International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:12, No:10, 2018

An Elaborate Survey on Node Replication Attack in Static Wireless Sensor Networks

N. S. Usha, E. A. Mary Anita

***Abstract*—**Recent innovations in the field of technology led to the use of wireless sensor networks in various applications, which consists of a number of small, very tiny, low-cost, non-tamper proof and resource constrained sensor nodes. These nodes are often distributed and deployed in an unattended environment, so as to collaborate with each other to share data or information. Amidst various applications, wireless sensor network finds a major role in monitoring battle field in military applications. As these non-tamperproof nodes are deployed in an unattended location, they are vulnerable to many security attacks. Amongst many security attacks, the node replication attack seems to be more threatening to the network users. Node Replication attack is caused by an attacker, who catches one true node, duplicates the first certification and cryptographic materials, makes at least one or more copies of the caught node and spots them at certain key positions in the system to screen or disturb the network operations. Preventing the occurrence of such node replication attacks in network is a challenging task. In this survey article, we provide the classification of detection schemes and also explore the various schemes proposed in each category. Also, we compare the various detection schemes against certain evaluation parameters and also its limitations. Finally, we provide some suggestions for carrying out future research work against such attacks.

***Keywords*—**Clone node, data security, detection schemes, node replication attack, wireless sensor networks.

I. Introduction

THE recent innovations in the field of technology have led to the development of small low-cost and non-tamper proof sensor nodes. Usually, the nodes of a wireless sensor network are distributed and deployed in an unattended environment so that they collaborate with each other to share data or information. These networks find a huge application in monitoring military war field/battle surveillance, temperature levels, pollution levels, climate sensing, patient health monitoring, etc. However, the sensor nodes exhibit certain constraints such as small size, low battery power, storage area, computation speed, cost, etc. [1].

As these nodes are freely deployed in an unattended environment, they are vulnerable to many security attacks. Some of the security attacks are Spoofing, Sybil attack, Black hole attack, Node Replication attack, Sinkhole attack, etc. Among them the most challenging and vulnerable is Node Replication attack. In this survey paper, we are going to discuss about the effects of Node Replication attacks in the network.

To make the survey more effective and informative it has been split into 5 sections. Section I gives introduction about Wireless Sensor Networks. Section II concentrates on concepts such as Node replication attacks, how to compromise a node, creation of clone node. Section III defines the effects of replica on security goals and also specifies the various metrics involved in evaluating the performance of replica detection schemes. Section IV discusses the replica detection schemes used for static WSN. Finally, the survey article is concluded with possibilities of eradicating the effects of replicas in Static Wireless Sensor Network.

A. Static vs. Mobile Wireless Sensor Network (WSN)

In static wireless sensor network (SWSN), the position of the sensor nodes are fixed at the time of the deployment and do not change. They rely on fixed routing and flooding schemes for data distribution. In contrast to SWSN, the sensor nodes of mobile wireless sensor network (MWSN) move freely after deployment in the network. They interact with other nodes that are within the range, reposition and organize themselves in the network in order to gather information about the environment. The mobile WSN uses dynamic routing to disseminate data. In view of the above features the Replica Detection schemes of Static WSN varies from Mobile WSN [1].

B. Issues in WSN

There are several issues prevailing in WSN such as cryptography, key management, secure routing, data aggregation and intrusion detection. Among these the most challenging is secure routing as the sensor nodes are mostly deployed in unattended environments where they can be easily captured and compromised by an adversary. One such example is the Battlefield Surveillance area, where the nodes of WSN are mainly used to monitor and tackle the attacks caused by an attacker. As the sensor nodes are non-tamper proof, they can be easily accessed by an adversary, who injects false messages so that the warriors get confounded and reveal their secret locations [19]

Sensor nodes are mainly used for Battlefield Surveillance, to screen weapon or medication carrying, human trafficking and movement of illicit objects in the protected zone [2]. So it is very important to provide security to sensor nodes for performing efficient monitoring and communication in WSN [22].

N.S.Usha is an Associate Professor in Department of Computer Science and Engineering at S.A.Engineering College, also Research Scholar at St. Peter's University, Chennai, India (e-mail: usha@saec.ac.in).

Dr.E.A.Mary Anita is a Professor in Department of Computer Science and Engineering at S.A.Engineering College, Chennai, India (email: maryanita@saec.ac.in).

C. Attacks in Wireless Sensor Network

The unattended nature of the WSN nodes are easily exploited by adversary, which can launch a variety of physical attacks such as signal jamming, node replication attacks, DoS attack, eavesdropping, node outage, sybil attack, worm hole attack, sinkhole attack, etc.

Generally the attack or threat to wireless sensor network usually falls in two main categories namely: layer-dependent attacks and layer-independent attacks.

