IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received February 8, 2020, accepted March 1, 2020, date of publication March 24, 2020, date of current version April 17, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2983091

A Systematic Review on Clone Node Detection in Static Wireless Sensor Networks

MUHAMMAD NUMAN[1], FAZLI SUBHAN[1], WAZIR ZADA KHAN[2], (Senior Member, IEEE), SAQIB HAKAK[3], SAJJAD HAIDER[1], G. THIPPA REDDY[4], ALIREZA JOLFAEI[5], (Senior Member, IEEE), AND MAMOUN ALAZAB[6], (Senior Member, IEEE)

[1]Department of Computer Science, National University of Modern Languages, Islamabad 44000, Pakistan
[2]Department of CS and IS, Jazan University, Jazan 45142, Saudi Arabia
[3]Department of Computer Science, University of Northern British Columbia, Prince George, BC V2N 4Z9, Canada
[4]School of Information Technology and Engineering, Vellore Institute of Technology, Vellore 632014, India
[5]Department of Computing, Macquarie University, Sydney, NSW 2113, Australia
[6]College of Engineering, IT, and Environment, Charles Darwin University, Casuarina, NT 0909, Australia

Corresponding author: Mamoun Alazab (mamoun.alazab@cdu.edu.au)

The work of Saqib Hakak was supported by the University of Northern British Columbia under Grant 15021 ORG 4460.

ABSTRACT The recent state of the art innovations in technology enables the development of low-cost sensor nodes with processing and communication capabilities. The unique characteristics of these low-cost sensor nodes such as limited resources in terms of processing, memory, battery, and lack of tamper resistance hardware make them susceptible to clone node or node replication attack. The deployment of WSNs in the remote and harsh environment helps the adversary to capture the legitimate node and extract the stored credential information such as ID which can be easily re-programmed and replicated. Thus, the adversary would be able to control the whole network internally and carry out the same functions as that of the legitimate nodes. This is the main motivation of researchers to design enhanced detection protocols for clone attacks. Hence, in this paper, we have presented a systematic literature review of existing clone node detection schemes. We have also provided the theoretical and analytical survey of the existing centralized and distributed schemes for the detection of clone nodes in static WSNs with their drawbacks and challenges.

INDEX TERMS Wireless sensor networks (WSNs), clone attack, clone attack detection schemes, systematic literature review (SLR).

I. INTRODUCTION

Wireless Sensor Networks (WSNs) is gaining immense attention from the researchers due to its enormous applications in different areas such as flood detection, weather prediction, vehicle tracking, localization, target tracking. WSN is a type of technology which can perceive data and accomplish actions through the sensors [1]. One of the primary and fundamental components of WSN are sensor nodes which can become faulty/unreliable anytime. A typical sensor usually comprises four basic components i.e. power supply, a processor, a radio and an actuator. Moreover, these are not resilient to tampering. Fig. 1 depicts the general structural design of a sensor node. According to [2], [3], sensor nodes are so economical that thousands of these can be installed in the preferred locations and can be used to collect and monitor data. Various types of sensors that can monitor environment, industries, smart homes, etc. are depicted in Fig. 2. Moreover, these sensors can also detect/ monitor items that are not practically existent and even invisible, like gas and temperature.

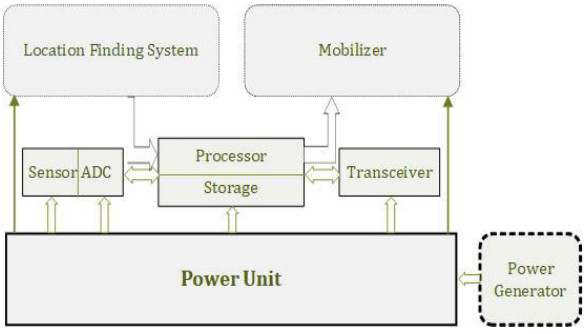

FIGURE 1. General architecture of wireless sensor node.

Although these nodes are economical and highly needed, they do have certain constraints with respect to the hardware

The associate editor coordinating the review of this manuscript and approving it for publication was Zihuai Lin.

