLSE (Unary Time Location Storage and Exchange) and MTLSD (Multi-Time-Location Storage and Diffusion). The protocols depend on development of hubs in arrange; subsequently they are free of steering protocol and are appropriate for different portable settings. In [26], creators have proposed RBDM (Range-Based Distributed Detection Method) .It is a separation based approach that adventures RSSI (received flag quality sign) to compute the separation between hubs. Ko, et. al. [27] have proposed a scheme that exploits trusted BS. Each node is assigned a unique ID and pair of identity-based public and private keys. Alongside this every hub records ID's of every one of its neighbors in a table called neighbor table. At the point when any hub moves to another area in the system, it communicates rejoining case to new neighbors. All neighbor hubs initially confirm the mark. On the off chance that the mark is confirmed, each neighbor hub communicates rejoining case to haphazardly chose hubs. At the point when goal hub gets rejoining claims, it again approves the mark and checks the hub I ID in its neighbor table. On the off chance that neighbor table does not contain ID, beneficiary hub sends rejoining case to BS for dealing with the issue. Presence of hub's ID in neighbor table demonstrates that the collector hub isn't just new but at the same time is past neighbor of hub I. Recipient hub at that point checks whether hub I is as yet existing in neighborhood by sending one-hope challenging message. If existing claim is gotten, neighbors of hub I move toward becoming observer of replicated attack.

4. Comparative analysis and discussion

4.1. Comparison of node replication attacks in static WSNs

Right off the bat, every incorporated system, for example, SET [5], Bekara's protocol [6] and CSI [7] plans experience the ill effects of one normal issue that these have single purpose of disappointment. Also, SET protocol is very mind boggling because of its five parts (select subset development, validation of subset covering, disseminated set Computation, interleaved verification on subset trees, and evident arbitrary choice). Protocol proposed by Bekara, isn't just fit for detecting replicated node but is also capable of detecting interruption and restoration of key a little while later interim makes it very troublesome for an assailant to prevail with regards to setting up keys in the network. Therefore, assailant can't send duplicated hubs. CSI has most minimal correspondence overhead and most elevated likelihood rate for recognizing reproduction hubs [7]. Rather than brought together schemes, distributed techniques are more reliable. Failure of the BS hub does not crash the whole framework. The circulated protocol N2NB [8] is fit for identifying 100% copied area guarantees by having suspicion that, verified communicate comes to at each hub in network. However, if an adversary jams some key nodes in the system, this presumption won't remain constant and therefore the likelihood of recognizing copy nodes will decrease. The main drawback of N2NB is that ith as significant communication overhead. As compared to N2NB protocol, DM [8] limits preparing/correspondence overheads by choosing a settled number of witnesses, in any case, those settled hubs can be bargained by a foe effectively, subsequently can lose strength against assault. In LSM [8] cloned hub is distinguished at meeting hub of two ways where two diverse area claims are gotten with same ID. In LSM bigger drawn line portion builds likelihood of intersection significantly. But smaller line segments will essentially decrease likelihood of identifying copy hubs. LSM has second most minimal rate (as appeared in Table 2) of recognizing assault being talked about. Further, it has low communication and storage overheads. In RM [9] protocol all witnesses are chosen haphazardly. This randomized determination of witnesses make witnesses unpredictable for adversary. Henceit has high resiliency of identifying imitated hubs, however when contrasted with different systems RM has least likelihood of distinguishing copies among all methods. The RED [10] protocol has higher flexibility of distinguishing imitated hubs when contrasted with LSM and has higher copies location rate than RM, DM and LSM protocols, be that as it may it has high correspondence overheads. In SDC [16] witness hubs are picked arbitrarily from the hubs of a given set rather than the entire system as in the RM protocol. It additionally gives higher strength against hub replication assault and it likewise has great rate of recognizing imitations. P-MPC [16] protocol works same as SDC, yet is more memory effective than SDC and furthermore has better rate of distinguishing duplicated hubs in WSNs. RAWL[12] appropriates obligation of choosing witness hub to each go-between hub go in irregular walk, so for a foe it turns out to be very hard to discover witness hubs. While TRAWL [12] protocol works same as RAWL but as compared to RAWL it significantly reduces memory overheads by making utilization of follow table, where just a passage for a hub is recorded as opposed to putting away area guarantee. Be that as it may, the two protocols have high rate of distinguishing copy hubs. Table 2 indicates correlation of the talked about protocols and plans as far as utilized approach, nature of strategy (concentrated versus distributed) along with communication cost and memory cost. Note that table 1 contains rundown of documentations utilized as a part of Tables2-3.

