On Node Replication Attack in Wireless Sensor Networks

MUMTAZ QABULIO*, YASIR ARFAT MALKANI*, AND AYAZ AHMED KEERIO*

RECEIVED ON 15.01.2015 ACCEPTED ON 28.05.2015

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 re-deploy 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.

Key Words: Wireless Sensor Networks Security, Node Replication, Clone Node Attack.

1. INTRODUCTION

WSNs are collection of independent self organizing sensor nodes with constrained resources. A sensor node is typically consist of one or more sensors, RF transceiver, a microcontroller (for performing processing), one or more memories, an energy source and actuator. WSNs have many attractive and emerging applications including military (e.g. battle field management, monitoring of equipment), environmental control and monitoring (e.g. flood and fire detection), health care, traffic control system, smart home/office environments, interactive games and toys, etc. However, use of wireless channel, broadcast nature of transmission medium and their deployment in hostile, physically unprotected and unattended environments have made security of WSNs very critical and challenging issue. Some of the security threats include active and passive eavesdropping, MiTM (Man-in-the-Middle) attack, selective forwarding attack, sinkhole attack, wormholes attack, sybil attack, node subversion, HELLO flood attack, sniffing attack, black hole attack, false node attack, DoS (Denial of Service) attack, and node replication attack [1]. The focus of this paper is node replication attack, which is also referred as clone node attack in the literature. In this type of attack

* Institute of Mathematics & Computer Science, University of Sindh, Jamshoro.

an adversary first physically captures one or more legitimate node(s) of the WSN, creates clone nodes of the captured node(s) by copying their ID(s), and then deploy them in the network. Once adversary succeeds in launching node replication attack, it is possible to launch several other active and passive attacks, such as intrusion, packet modification, DoS attack and selective forwarding, etc [1]. Recently node replication attack has got significant attention from researchers and more than two dozen schemes and protocols [2-29] have been proposed for resiliency against node replication attack in static as well as mobile WSNs. In this paper, we have surveyed both types of approaches and have also classified and compared them in terms of communication cost, memory cost and type of approach they use.

The rest of this paper is organized as follows. Section 2 is the motivation and contribution, which describes the justification, need and the main contribution of this piece of work. Section 3 presents the classification and working mechanism of the approaches proposed to date addressing the issue of node replication attack. In section 4, a detailed comparative analysis of all of the discussed schemes is presented, and finally section 5 concludes the paper.

2. MOTIVATION AND CONTRIBUTION

During the last decade extensive work has been done to detect and mitigate the node replication attacks in static as well as mobile WSNs. In order to provide the state-of-the-art on node replication attack several survey papers [2-4, 26-27] have also been published, each of which has its own trade-offs. For example in [2], Singh, et. al. have discussed protocols for handling node replication attack in static WSNs only, while in [3], Ansari, et. al. have surveyed node replication resiliency techniques available for mobile WSNs only. In [4], authors have presented a survey on distributed protocols addressing the issue of node replication attack, but it lacks discussion on centralized approaches. To the best of our knowledge, none of the mentioned surveys have provided comprehensive classification of the node replication attacks detection and prevention techniques for both static as well as mobile WSNs and prior surveys are also lacking probabilistic analysis of these schemes. In this paper, we have filled the gap left by prior surveys and exhibit the description and classification of the 25 schemes and protocols that have been proposed for detection and prevention of node replication attack in both static as well as mobile WSNs. Further, a comparative study of the classified schemes and protocols is also carried out. In addition, this paper also includes probabilistic analysis of 11 protocols. Succinctly, this paper will be a guide for those newbie researchers who wants to work for the detection and prevention of node replication attack in WSNs as well as this paper will be helpful for WSNs application developers to select the best suited protocol for their application(s) in order to mitigate the node replication attack.