1. **Layer-dependent attacks:** These types of attacks are application dependent and also use specific functionalities of OSI layers thereby affecting routing, data aggregation, node localization, synchronization of events, etc.
2. **Layer-independent attacks:** These types of attacks are application independent and affect a variety of application in various forms. Some of the attacks that fall in this category are Node replication attacks, Sybil attack, etc.

There may be several attacks witnessed by sensor node, among them we consider the most severe and sensitive physical attack on WSN, namely the Node replication attack. It is also referred to as *Identity attack* or *Clone attack.*

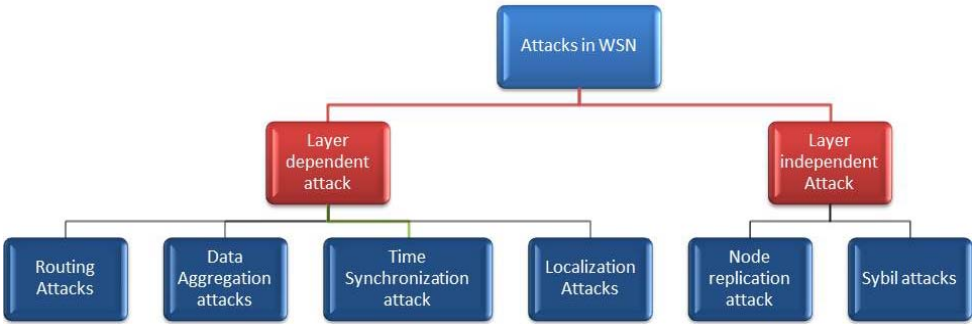

Fig. 1 Layout of Attacks in WSN

II. Node Replication Attack

A. Node Replication Attack in SWSN

Initially the adversary captures a node and copies all the secret credential information's of the node. It then creates one or more clones or replicas of the node with same ID value and deploys these clones at various places/ positions in the network thereby making the network ineffective. It is possible to create clones with single node capture alone. It is mainly due to the fact that sensor nodes are not tamper-proof or shielded.

B. Steps of Node Replication Attack

- The sensor nodes are initially deployed in the environment.
- The adversary captures one or more legitimate nodes deployed in the network.

The adversary extracts all the fabricated, confidential and cryptographic materials from the captured node.

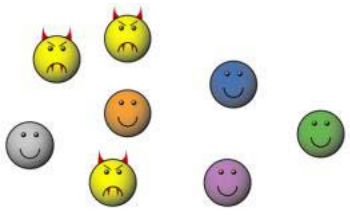

Fig. 2 Node Replication Attack

C. How to Compromise a Node in a Network

There are many ways to compromise a node in a network so as to gain access to critical information and secret keys. The commonly used techniques are 'off the shelf' product and free software which are readily available in the market [2]. A node compromise is defined as a state, when the attackers through some subvert gains control over the node in the network after it has been successfully deployed [5]. Once the attacker gains the control over the node, it can make the node to insert false data, listen traffic flow in the network, use the keys to decrypt data/message, DoS attack, black hole attack, etc. The attacker connects the compromised node to a system and extracts all critical information such as routing protocols, security keys and data for creating a variety of insider attacks. Generally, the sensor nodes are not tamper-proof; they can be easily re-programmed and used for specific purposes. Tampering of nodes requires use of expensive hardware and does not support re-programming. The attacker extracts all credential data located from EEPROM, RAM, SDRAM within < 1 min.

D. What Is a Clone Node?

A clone node contains legitimate information (ID, & cryptographic keys) and can participate in the network operation as same as non-compromised node. It mainly launches a variety of malicious node or insidious attack in the network.

Capabilities of a Clone Node

Normally a clone node can create a black hole, inject false data, initiate a wormhole attack with collaborative adversary, leak sensitive data, and do incorrect aggregation of data so as to bias the final result. If left unattended or uncontrolled they make the network vulnerable to many insidious attacks [4].

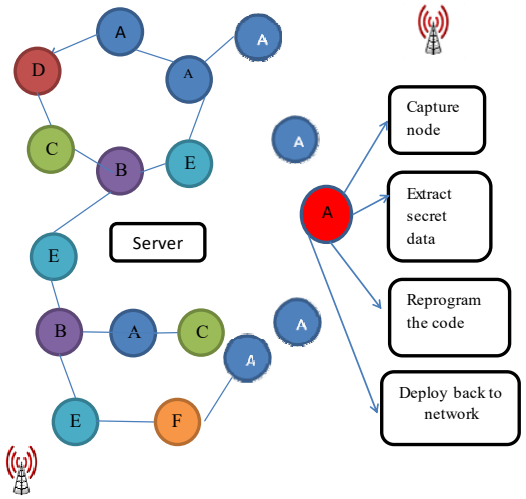

Fig. 3 Steps of Node Replication attack

Characteristics of a Clone Node

i. As created by an adversary, the clones are considered as honest and legitimate node by its neighbors.
ii. Like other nodes, it can participate in the network operation.
iii. It is enough to compromise a single node to create multiple clones.