Table 1: Notations Used in Tables 2-3

n	Number of Nodes in the Network	r	Communication Radius
g	Number of Witnesses Selected by each Neighbor	n	Number of Cluster Heads
s	Number of Nodes in a Cell	k	Average Number of Line Segments for each Claim
a	The Node Sending the Location Claim	t	Size of Location Claim
w	The Number of the Witness Nodes that Store the Local Claim	t’	The Number of Bytes that a Bloom Filter Uses to Record the Membership of an Element

4.2. Comparison of defending node replication attacks schemes in mobile WSNs

There has been done less work for recognizing node replication attacks for mobile WSNs and only few schemes are proposed, while a very few of them are implemented. The protocol proposed in [18] for portable WSNs is a brought together procedure so it experiences the issue of single point of failure. In addition to this, it exploits GPS gadgets which are more costly, in this way it includes high cost. XED [22] is an appropriated strategy and its working is quite simple. The advantage of XED algorithm is that it has low memory and communication over-

heads however in the meantime it has less likelihood of recognizing reproductions in system and it is helpless against savvy assaults [4]. SEDD [23] and EDD [23] are likewise conveyed strategies; they don't depend on area information of hub and the two protocols have less correspondence overheads, however EDD is not efficient solution for large scale networks. Also note that EDD has high computation overhead. RBDM [26], an area autonomous strategy, works well for both small-scale as well as large-scale sensor networks; however its real correspondence and calculation cost is obscure.

Hypothetically RBDM has 100%probabilityfordetectingreplicanodes.Table3shows near examination of different protocols for safeguarding node replication attack in mobile WSN.

Table 2: Comparison of Schemes for Defending Against Node Replication Attack in Static Wsns

Protocols	Approach	Centralized/ Distributed	Communication Cost	Memory Cost
Node to Network Broadcasting	Location-Based		$O(n^2)$	O(1)
Deterministic Multicast			O(glog□n/d)	O(g)
Randomized Multicast			$O(n^2)$	O(□n)
Line Select Multicast	Location-Based + Witness-Based	Distributed	O(n□n)	O(□n)
A Group Based Deployment Protocol by Bakar	(Generation/Group Based)	Centralized	O(□n)	O(1)
Randomized, Efficient Distributed	Location-Based + Witness-Based		O(g.0.dn□n)	O(g.p.d)
Hierachical Node Replication Detection	Cluster Based (Uses Bloom Filer	Distributed	O(n)	-
SET (Set Operations)	Location-Based		O(n)	O(d)
Compressed Sensing Based	Sensed Data Based	Centralized	O(n)	-
Single Deterministic Cell			O(r.□n)+O(s)	O(□)
Parallel Multiple Probabilistic Cell			O(r.□n)+O(s)	O(□)
RandomWalk			O(□nlogn)	O(□nlogn)
Table-Assisted Random Walk			O(□nlogn)	O(1)2
Randomly, Directed Exploration			O(d.n□n)	O(1)
Memory Efficient Multicast			O(k.n.□n)	O(tk+t'k□n')
Memory Efficient Multicasting Used Bloom Filters and Cell Forwarding	Location-Based + Eitness-Based	Distributed	-	O(tk+t'k□n')

Table 3: Comparison of Schemes for Defending Against Node Replication Attack in Mobile Wsns

Protocols	Approach	Centralized/ Distributed	Communication Cost	Memory Cost
Exteremely Efficient Detection Algorithm	Location-Independent, Information Exchange Based		O(1)	O(4.dE[X]
Efficient and Distributed Detection Algorithms	Location-Independent	Distributed	O(1)	-
Fast Protocol	Sequential Probability Ratio Test (Node'ss Speed Based)	Centralized	O(n□n)	O(n)
SEDD	Location-Independent		O(n)	-
Single-Hop Detection	Information Exchange Based		O(□n)	O(□n)
Unary Time Location Storage and Exchange	Location Based		-	-
MTLSD	Location Based		-	-
Range Based Detection Method	Received SingelStrenth Indicator Based		-	-
EDD	Location-Independent	Distributed	O(1)	-