3. CLASSIFICATION OF NODE REPLICATION ATTACKS DETECTION AND PREVENTION SCHEMES

Figs. 1-2 show the classification of the schemes proposed to date for detecting and mitigating node replication attacks in WSNs. These can be classified into two broad categories: Node replication resiliency schemes for static WSNs and for mobile WSNs respectively. In static WSNs nodes are fixed and they are supposed not to change their location; whereas in mobile WSNs nodes keep changing their location. They use ad-hoc topology where any time any node can be added or removed, and the structure of the network is keep changing. Further classification is done in each of

the above mentioned categories as: distributed and centralized schemes respectively. Distributed and centralized schemes are further divided as location dependent and location independent schemes. Centralized schemes are simple and are very first solution to prevent the node replication attacks. These schemes heavily rely on BS (Base Station), which is considered as a powerful central node. All the information is stored at BS and it is responsible for decision making and detecting replicated nodes. Whereas distributed techniques does not rely on single central authority or node. Instead replicated nodes are

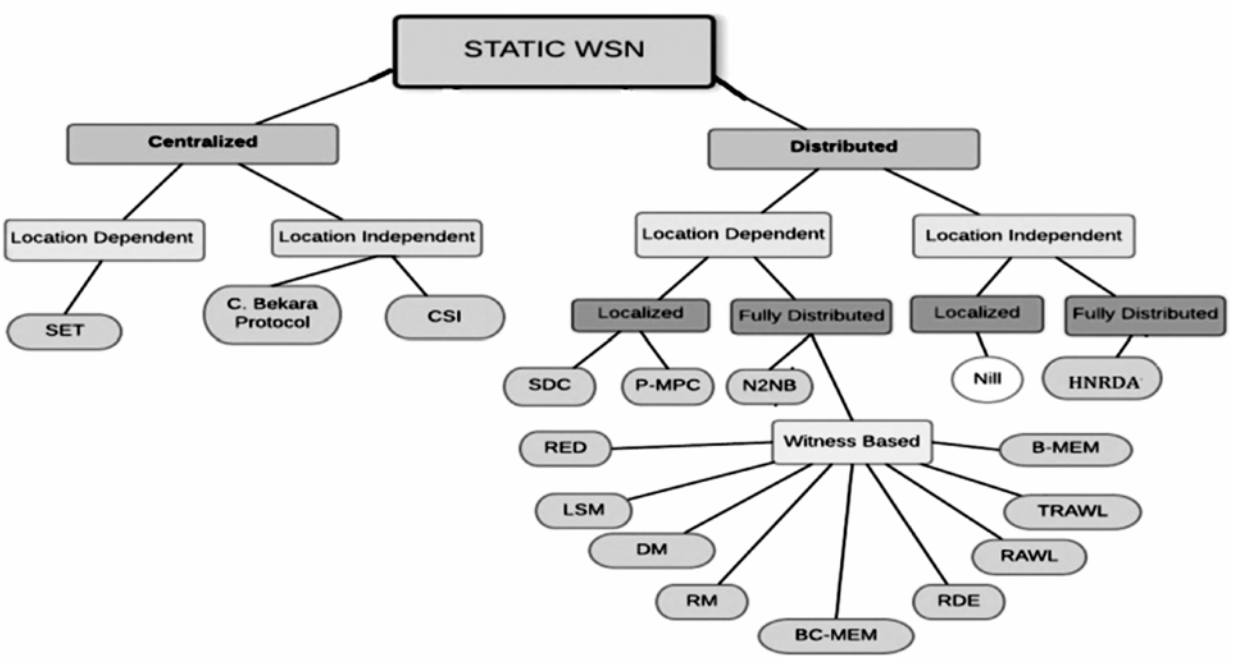

FIG. 1. CLASSIFICATION OF NODE REPLICATION ATTACK RESILIENCY SCHEMES IN STATIC WSNS

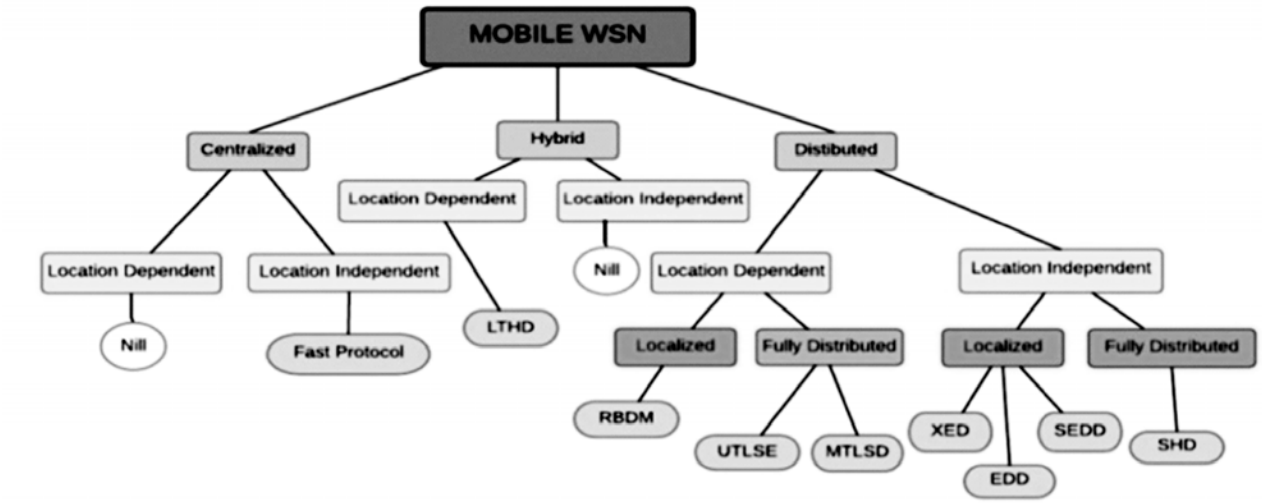

FIG. 2. CLASSIFICATION OF NODE REPLICATION ATTACK RESILIENCY SCHEMES IN MOBILE WSNS

detected either by neighbor nodes, by randomly selected nodes (i.e. witness nodes), or by combined effort of all the nodes in the network. Location dependent schemes, makes use of nodes physical location for taking decision about replicated nodes. While location independent schemes detects replicated nodes without using nodes location information. Each of the subcategory is additionally divided as localized scheme or fully distributed scheme. The localized schemes are special form of distributed