E. A Powerful Threat Model

The adversary must be capable enough to compromise a single or group of nodes, to create one or more clones or replicas. The adversary takes full control over the compromised node and extracts the ID and cryptographic key materials to create replicas of same ID and place them at intelligent locations defined by it. Since the clone nodes have authenticated information, they also participate in network operations to launch various insider attacks [6].

The adversary also tries to hide the existence of clones from the network by interfering with the detection algorithm. Usually the sensor nodes report their presence at regular intervals. An adversary may drop or manipulate the data sent by other nodes. Moreover the clones collaborate to remove their identifiers from reports [31].

III. Evaluation Metrics for Node Replication Detection Schemes

There are several parameters that are involved in evaluating the performance of various node replication detection schemes. The main parameters include the communication overhead, storage overhead, data security, detection probability, detection time, cost and energy conservation, delivery rate, end-to-end delay, Quality of Service, power usage, packet loss, etc. [2], [10]. They are:

- *Communication overhead*: It is defined as the average number of messages sent by the nodes to verify the location claims.
- *Storage overhead:* It is defined by the number of location claims stored by the sensor node.
- *Data security*: It means protecting of data from illegal usage by unwanted users.
- *Detection probability*: It measures how accurately a detection protocol identifies and detects the clones or replicas.
- *Detection time*: It is the average time delay between the deployment and detection of replica in a network.
- *Cost factor*: It is the amount of cost incurred in delivering the packet/data from source node to destination.
- *Energy efficient*: It is defined as the minimum energy used by node to route the packet to desired location.
- *Delivery rate:* It is given by the ratio of no. of packets received by total no. of packets sent.
- *Packet loss*: It mainly occurs due to congestion or failure in the network. It deals with the no. of packets failed to reach the destination.
- *Revocation*: It refers to the cancelling or annulment of something by some authority.

A. Effects of Node Replication Attack on the Security Goals

The main security goals of WSN include availability, authenticity, confidentiality and data integrity [15]. When an adversary launches node replication attacks, all these security goals gets affected thereby making the network unreliable and unsuitable for further communication. Two main reasons for this are first, there is no proper and efficient detection schemes to identify and revoke the attacks. Secondly, some detection schemes offer less detection probability [7].

The presence of replicas or clones causes several damages to the network as they are considered as honest/legitimate nodes by their neighbor and use the cryptographic keys to participate in the network operation. The adversary mainly creates these clones to launch a variety of insider attack such as monitor the traffic in the network, falsify sensor data, inject false data, subvert data aggregation, jam the signals, launch DoS attack and also try to disrupt the network operations [30].

B. Security Goals of WSN

- ***Availability:*** It ensures the availability of network services in amidst of attacks. Due to node replication attack, the adversary tries to compromise the availability of network services by hindering its operations.
- ***Authenticity*:** It usually defines the identity of the participating nodes in the network communication. Due to node replication attack, as the clone also possesses the same key information like the original node, it becomes difficult to differentiate a clone and original/legitimate node.
- ***Confidentiality-*** It assures secure exchange of data between authorized nodes. Due to node replication attack, as the clone node behaves similarly as normal node, they try to misuse the data transmitted in the network thereby making the private data as public data.
- ***Data integrity-*** It ensures that data are reliable, unchanged and can be used for communication between nodes. Due to node replication attack, an adversary can inject false data, change the code, falsify the data, etc. thereby

making the data unreliable for transmission.

IV. Classification of Node Replication Attack Detection Schemes in Static WSN

The presence of node replication attack affects the security goals namely, availability, authenticity, confidentiality and data integrity [33]. Hence various detection schemes were proposed to remove and control node replication attacks. Normally the replica detection mechanisms are classified into two main categories namely network-based and radio-based. Earlier, radio-based detection was used which authenticate nodes and detect replicas using signal strength or other physical characteristic of communication network [8]. The network-based approach is further classified as SWSN and MWSN, which in turn is further classified Centralized and Distributed Schemes [20].

The above categorizations of schemes are represented using a neat sketch that offers better understanding of various detection schemes. The detection techniques employed for static WSN are broadly classified into two types namely centralized and distributed techniques [34]. In subsequent section the various schemes for static WSN are described briefly followed by the comparative analysis and further discussions.

A. Local Voting Scheme

In [3], Chan et al. initially proposed a local voting scheme to detect the replicas in the network. The scheme allows the neighbor nodes to cast public votes against the identified misbehavior node. If a node B sees that the public votes for a node A exceed the threshold t value then B stops its communication with A. Eventually this scheme helped to identify replicas but it is limited only to less number of neighbor nodes. It failed to detect the replicas within the neighborhood. It also makes accuracy and sensitivity a challenging problem.