4.3. Probabilistic analysis

Despite the fact that few plans for distinguishing hub reproduction assaults for WSNs have been proposed, yet not every one of them are fit for recognizing 100% imitation hubs in pragmatic manner. So inorder to set the best suitable protocol for a particular WSNs application, it is necessary to know the protocol's likelihood for identifying hub replication assault. Table4 shows probability of detecting replica nodes of 11 protocols. The reason is to provide probabilistic analysis of specific plans and protocols is twofold: right off the bat these are usually utilized and surely understood to detect node replication attacks in WSNs, and secondly study on hub replication assaults does not give adequate probabilistic information for other schemes and protocols. P is Probability, a is Directly Proportional, t is Number of Steps/Walk, Pr is The Probability of Neighbor Decides to Forward the Location Claim, m is Number of Measurements, pn is Probability of Neighbor Decides to Forward the Location Claim, nc is Number of Compromized Nodes, L is Length of Line, Ln is Number of Line Segments, and R is Range.

5. Conclusion

This paper exhibited an overall survey on one of the very crutial security threat– node replication attack– in WSNs. A point by point coordination of the state-of-the-craftsmanship on hub replication assault versatility protocols, plans and algorithms to both static as well as mobile WSNs is introduced. This paper likewise exhibited the near examination of the characterized approaches regarding correspondence cost, memory cost and the method used in these proposed hub replication assault versatility plans. What's more, the probabilistic investigation of the eleven protocols is additionally displayed. We advocate that this paper serves the purpose of complete guide for newbie researchers working in the domain of security of WSNs as well with respect to WSNs application engineers to consolidate the most appropriate reproduction identification methodology to their applications.

Table 4: Various Node Replication Scheme'S Probability of Detecting Replicated Nodes in Wsns

Protocols	Number of Nodes Deployed	Probability (%)	Depending Factor
N2NB	1000	100	-
RM	1000	63	-
LSM	1000	72	(P □ L) and (P □ Ln)
RED	1000	88	-
Hnrda	200-600	90	P □nc
CSI	1000	100	P □ m
SDC	1000	86	P □pr
P-MPC	1000	95	With t=9, P □ (t)
RAWL	1000	95	With t=9, □ P(t)
TRWL	1000	95	With t=9, □ P(t)
RDBM	1000	100	With Range = 6m (P□N) and (P□R)

P is Probability, is DirectlyProportional, t is Number of Steps/Walk, Pris The Probability of Neighbor Decides to Forardthe Location Claim, m is Number of Measurements, pnis Probability of Neighbor Decides to Forward the Location Claim, ncis Number of CompromizedNodes, L is Length of Line, Ln is Number of Line Segments, and R isRange.

References

[1] Padmavathi, G.M.D.S., "A Survey of Attacks, Security Mechanisms and Challenges in Wireless Sensor Networks", International Journal of Computer Science and Information Security, Volume 4, No. 1, 2009.

[2] Singh, M.M., Ankita, S., and Jyotsna, K.M., "Towards Techniques of Detecting Node Replication Attack in Static Wireless Sensor Networks", International Journal ofInformation and Computation Technology, Volume 4, No. 2, 2014.

[3] Ansari, M.H.V.T., "Classification AndAanalysis of Clone Attack Detection Procedures in Mobile Wireless Sensor Networks", International Journal of Scientific and Research Publications, Volume 2, No. 11, 2012.

[4] Sagar, C.J.G.N., "Survey on Distributed Detection of Clone Attacks in Wireless Sensor Networks", 2014.

[5] Choi, H., and Thomas, S.Z., "SET: Detecting Node Clones in Sensor Networks", Proceedings of 3rdInternational Conference on Security and Privacy in Communications Networks and the Workshops- SecureComm, 2007.

[6] Bekara, C., "Defending Against Nodes Replication Attacks on Wireless Sensor Networks", 2012.

[7] Yu, C.M., "CSI: Compressed Sensing-Based Clone Identification in Sensor Networks", Proceedings of 8thIEEE International Workshop on Sensor Networks and Systems for Pervasive Computing, 2012. https://doi.org/10.1109/PerComW.2012.6197497.

[8] Parno, B.J., "Distributed Detection of Node Replication Attacks in Sensor Networks", Master Thesis, 2005.