schemes where replicated nodes are detected with combine effort of only one hope neighbor nodes of subsequent node. While in fully distributed schemes any combination of nodes within a network detects the replica nodes. In subsequent subsections approaches belonging to each of the above mentioned categories are described briefly followed by the comparative analysis and discussion.

3.1 Centralized Techniques for Detecting Node Replication Attacks in Static WSNs

SET [5] makes use of set operations to reduce communication overheads. It logically divides network into non-overlapping sub-regions, nodes in sub-regions forms exclusive subsets called clusters. Each cluster is consisted of cluster head and member nodes. All nodes are assigned unique ids. Cluster heads first collects list of node ids in region and sends them to root of sub-tree in form of subset. Roots then send their reports to BS and BS detects node replication attack by calculating intersection of any two received reports of sub-trees. The scheme proposed by Bekara et, al. [6] uses group based deployment of nodes. Each node has unique ID and it belongs to unique generation. The basic idea of this protocol is that, when a node is deployed it must belong to newly deployed generation. All legitimate nodes know the current generation. Thus, when an adversary makes clones of the node, cloned nodes have same generation id as the original node, which causes generation conflict to occur and hence clone is detected. In [7], CSI (Compressed Sensing-Based Clone Identification), each node in the network broadcasts á (fixed number of sensed data) to its one hope neighbor nodes. Sensor nodes aggregate and forward the received sensed number from their successor nodes along the aggregation tree using compressed sensing-based data gathering techniques to the BS. BS then retrieves the fixed sensed reading from resultant tree. According to CSI technique node with sensor reading greater than á is cloned one, because genuine node can report a number once.