B. Random Key Pre-Distribution Scheme

Chan et al. [3] proposed a random key pre-distribution scheme where each node initially maintains a subset of random keys from a pool of keys. The keys serve as an authentication tool to test the trustiness of the nodes. In case, if two nodes possess the same common key, a secure communication link is established between them [9]. If same key is repeatedly used by a node for communication then it is detected as a clone. However it suffers storage overhead as each and every node has to maintain a list of keys, also its time consuming and the network size is fixed [14].

C. q-Composite key Pre-Distribution Scheme

Chan et al. proposed a new q-composite key pre-distribution scheme [3] to maintain the secrecy of the network in amidst of any node capture attack. It also includes node-node mutual authentication and quorum based revocation. If two nodes want to communicate, they must share latest q keys. When the match on share key is found, exclusive (XOR) function is performed on keys to get a new key which can be used for further communication. Here the computation time varies as it depends on the key size.

D. Centralized Base Station Scheme

In 2005, Parno et al. defined a Centralized Base Station scheme [4], wherein each node has to send the list of its neighbor nodes and its location claims. The base station then examines the list and looks for any replication. If identified, the Base station floods node revocation messages to the entire network. This scheme suffers a single point failure, if an adversary is able to compromise the communication channel or base station, making the scheme worthless. The nodes within the base station suffers communication burden that may shorten the network's life.

E. Distributed Techniques for Detecting Node Replication Attacks in Static WSNs

Node-to-Network Broadcast Scheme (N2NB)

In [4], Parno et al. proposed a distributed detection protocol "Node to network broadcast" that employs a simple broadcast mechanism. Here each node in the network sends authenticated broadcast message along with location information to other nodes of the network. The nodes save the location information for its neighbor and if any conflicting arises, then call the revocation procedure. It offers 100% detection of duplicate nodes provided the message has reached all the nodes. But it is possible for an adversary to induce a jam on the key locations or communication path. This situation can be avoided by nodes demanding acknowledgement for the authenticated message from the neighbors. It uses a suppression algorithm that allows the nodes to broadcast the message only once in the network. Still, the communication cost incurred by this protocol is high.

Deterministic Multicast (DM)

In order to improve the communication cost incurred by N2N broadcast protocol, a new distributed detection protocol named Deterministic Multicast (DM) was proposed [10]. This protocol sends the location claims of limited nodes only to deterministically selected *witness* nodes. When a node wants to establish a link, it broadcasts the location claim to its neighbor that forwards it to a group of nodes. The witness node looks for different location with same ID, which indicates the presence of replica. The communication cost of this protocol increases when more number of witness nodes is employed for detection process, at the same time, presence of less no. of witness favors the adversary to create unlimited replicas. Similarly, if an adversary takes control over the witness nodes, then it can create multiple replicas and suppress the conflicting reports reaching the witness node [11].

Randomized Multicast (RM)

To improve the resilient nature of the DM protocol, Parno suggested a new protocol namely RM protocol that chooses witness nodes randomly so as to make the adversary unpredictable about the replicas. In RM, each node sends its authenticated location claim information to its neighbors. This

is done by randomly choosing a location using geographic information (GPSR). Later the information is forwarded to nodes that are near/close to it. The witness node receives the location claim and verifies its signature [21]. It then crosschecks ID for the presence of different location information for the same ID with the already available list. Being found, the witness node floods the network with node ID information, thereby requesting the other nodes to not invite them for any communication. It confirms that communication is blocked from that ID in the network [18]. By implementing Birthday paradox methodology, there is a possibility for at least one of the witness node to receive conflicting locations for the same ID. This protocol securely detects and removes the replicas in a distributed fashion in the network. Also, the use of Birthday paradox increased the detection probability of replica with few witness nodes [13].

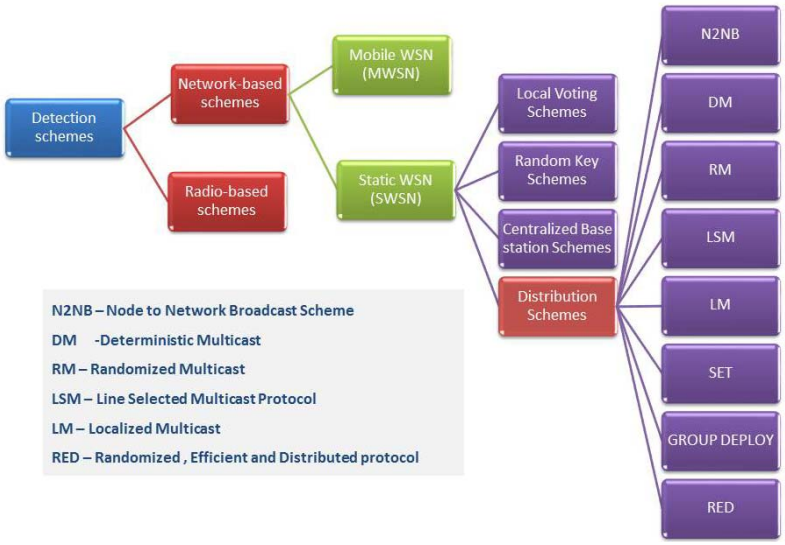

Fig. 4 Detection Schemes for Wireless Sensor Network

Line Selected Multicast Protocol (LSM)