[9] Bryan, P.A.P, and Gligor, V., "Distributed Detection of Node Replication Attacks in Sensor Networks", IEEE Symposium on Security and Privacy, pp. 49-63, 2005.

[10] Conti, C., "A Randomized, Efficient, and Distributed Protocol for the Detection of Node Replication Attacks in Wireless Sensor Networks", Proceedings of 8thACM International Symposium on Mobile Ad Hoc Networking and Computing, 2007. https://doi.org/10.1145/1288107.1288119.

[11] Conti, M., "Distributed Detection of Clone Attacks in Wireless Sensor Networks", IEEE Transaction on Dependable and Secure Computing, 2011.

[12] Zeng, Y., "Random-Walk Based Approach to Detect CloneAttacksin Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, Volume 28, No. 5, 2010. https://doi.org/10.1109/JSAC.2010.100606.

[13] Li, Z., and Gong, G., "Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks", IEEE 6thInternational Conference onMobileAdHocandSensorSystems, 2009.

[14] Znaidi, W.M.M., and Ubéda, S., "Hierarchical Node Replication Attacks Detection in Wireless Sensor Networks", International Journal of Distributed Sensor Networks, 2013. https://doi.org/10.1155/2013/745069.

[15] Xia, D., and Vlajic, N., "Near-Optimal Node Clustering inWireless sensor Networks for Environment Monitoring", Proceedings of IEEE 21stInternational Conference on Advanced Information Networking and Applications, 2007.

[16] Zhu, B., "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks", Proceedings of IEEE 23rdInternational Conference on Computer Security Applications, 2007. https://doi.org/10.1109/ACSAC.2007.26.

[17] Zhang, M., "Memory Efûcient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks", Proceedings of 17thIEEE International Conference on Neywork Protocols, 2009.

[18] Ho, J.W., "Fast Detection of Replica Node Attacks in Mobile Sensor Networks Using Sequential Analysis", INFOCOM, 2009. https://doi.org/10.1109/INFCOM.2009.5062097.

[19] Abraham, W., "Sequential Tests of Statistical Hypotheses", TheAnnals of Mathematical Statistics, 1945.

[20] Raja, G., "Efficient Detection of Node Replication Attacks in Mobile Sensor Networks", International Journal of Innovative Research in Computer and Communication Engineering, Volume 2, No. 2, 2014.

[21] Balaji, N., and Anitha, M., "Efficient Distributed Detection of Node Replication Attacks in Mobile Sensor Networks", International Journal of Research in Engineering and Technology, 2014.

[22] Yu, C.M., "Mobile Sensor Network Resilient Against Node Replication Attacks", 5th Annual IEEE Communications Society Conference Sensor on Mesh and Ad Hoc Communications and Networks, 2008. https://doi.org/10.1109/SAHCN.2008.82.

[23] Yu, C.M., "Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks", Proceedings of IEEE Conference on Vehicular Technology, 2009. https://doi.org/10.1109/VETECF.2009.5379092.

[24] Loua, Y., "Single Hop Detection of Node Clone Attacks inMobile Wireless Sensor Networks", ProcediaEngineering, Volume 29, 2012.

[25] Deng, X., "Mobility-Assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks", Proceedings of 6thInternational Conference on Wireless and Mobile Computing, Networking and Communications, 2010.

[26] Jian1, H., "A Range-Based Detection Method of Replication Attacks in Wireless Sensor Networks", Proceedings of International Conference on Information and Computer Networks, 2012.

[27] Ko, L.C., "A Neighbor-Based Detection Scheme for Wireless Sensor Networks Against Node Replication Attacks", International Conference on Ultra ModernTelecommunications &Workshops, 2009. https://doi.org/10.1109/ICUMT.2009.5345637.

[28] Khan, W.Z., and Mohammed, Y., "Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey", International Journal of Distributed Sensor Networks, Volume 2013, pp. 22, Article ID 149023,2013.

[29] Khan, W.Z., Saad, M.N.B.M., Mohammed, Y., "Scrutinising Well-Known Countermeasures Against Clone Node Attack in Mobile Wireless Sensor Networks", International Journal of Grid and Utility Computing, Volume4,No.2,pp.119-127, 2013. https://doi.org/10.1504/IJGUC.2013.056247.