3.2 Distributed Techniques for Detecting Node Replication Attacks in Static WSNs

In [8], N2NB (Node to Network Broadcasting) protocol each node stores location information of its all neighbors and each node in WSN broadcasts an authenticated message along with its localization information after fixed interval time. If receiver node receives multiple location claims for one node it invokes a revocation method against the sender node. This process is repeated by every node in the network that ultimately excludes the replicated node from the network. DM (Deterministic Multicast) protocol is proposed by Parno, et. al. [8], which is a witness based approach. In DM protocol claimer node broadcasts its location information to reporter node (neighbor nodes) and reporter node forwards claim to witness node. Witness node stores location along with id. Thus, when adversary replicates the node, witness node receives two different location claims for same node id and detects the attack. In [8] LSM (Line Select Multicast) protocol, a unique key is used to create digitally signed location-claims for each

node. Nodes then send their location claims to selected witnesses. All intermediary nodes between sources to destination also stores location claim and server the purpose of additional witnesses. Each intermediary node before forwarding claim to next hope in path matches it with already stored claims. Two different claims with same id points to replicated node. After replica detection, a revocation action is taken against replica node. RM (Randomize Multicast) [9] protocol is similar to LSM. The only difference is, in LSM all intermediary nodes, between sender node and witness node, are also considered as witness and saves location claim. While in RM all witnesses are selected randomly. This randomized selection of witnesses make witnesses unpredictable for adversary. RED (Randomized Efficient Distributed) [10-11] protocol works in two steps. In first step BS broadcasts a random value, rand, to each node in network. In second step, called detection phase, nodes broadcast their digitally signed claims to neighbor nodes. Witness nodes are then selected by neighbor nodes. When witness receives location claim it checks whether it is first time receiving location claim for this ID, if yes then it stores the claim in respective memory. Then, when next time claim from same node ID is received, witness nodes compare the received claim with already stored location claims, if it finds two different location claims it invokes revocation method. In RAWL (RAndom WaLk) [12], a node starts many random walks in the network and then select nodes it has went through as witness nodes. RAWL protocol has four steps. First, nodes broadcast their signed location claim. Second, the node's neighbors forward location claim to some randomly selected nodes. In third step, randomly chosen nodes send the message to start random walk, the message contains location claim. In fourth step, if conflicting claims for same ID are received, witness will invoke revocation. TRAWL (Table-Assisted RAndom WaLk) [12] is a variant of RAWL protocol. It works same as 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 memory during detection. In [14] Znaidi, et. al. have proposed a HNRDA (Hierarchical Node Replication Detection Algorithm), which uses cluster based approach [15] and bloom filter 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 replicated 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 Multicast using Bloom) filters, which uses Bloom filters (memory efficient data structure) and (2) BC-MEM (Memory Efficient Multicast using Bloom 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

node speed and nodes location information. Protocol is formed on fact that the legitimate node should never move at speeds more than the system-configured maximum speed. Hence, the legitimate sensor nodes are allowed to move up to speed of maximum system-configured speed. At the other hand, compromised nodes could move at speed more than system-configured speed. If such nodes are founded there is probability of existence of replicated nodes.