To reduce the communication cost incurred by RM scheme, a new kind of distributed protocol is devised based on the work of Braginsky and Estrin which describes a "Rumor routing" concept. It says that a sensor node can serve both as a sensing node and as router. Initially the node broadcasts its location claim to the neighbor nodes. As the location claim passes through several intermediate nodes, let all the intermediate nodes maintain a copy of this location claim in their memory [16]. The presence of replicas are identified by looking for intersection to two paths generated by two different node claims carrying same ID coming from different location. If a node comes across any conflicting location claim, it immediately calls the revocation procedure to revoke the replicas. If collision of location claim does not occur, then a communication link is established between the nodes to ensure secure transmission of data. This protocol offers secure and clear detection of replicas, as it is very difficult for the adversary to trace where collision occurred in the network. This scheme offers less communication and storage cost when compared to RM scheme and its detection rate purely depends on the network routing topology. The storage requirements of these protocols can be further reduced by using Time Synchronization methods.

Localized Multicast (LM)

In [27], Zhu proposed a novel and efficient distributed protocol to detect node replication attacks that use a different approach in selecting witness nodes. Here witness for sensor nodes are randomly selected from a group of nodes that belong to a particular geographical region or locality (cell). LM is broadly classified into two types namely Single Deterministic Cell (SDC) and Parallel Multiple Probabilistic Cell (P-MPC). Initially the node ID is deterministically mapped to one or more cells and then randomization technique is employed in the cells to improve security and resilience against node compromise.

(i) SDC

This scheme uses one-way hash function to map node ID to the corresponding cell in the grid. When a node broadcasts its location claim, the one hop neighbor nodes receive it, perform a one-way hash function so as to map the node ID with the appropriate cell and then forwards to claim information to that cell. On receiving, the witness node checks the location claim for similarity. If a match is found, then informs the base station. Now it is the responsibility of the Base Station to flood the network with that ID information to revoke the replicas. Here, flooding of the network starts until the further copies of the same data are ignored. The cost incurred in communication and storage is very less when compared to LSM [29].

(ii) P-MPC

It slightly differs from SDC, wherein the ID of the node is

mapped to multiple cells instead of single cell. Other functionalities of MPC are same as that of SDC. However, the two schemes fail to detect the replicas in two conditions. First, the neighbor fails to forward the location claim information to other nodes. Second, the nodes fail to store the claim information in their memory.

SET

In [11], Choi et al. proposed SET, an effective and efficient scheme to detect node clone attacks. It performs set operations specifically intersection and union of the subsets in the network to discover clones. The system generates exclusive subsets in the network where each subset includes a subset header/subset Leader (SLDR). The sensor nodes deployed in the subset are unique and no two subsets contain overlapping information. All nodes in the network possess a unique ID and nodes join the subset based on the hop-count details. Each SLDR submits reports about its member nodes to the base station for detecting clones in the network. Suppose if an adversary creates replicas and deploys them within the network and therefore the result of intersection of two subsets not equal to zero, this means clone has been detected. It also ensures authentication of nodes by constructing tree structures with non-overlapping subtrees. Further, it uses randomization techniques to make exclusive subsets and tree structure unpredictable to adversary. SET reduces the communication and memory overhead when compared to RM, LSM and LM. However, it takes a longer time to detect clones, as it has to get reports from all SLDR to confirm the presence of a replica.

Group Deployment Scheme

In [23], [24] Yu et al. proposed a secure, distributed and efficient detection scheme for node replicas, with an assumption that nodes are deployed in groups with respect to a predetermined deployment point and nodes are aware about their group location. This scheme allows the nodes to communicate only with their group members, thereby highly reducing the overhead caused by sending, receiving and verifying of location claims by the nodes. By using the group knowledge, it can avoid node replication attack. It also does not support inter-group communication. This scheme defines two types of nodes namely, *trusted nodes*- that are close to the group deployment point and *untrusted nodes*- that are far away from the deployment point. In this scheme, the node accepts only those messages coming from trusted nodes and ignores other messages. Here the adversary must be aware of the deployment knowledge to create replicas. It mainly reduces the overhead caused by communication, storage and computation. Sometimes there is a possibility of having honest nodes far away from the deployment point

Randomized, Efficient and Distributed protocol (RED)