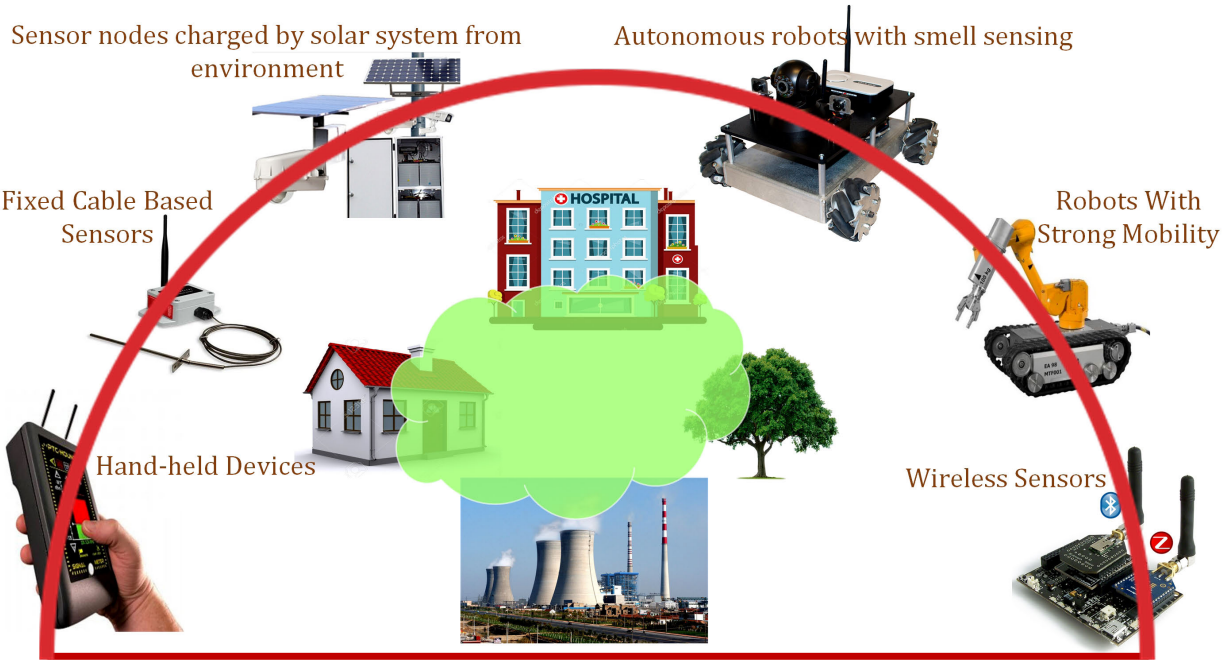

FIGURE 2. Various types of sensors monitoring environment, industries, smart homes etc.

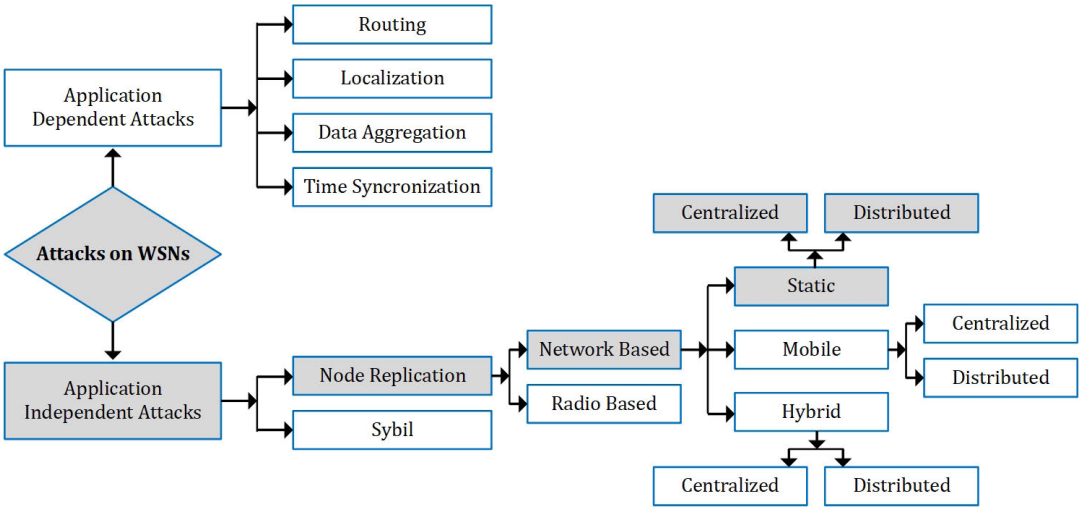

FIGURE 3. Taxonomy of attacks on WSNs.