3.4 Distributed Techniques for Detecting Node Replication Attacks for Mobile WSNs

In [20-21], authors have proposed a distributed technique – called XED (Extremely Efficient Detection) – for the solution of node replication attacks for mobile WSNs. Since selection of witness node involves high communication and energy overheads, XED does not make use of witness-based approach. Instead, it uses challenge-and-remember strategy to detect node replication attack. Each sensor node has random number generator and has a unique ID assigned. When two nodes come in each other's communication range, they generate random numbers and exchange them. Exchanged numbers are then stored in their memory table along with neighbor's node ID received random number and generated random number. When both nodes meet again they again generate and exchange RN (Random Numbers). At this time, nodes first search memory table to check availability of neighbor node, if found, nodes ask to send previously exchanged RN. If sent number matches with the number already stored in memory table, node is verified as authenticated node and previously generated and received RN are replaced with currently generated and received RN. In other case, node is considered as replica node and a revocation message for replicated node is broadcasted. EDD (Efficient Distributed Detection) [20-23] scheme has two steps (offline step and online step). The offline step is performed before deployment of sensor nodes. It deals with calculation of interval length and threshold of the two nodes met in a certain interval. The online step is performed by each node per move. It deals with exchanging and comparing the messages of different nodes and detects node replication attack. Since EDD scheme has high memory overheads, SEDD (Storage-Efficient EDD) [23] has been proposed. SEDD scheme works in the same way as EDD, however instead of analyzing and storing messages of all nodes of the network, each node only analyses a subset of the network nodes, called monitor set, in a specific time interval. By adopting this approach memory overhead is significantly reduced. SHD (Single-Hop Detection) [24], makes use of identity-based public key system where each node stores unique private key and a master public key. The protocol is divided into fc (fingerprint claim) and fingerprint verification phases. In fc phase, each node signs its neighbor node list. Signed neighbor list is fingerprint claim fc of its current neighborhood community. fc is then forwarded to one hope neighbors. Neighbors after receiving claim verify fingerprint claim and locally store fc. In second phase, when two nodes meet with each other, they exchanges their witness node lists and perform intersection. If intersection of both lists is non-empty, both nodes check for fc conflict. The two fc with the same ID and private key claiming two different neighborhood communities leads to node replication. Xiaoming, et. al. [25] have proposed two mobility assisted, distributed and location based protocols for detecting replicatd nodes in mobile WSN. The two protocols are UTLSE (Unary Time Location Storage and Exchange) and MTLSD (Multi-Time-Location Storage & Diffusion). The protocols are based on movement of nodes in network; hence they are

independent of routing protocol and are suitable for various mobile settings. In [26], authors have proposed RBDM (Range-Based Distributed Detection Method) . It is a distance based approach that exploits RSSI (received signal strength indication) to calculate the distance between nodes. 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. Along with this each node records ID's of all its neighbors in a table called neighbor table. When any node moves to another location in the network, it broadcasts rejoining claim to new neighbors. All neighbor nodes first verify the signature. If the signature is verified, each neighbor node broadcasts rejoining claim to randomly selected nodes. When destination node receives rejoining claims, it again validates the signature and checks the node i ID in its neighbor table. If neighbor table does not contain ID, receiver node sends rejoining claim to BS for handling the problem. Existence of node's ID in neighbor table shows that the receiver node is not only new but is also previous neighbor of node i. Receiver node then checks whether node i is still existing in neighborhood by sending one-hope challenging message. If existing claim is received, neighbors of node i become witness of replicated attack.

4. COMPARATIVE ANALYSIS AND DISCUSSION

4.1 Comparison of Node Replication Attacks in Static WSNs

Firstly, all centralized techniques such as SET[5], Bekara's protocol [6] and CSI [7] schemes suffer from one common problem that these have single point of failure. In addition to this, SET protocol is highly complex due to its five components (exclusive subset construction, authentication of subset covering, distributed set Computation, interleaved authentication on subset trees, and verifiable random selection). Protocol proposed by Bekara, is not only capable of detecting replicated node but is also capable of detecting intrusion and renewal of key after a short time interval makes it quite difficult for an attacker to succeed in establishing keys in the network. Consequently, attacker is unable to deploy replicated nodes. CSI has lowest communication overhead and highest probability rate for detecting replica nodes [7]. In contrast to centralized schemes, distributed techniques are more reliable. Failure of the BS node does not crash the entire system. The distributed protocol N2NB [8] is capable of detecting 100% duplicated location claims by having assumption that, authenticated broadcast reaches at every node in network. However, if an adversary jams some key nodes in the network, this assumption will not be holding true and consequently the probability of detecting replica nodes will decrease. The main drawback of N2NB is that it has significant communication overhead. As compared to N2NB protocol, DM [8] minimizes processing/ communication overheads by selecting a fixed number of witnesses, however, those fixed nodes can be compromised by an adversary easily, thus can lose resiliency against attack. In LSM [8] cloned node is detected at intersecting node of two paths where two different location claims are received with same ID. In LSM larger drawn line segment increases probability of intersection significantly. But smaller line segments will significantly reduce probability of detecting replica nodes. LSM has second lowest rate (as shown in Table 2) of detecting attack being discussed. Further, it has low communication and storage overheads. In RM [9] protocol all witnesses are selected randomly. This randomized selection of witnesses make witnesses unpredictable for adversary. Hence it has high resiliency