In [12], [32], Conti et al. proposed a self-healing RED for detecting replicas in the network. This autonomous nature of the protocol allows it to perform continuous iterations to detect and remove clones/replicas from the network. During this process, it maintains the performance of the network and also offers high detection rate. RED is similar to Random Multicast (RM), but it selects witness node pseudo randomly purely based on the network-wide seed [17]. The protocol executes in two steps. First step involves sharing of a random value (rand) among all the nodes. The rand value can be shared either by using centralized mechanism of employing a leader selection strategy to select a leader among the nodes and that broadcast the random value. In the second step, each node digitally sign's the location claim using its private key and broadcast along the geographic location in the network. When the neighbor receives the claim, it just forwards to pseudo randomly selected witness nodes in the network. Here the intermediate nodes will not verify the claim signature and store a duplicate copy of the message as it may be viewed only by the destination node as against LSM. Instead of storing the entire message, each intermediate node is allowed to maintain the copy of the path of the message so as to detect the sender of it. Once the destination receives the message, it verifies the signature and the nonce of the message to confirm its freshness. Once it is confirmed as an original message, the witness node tries to extract the details about the message (node_ID, location) [28]. If it comes across two conflicting details for the same ID (locations/time), it indicates the presence of clone and the corresponding revocation procedure is invoked. RED offers less computation and storage overhead when compared to LSM. RED is a lot more resilient to replica attack than LSM. If the adversary tries to compromise the witness node, then the presence of clone gets unnoticed till it reaches the desired location, as the intermediate nodes just replay the message. Taking it into account, when same no of witness nodes are compromised in LSM and RED, LSM offers a slightly higher detection rate when compared to RED [26].

V. Comparison of Node Replication Attacks in Static WSNs

This section mainly provides clear comparative study of the various detection mechanisms against critical parameters of the sensor nodes. Comparative analysis of different detection schemes are mentioned in Table I. From Table I it is clearly understood that almost all detection schemes suffer high communication overhead and storage overhead but still offer high detection rate. There are also certain schemes that provide a good detection rate of replicas with low communication and storage overheads.

VI. Contribution of Detection Schemes

In addition to detecting replication attacks in WSN, these schemes also identify other attacks while routing data in the WSN [25]. Some of them are summarized in Table II. From Table II it is clear that the distributed detection schemes are the most robust and resilient against many security breach attacks in the network.

TABLE I
COMPARISON OF EVALUATION METRICS OF VARIOUS DETECTION SCHEMES

Schemes	Communication Overhead	Storage overhead	Accuracy	Security	Detection rate	Cost	No of nodes
Centralised-BS	High	High	High	High	High	Low	Medium
Random key Pre-distribution Scheme	High	High	High	High	High	High	Fixed
Localized-voting	High	High	Low	Low	Low	high	Medium
N2NB	High	High	Yes	Yes	High	High	Medium
DM	High	high	Medium	Medium	High	medium	Fixed
RM	High(non-trivial)	High(cost)	High	High	High	Very high	Less
LSM	Less	Less	High	High	High	Slightly Less	Less
LM	Less	Less	High	High	Very high	Less	WN/ cell
SET	Low	Low	High	High	High	Moderate	Fixed
Group Deployment Protocol	Less	Less	Medium	Medium	Medium	Medium	-
RED	Low	No	No	No	Highly detects	High	Less

TABLE II
OTHER ATTACKS DETECTED BY REPLICATION DETECTION SCHEMES

Type Of Scheme	Protocol/Technique/ Scheme	Detect Other Attacks
Centralized	Centralized Base Station	ARP Spoofing, ARP Cache Poisoning, Jamming, Blackhole, Wormhole
	SET	Collusion attack
	Local Negotiated algorithm	Collusion attack, Sybil attack
	CSI	Sinkhole, Wormhole, Selective forwarding, Sybil attack
Key Predistribution	Random key Pre-distribution	Jamming, Spoofing, Replay , Collusion attack
	Polynomial-based Space-time related Pairwise Key Predistribution (PSPP-PKPS)	DoS attack, Wormhole
Local	Trusted Voting	Man-in-the-middle attack
Distributed	Node-to-Network Broadcast (N2NB)	ARP Spoofing, ARP Cache Poisoning
	DM	Sybil attack
	RM	Node Clone attack
	Line-Selected Multicast (LSM)	Node Clone attack
	RED	Sybil attack
	SDC	Sybil attack
	P-MPC	Sybil attack
	Neighbor-based Detection	Node/Link failure, DoS attack, Jelly fish attack
	Memory efficient protocols: B-MEM,BC-MEM,C-MEM	DoS attack ARP Spoofing
	Distributed Protocol	DoS attack, ARP poisoning,, DNS attack
	Randomly Directed Exploration (RDE)	Wormhole attack
	Random Walk (RAWL)	Sybil attack, Sybil identity
	Table-assisted Random Walk (TRAWL)	Node capture, Sybil attack
	CINORA	Man-in-the-middle attack, Blackhole attack
	Node-based Randomized and Distributed Protocol(NRDP)	Sybil attack
	Group Deployment Knowledge based scheme	ARP poisoning, Sybil attack