structure, lack of robust security mechanisms, etc., that needs to be addressed [1]. It was also pointed out that conventional security methods deployed in conventional devices cannot be directly deployed in the devices with these sensor nodes [4]. One of the most challenging tasks of devices operated within sensor networks is, they face the risk of being damaged by physical attacks like node replication. This will facilitate the enemy to attack the node and duplicate them into several clones and hence, taking charge of the whole network. This makes the clone recognition a very crucial aspect to sense the illicit copies and safeguard the sensor networks; while clones have a major effect on network routing, data accumulation, key distribution, etc. Hence, networks should be protected and be able to assess the exposure to risks and attacks [2]. Fig. 3 shows that sensor networks could either be vulnerable to layer dependent or layer independent attacks. The two most hazardous layer independent attacks are clone node (which is also called node replication) and Sybil attack [5], [6]. In Sybil attack, attacker generates several IDs for a single node by sneaking into the existing ones from a corrupted node. Such attacks can be minimized by methods and protocols based on RSSI [7] or by knowledge-based authentication mechanisms of a fixed key set [8]–[12]. On the other hand, in the clone node attack, the attacker physically captures a node, then generate clones or duplicates of it and finally deploy these clones in strategic positions of the WSNs.

A more alarming feature is that the attackers are so intelligent that they can interact with the newly generated clones easily by pretending as legal nodes within a short span of time [13]. This may explain why the conventional secured routing system [14], [15] and validation schemes [16]–[21] will never be capable of assessing or minimizing clone damage from the occurrence. Many schemes are proposed for the detection of clone nodes but most of them are not effective. The only exemption is the distributed witness node based techniques that seem to have promising results until now and this is the main focus of this paper. But these techniques do have their own limitations such as the deterministic selection of witness nodes, uneven distribution of witness nodes (crowded center problem) and a trade-off between high detection probability with high communication and memory costs.

Compared to the existing studies, to the best of our knowledge, this study is the first survey that has explored advanced pattern for conducting survey in the area of clone node detection through systematic literature review (SLR). In this survey, the main aim is to develop the theoretical understanding of centralized and distributed based clone node detection schemes in static WSNs. The classification of current detection approaches in light of the literature review is highlighted. We have also identified challenges and drawbacks in the prominence of WSNs security through the Research Questions (RQ).

The organisation of the paper as follows. Section 2 provides a detailed background about WSNs and clone node attack. Section 3 describes in detail the conducted SLR along with clone detection schemes with obtained results and challenges. Finally, Section 4 concludes the paper.

II. BACKGROUND

In this section, we have highlighted the procedure for carrying out the clone node attack and provided a brief overview of clone detection techniques used in static Wireless Sensor Networks.

A. CLONE NODE ATTACK

WSNs are primarily categorised into two types i.e, Static and Mobile WSNs. In Static WSN, once the sensor nodes are deployed, their position remains fixed compared to Mobile WSN where nodes can move freely after deployment. In other words, we can say Static WSNs use fixed flooding/routing for data distribution whereas Mobile WSNs use dynamic routing. Both of these categories of WSN are prone to clone node attacks.

Clone node attack is regarded as one of the most hazardous attacks on WSNs. In a clone attack, the attacker initially targets and captures a legal node, extracts the stored credentials using some specialized tools in less than one minute [13]. The attacker then creates clones using the credentials and deploys them to several important locations of the network to carry out internal attacks like denial of service (DoS), a black hole or even wormhole attack [22]. Subsequently,