of detecting replicated nodes, but as compared to other techniques RM has lowest probability of detecting replicas among all techniques. The RED [10] protocol has higher resiliency of detecting replicated nodes as compared to LSM and has higher replicas detection rate than RM, DM and LSM protocols, however it has high communication overheads. In SDC [16] witness nodes are chosen randomly from the nodes of a given set instead of the whole network as in the RM protocol. It also provides higher resiliency against node replication attack and it also has good rate of detecting replicas. P-MPC [16] protocol works same as SDC, but is more memory efficient than SDC and also has better rate of detecting replicated nodes in WSNs. RAWL[12] distributes responsibility of selecting witness node to every intermediary node passed in random walk, so for an adversary it becomes quite difficult to find witness nodes. While TRAWL [12] protocol works same as RAWL but as compared to RAWL it significantly reduces memory overheads by making use of trace table, where only an entry for a node is recorded rather than storing location claim. However, both protocols have high rate of detecting replica nodes. Table 2 shows comparison of the discussed protocols and schemes in terms of used approach, nature of technique (centralized vs. distributed) along with communication cost and memory cost. Note that table 1 contains list of notations used in Tables 2-3.

4.2 Comparison of Defending Node replication Attacks Schemes in Mobile WSNs

There has been done less work for detecting 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 mobile WSNs is a centralized technique so it suffers from the problem of single point of failure. In addition to this, it exploits GPS devices which are more expensive, therefore it involves high cost. XED [22] is a distributed technique and its working is quite simple. The advantage of XED algorithm is that it has low memory and communication overheads but at the same time it has less probability of detecting replicas in network and it is vulnerable to smart attacks [4]. SEDD [23] and EDD [23] are also distributed techniques; they do not rely on location information of node and both protocols have less communication overheads, however EDD is not efficient solution for large-scale networks. Also note that EDD has high computation overhead. RBDM [26], a location independent method, works well for both small-scale as well as large-scale sensor networks, however its actual communication and computation cost is unknown. Theoretically RBDM has 100% probability for detecting replica nodes. Table 3 shows comparative analysis of various protocols for defending node replication attack in mobile WSN.

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

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	Distributed	$O(n^2)$	O(1)
Deterministic Multicast	Location-Based + Witness-Based		O(glog√n/d)	O(g)
Randomized Multicast			$O(n^2)$	O(√n)
Line Select Multicast			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	Distributed	O(g.0.dn√n)	O(g.p.d)
Hierachical Node Replication Detection	Cluster Based (Uses Bloom Filer		O(n)	-
SET (Set Operations)	Location-Based	Centralized	O(n)	O(d)
Compressed Sensing Based	Sensed Data Based		O(n)	-
Single Deterministic Cell	Location-Based + Eitness-Based	Distributed	O(r.√n)+O(s)	O(ω)
Parallel Multiple Probabilistic Cell			O(r.√n)+O(s)	O(ω)
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			-	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	Distributed	O(1)	O(4.dE[X]
Efficient and Distributed Detection Algorithms	Location-Independent		O(1)	-
Fast Protocol	Sequential Probability Ratio Test (Node'ss Speed Based)	Centralized	O(n√n)	O(n)
SEDD	Location-Independent	Distributed	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 Singel Strenth Indicator Based		-	-
EDD	Location-Independent		O(1)	-

4.3 Probabilistic Analysis

Although many schemes for detecting node replication attacks for WSNs have been proposed, but not all of them are capable of detecting 100% replica nodes in practical. Hence in order to select the best suited protocol for a particular WSNs application, it is necessary to know the protocol's probability for detecting node replication attack.