VII. CONCLUSION

This article reviewed one of the most critical issues in WSN named node replication attack. We also discussed the hierarchy of attacks, classification of different schemes available to prevent and detect replication attack from the network such as Local voting Scheme, Random Key Scheme, Centralized and Distributed Schemes. Also the above survey highlights the facts that there are still a lot of critical challenges in replication detection schemes that need to be resolved so as to make this network more suitable for real-time application.

ACKNOWLEDGMENT

The author thanks to Ph.D. Supervisor for guiding in crafting the survey paper.

REFERENCES

[1] C. Karlof and D. Wagner, "*Secure routing in Wireless Sensor Networks: Attacks and Countermeasures",* in proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003.
[2] Haowen Chan and Adrian Perrig, "*Security and Privacy in Sensor Network",* Carnegie Mellon University, Oct.2003.
[3] Haowen Chan, Adrian Perrig and Dawn Song, "*Random Key Predistribution Scheme Key for Sensor Networks"*, Carnegie Mellon University, 2003.
[4] Bryan Parno, Adrian Perrig and Virgil Gligor, *"Distributed Detection of Node Replication Attacks in Sensor Networks***", i**n proceedings of the IEEE Symposium on Security and Privacy (IEES and P'05), pp.49-63, May 2005.
[5] Carl Hartung, James Balasalle, Richard Han, "*Node Compromise in Sensor Networks: The Need for Secure System (*Technical Report CU-CS-990-05)", Dept of Comp Sci, Univ of Colorado at Boulder, Jan. 2005.
[6] H. Luo, L. Zhang "*Statistical en-route filtering of injected false data in sensor network",* in proceedings of the IEEE Journal on Selected areas