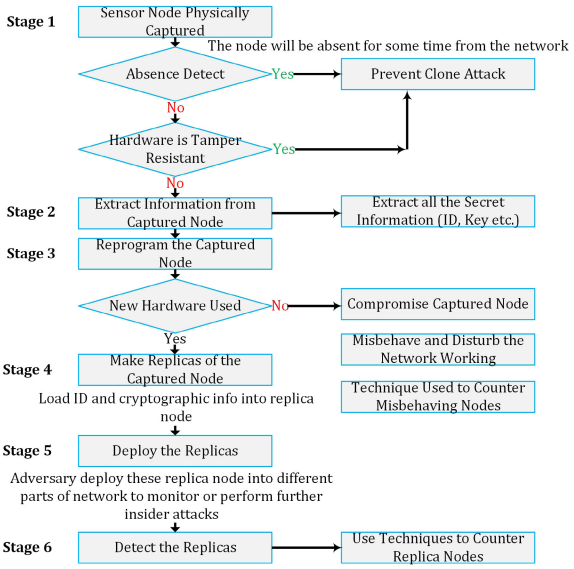

FIGURE 4. Stages of node clone/replication attack in WSNs.

the attacker will isolate the acquired legal node from the network and implement the clones and thus be able to capture and may even cancel the node withdrawal scheme [23]. Hence, to minimize further damage, clones must be detected in minimal time, which is not an easy task due to several factors such as nodes having legal IDs, information, etc. However, as the sensor nodes of the static WSNs have fixed positions, it becomes easier to detect if there are any node replicas or clones compared to Mobile WSN. This is usually done by analysing whether a logical ID of a legitimate node is associated with more than one node in the network. However, in mobile WSNs the scenario is different, as the nodes roam around in the network, so even if an ID is detected in a certain position, it may be difficult to assume that there is a clone if the ID is found again in another place, as the node may be roaming. More details about Mobile WSNs clone detection techniques can be found in [24].

To carry out the Clone Node attack, the following four steps are undertaken:

1. The primary and initial step is that an adversary capture the legal nodes in the network physically.

2. Afterward, the attacker acquires all the confidential credentials (i.e. IDs, information, data, etc.) of the captured node.

3.Then attacker utilizes all the information obtained to generate new nodes using the same identities of the grabbed legal nodes.

4. Finally, the last step involves mounting the clone nodes into key positions throughout the network.

Once the above-mentioned procedure is accomplished, the attacker can then perform various actions with the help of these clones, or carry out more internal attacks to the network. The entire process of launching and detection of clone attacks is depicted in a flow chart shown in Fig. 4.

TABLE 1. Centralized clone detection techniques.

Scheme	Algorithm	Communication Cost	Memory Cost	Advantages	Drawbacks
Key usage based	Brooks et al [2]. Scheme	O(n log(n))	N/A	N/A	Higher rate of false positive and negative, how to guarantee that malicious nodes reliably report their credentials to BS is not addressed
Base station based	SET [22]	O(n)	O(d)	Location independent, Low memory overhead	Single point of failure, Costly
	RED [25], [26]	$O(\sqrt{n})$	$O(d\sqrt{n}$	Low memory overhead, Higher detection probability, uniform distribution of witnesses due to pseudo-random selection of the witness nodes	Need a trusted entity (Trusted third party is needed), Deterministic
	CSI-1 [27]	O(n log(n))	O(log(n))	Highest probability rate for detecting replica nodes	Communication and storage overhead are high
	Tayeb Kenaza et al [28].	Trans, to the BS*NS+ response of the BS*NS	2 keys (IK U and P)	Achieved high clone detection rates	This approach suffers from the lack of scalability and also shares other common drawbacks of centralized solutions
	CSI-2 [29]	O(n)	O(1)	Lowest Communication and storage overhead	Low detection probability of replica nodes
	PVM-MVP [30]	$O(N^2)$	$O(N)$	Detection rate of the replication attack is more accurate	Throughput of the network is higher due to which the network lifetime is decreasing, time consuming and cost effective
Neighborhood social signature based	K. Xing et al [31]. Scheme	C. (1 + ratio)	O(d) + min(M wlog2 M)	Low computation overhead	Can't grip a sophisticated clone which can smartly work out by itself, a fingerprint dependable by its neighborhood for detection and protection
Cluster head based	ABCD [32]	O(n log(n))	O(n)	Probability of detection is high	Single point of failure, High communication overhead, decrease network lifetime
	LNCA and Bloom Filter [33]	$O(t^2)$	$O(t)$	Communication overhead is comparatively low	Clone nodes detection probability is very low
Zone based	ZBNRD [34]	$O(N.\sqrt{nZ}) + O(Nz.\sqrt{N})$	$O(d)/O(nZ)$	Dynamic detection of replicas	Deterministic
Neighbor ID based	X-RED [35]	$O(nlog(n))$	$O(n)$	Detection probability is higher, reduced memory overhead	Large traffic overhead