Table 4 shows probability of detecting replica nodes of 11 protocols. The reason to provide probabilistic analysis of these selective schemes and protocols is twofold: firstly these are very commonly used and well known schemes to detect node replication attacks in WSNs, and secondly literature on node replication attacks does not provide 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 Forard 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 presented a comprehensive review on one of the very critical security threat – node replication attack – in WSNs. A detailed classification of the state-of-the-art on node replication attack resiliency protocols, schemes and algorithms for both static as well as mobile WSNs is presented. The paper also presented the comparative analysis of the classified approaches in terms of communication cost, memory cost and the method used

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 α L) and (P α Ln)
RED	1000	88	-
Hnrda	200-600	90	P α nc
CSI	1000	100	P α m
SDC	1000	86	P α pr
P-MPC	1000	95	With t=9, P α (t)
RAWL	1000	95	With t=9, α P(t)
TRWL	1000	95	With t=9, α P(t)
RDBM	1000	100	With Range = 6m (PαN) and (PαR)

P is Probability, α is Directly Proportional, t is Number of Steps/Walk, Pr is The Probability of Neighbor Decides to Forard 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.

in these proposed node replication attack resiliency schemes. In addition to this, the probabilistic analysis of the eleven protocols is also presented. We advocate that this paper serves the purpose of complete guide for newbie researchers working in the domain of security of WSNs as well as for WSNs application developers to incorporate the best suited replica detection strategy to their applications.

ACKNOWLEDGEMENT

The research work presented in this paper is mainly carried out by the first author as part of her M.Phil. research, Institute of Mathematics & Computer Science, University of Sindh, Jamshoro, Pakistan.

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 of Information and Computation Technology, Volume 4, No. 2, 2014.

[3] Ansari, M.H.V.T., "Classification And Aanalysis 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 3rd International 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 8th IEEE International Workshop on Sensor Networks and Systems for Pervasive Computing, 2012.

[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 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing, 2007.

[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 CloneAttacks in Wireless Sensor Networks", IEEE Journal on Selected Areas in Communications, Volume 28, No. 5, 2010.

[13] Li, Z., and Gong, G., "Randomly Directed Exploration: An Efficient Node Clone Detection Protocol in Wireless Sensor Networks", IEEE 6th International Conference on Mobile Ad Hoc and Sensor Systems, 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.

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

[16] Zhu, B., "Efficient Distributed Detection of Node Replication Attacks in Sensor Networks", Proceedings of IEEE 23rd International Conference on Computer Security Applications, 2007.

[17] Zhang, M., "Memory Efûcient Protocols for Detecting Node Replication Attacks in Wireless Sensor Networks", Proceedings of 17th IEEE 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.

[19] Abraham, W., "Sequential Tests of Statistical Hypotheses", The Annals 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.

[23] Yu, C.M., "Efficient and Distributed Detection of Node Replication Attacks in Mobile Sensor Networks", Proceedings of IEEE Conference on Vehicular Technology, 2009.

[24] Loua, Y., "Single Hop Detection of Node Clone Attacks in Mobile Wireless Sensor Networks", Procedia Engineering, Volume 29, 2012.

[25] Deng, X., "Mobility-Assisted Detection of the Replication Attacks in Mobile Wireless Sensor Networks", Proceedings of 6th International 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 Modern Telecommunications & Workshops, 2009.

[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, Volume 4, No. 2, pp. 119-127, 2013.