in Communications, vol., No. 4, Apr. 2005.
[7] Yun Zhou, Yanchao Zhang, Yuguang Fang, "*Access control in Wireless Sensor Networks,* Elsevier 2006.
[8] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "*Secure sensor network routing: A Cleanslate approach",* in Proceedings of the ACM CoNEXT Conference, Dec.2006.
[9] Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan, Mahmut T. Kandemir., "*On the Detection of Clones in Sensor Networks Using Random Key Predistribution",* IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol., No. 6, Nov. 2007.
[10] Bo Zhu, et.al, "*Efficient Distributed Detection of Node Replication Attacks in Sensor Networks* (A Research article)", Concordia University, 2007.
[11] H. Choi, S. Zhu, T.F.L. Porta, "*SET: Detecting node clones in sensor networks***", i**n proceedings of the 3rd International Conference on Security and Privacy in Communication Networks, pp.341–350, Sep.2007.
[12] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei, "*A Randomized, Efficient and Distributed Protocol for Detection of Node Replication Attacks in Wireless Sensor Networks",* IEEE Transactions on Dependable and Secure Computing, Sep. 2007.
[13] C. Bekara, M. Laurent-Maknavicius, "*A new protocol for securing wireless sensor networks against nodes replication attacks", in* proceedings of the 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications, 2007.
[14] Richard Brooks, P. Y. Govindaraju, Matthew Pirretti, N. Vijaykrishnan, Mahmut T. Kandemir, "*On the Detection of Clones in Sensor Networks Using Random Key Predistribution",* IEEE Transactions on Systems, Man, and Cybernetics—Part C: Applications and Reviews, vol.,No. 6, Nov. 2007.
[15] Yun Zhou and Yuguang Fang, Yanchao Zhang, "*Securing Wireless Sensor Networks: A Survey*," in IEEE Communication Surveys, Vol., No.2, 3rd Quarter 2008.
[16] Jun-Won Ho, "*Distributed Detection of Node Capture Attacks in Wireless Sensor Networks*", Smart Wireless Sensor Networks, www.intechopen.com.
[17] Y. Sei and S. Honiden, *"Distributed detection of node replication attacks resilient to many compromised nodes in Wireless Sensor Networks*", in proceedings of the 4th Annual International Conference on Wireless Internet, 2008.
[18] K. Xing, F. Liu, X. Cheng, D. H.C. Du., "*Real-time detection of clone attacks in wireless sensor networks***", i**n proceedings of the 28th International Conference on Distributed Computing Systems (ICDCS), 2008.
[19] Jennifer Yick, Biswanath Mukherjee, Dipak Ghosal, "*Wireless Sensor Network Survey* (Computer Networks 52 (2008) 2292–2330)", Journal homepage: www.elsevier.com/locate/comnet.
[20] Jun-Won Ho∗, Donggang Liu, Matthew Wright, Sajal K. Das, *"Distributed Detection of Replicas with Deployment Knowledge in Wireless Sensor Networks",* Elsevier Mar. 2009.
[21] Chano, Seungjae Shin, Chanil Park, Hyusoo Yoon, "*A resilient and Efficient Replication Attack Detection Scheme for Wireless Sensor Networks", i*n IEICE Trans INE & SYST,vol., No.7, July 2009.
[22] R. Di Pietro, L. V. Mancini, C. Soriente, A. Spognardi, and G. Tsudik, "*Data security in unattended wireless sensor networks",* IEEE Transactions on Computers, vol. 58, No. 11, pp. 1500–1511, 2009.
[23] L. Yu and J. Li, "*Grouping based resilient statistical en-route filtering for sensor networks*", in the proceedings of the IEEE INFOCOM, 2009.
[24] J.W. Ho, D. Liu, M. Wright, and S. K. Das, "*Distributed detection of replica node attacks with group deployment knowledge in wireless sensor networks*", Ad Hoc Networks, vol., No. 8, pp. 1476–1488, 2009.
[25] Y. Zeng, J. Cao, S. Zhang, S. Guo, L. Xie.,"*Random walk based approach to detect clone attacks in wireless sensor networks***",** IEEE Journal on Selected Areas in Communications, vol. 28, No.5, pp.677–691, June 2010.
[26] Yingpei Zeng, Jiannong Cao, *Senior Member, IEEE,* Shigeng Zhang, Shanqing Guo and Li Xie., "*Random-Walk Based Approach to Detect Clone Attacks in Wireless Sensor Networks",* IEEE Journal on Selected Areas in Communications, vol. 28, No. 5, June 2010.
[27] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L. Wang, "*Localized multicast: efficient and distributed replica detection in large-scale sensor networks",* IEEE Transactions on Mobile Computing, vol. 9, No. 7, pp. 913–926, 2010.
[28] X. Meng, K. Lin, and K. Li, "*Note based randomized and distributed protocol for detecting node replication attack*," in Algorithms and Architectures for Parallel Processing, vol. 6081 of Lecture Notes in Computer Science, pp. 559–570, 2010.
[29] T. Bonaci, P. Lee, L. Bushnell, "*Distributed Clone detection in wireless sensor networks: an optimization approach", i*n Proceedings of the 2nd IEEE International Workshop on Data Security and Privacy in Wireless Networks, June 2011.
[30] Deng XM, 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 July 2011. DOI 10.1007/s11390-011-1172-1
[31] Yuh-Ren Tsai, "*Location Privacy in Unattended Wireless Sensor Networks upon the Requirement of Data Survivability",* IEEE Journal on Selected Areas in Communications, Vol. 29, No.7, pp.1480-1490, Aug. 2011.
[32] Mauro Conti, Roberto Di Pietro, Luigi V. Mancini, and Alessandro Mei,"*Distributed Detection of Clone Attacks in Wireless Sensor Networks*", IEEE Transactions on Dependable and Secure Computing, Vol.8, No.5, pp. 685–698, Sep. 2011.
[33] Wazir Zada Khan, Mohammed Y. Aalsalem, Mohammed Naufal Bin Mohammed Saad, and Yang Xiang, "*Detection and Mitigation of Node Replication Attacks in Wireless Sensor Networks: A Survey*", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, vol., ArticleID-149023, 22 pages, http://dx.doi.org/10.1155/2013/149023.
[34] Moirangthem Marjit Singh, Ankita Singh and Jyotsna Kumar Mandal, "*Towards Techniques of Detecting Node Replication Attack in Static Wireless Sensor Networks",* International Journal of Information and Computation Technology. ISSN 0974-2239 vol.., No. 2 (2014), pp. 153-164 @ International Research Publications House http: //www. irphouse.com

N.S. Usha holds a B.E. in Computer Science and Engineering from Madras University. She has completed M.E. in Computer Science and Engineering certified by Anna University. She is currently pursuing her Ph.D in Computer Science at St. Peter's University. She is presently working as Associate Professor in Department of Computer Science and Engineering at S.A. Engineering College. She has got 14 years of teaching experience and a member of ACM.

E.A. Mary Anita holds a B.E. in Electrical and Electronics Engineering and M.E. in Computer Science and Engineering, both from Government College of Engineering, Tirunelveli, India and a Ph.D. in Information and Communication from Anna University, Chennai. She is presently Professor in Computer Science and Engineering Department of S.A. Engineering College, Chennai. She has over 25 years of teaching experience and has published 52 research papers in International and national journals and conferences. Her main research interests are in the field of wireless networks, security and privacy. She is a Life member of Indian Society for Technical Education (ISTE), Computer Society of India (CSI), IEEE, IAENG and ACM.