B. THREAT MODEL

In WSNs, the attacker may possibly launch active and passive attacks. In this work, we consider the existence of an active attack, in which the attacker can launch a clone node attack by compromising a subclass of nodes and producing large amount of replicas for distribution all over the network. Upon compromising a node 'n', the attacker may produce a group of replicas $n' = n'_1, n'_2, n'_3, \ldots .n'_r$ of which the IDs and secret credentials are the same as the original node n. Replicas can easily override the authenticity and integrity of existing cryptographic security mechanisms because they can sign, encrypt, and decrypt messages to execute the rule, just like original vulnerable node. Once replicas are identified as a legitimate part of the network, they can launch a variety of attacks, such as Sybil attack, selective forwarding attacks, incorrect data injection, protocol interruptions and traffic jams.

C. CLONE DETECTION TECHNIQUES IN STATIC WSNs

There have been numerous techniques proposed for Clone Detection in Static WSNs which can be categorised into centralized and distributed techniques.

- Centralized Clone Detection Techniques:
  Apart from being complex and having low overheads, these techniques mainly rely on powerful Base Station (BS) for information convergence and decision making, where the nodes send their position claims to the BS with the help of their neighbors. Then the BS will check the node IDs, and if one ID is found in more than one location, an alarm is set up to give alertness about the presence of a clone attack. These techniques are capable enough to detect clone attacks. Yet, this does not mean that private information of the sensor is secured, where the attacker can do many negative things to spy on the transmitted information between the sink and sensor node. Thus, there may still be a threat to the network. Another problem is that the lifetime of the network may decrease quickly due to the fact that the nodes which are closer to the sink node lose their energy faster.
  The static WSNs centralized detection techniques can be categorized into one of these six categories, i.e. key usage-based, base station based, neighborhood social signature based, cluster head based, zone-based and neighbor ID-based technique [2], [22], [25]–[35] and their comparison is shown in Table 1.
- Distributed Clone Detection Techniques: The main difference here is that the process of clone detection is done by all the network nodes, which means that there is no central node of authority assigned to do the work. This also means that even the nodes that are located in distant

TABLE 2. Distributed clone detection techniques.

Scheme	Algorithm	Communication cost	Memory Cost	Advantages	Drawbacks
Node to network broadcasting	N2NB [36]	$O(n^2)$	$O(1)$	Higher detection rate, proficient than the centralized method	Higher communication cost
Witness node based	DM [36]	$O(glog\sqrt{n})/d$	$O(g)$	Reduced communication overhead	Less secure
	RM [36]	$O(n^2)$	$O(\sqrt{n})$	Enhanced resiliency, Hard to predict witnesses	High communication cost, also has lesser detection probability
	LSM [36]	$O(n\sqrt{n})$	$O(\sqrt{n})$	Less communication overhead than RM, memory efficient,	Crossover problem and crowded center problem
	SDC/ P-MPC [37], [38]	$O(r.\sqrt{n}) + O(s)$	$O(\omega)$	Low memory overhead, more efficient then LSM	Depends on trusted entity and cell size. High communication overhead (if size of cell is larger), if smaller then node can be compromised easily
	B-MEM [39]	$O(k.n.\sqrt{n})$	$O(tk + t'k\sqrt{n})$	Higher detection probability, lower memory usage	Location dependent
	BC-MEM [39]	N/A	$O(tk + t'k\sqrt{n'})$	High detection probability, less storage overhead, solved crowded center and crossover problems	Location dependent
	C-MEM [39]	N/A	$O(t + t'\sqrt{n})$	N/A	Location dependent
	CC-MEM [39]	N/A	$O(t + t'\sqrt{n'})$	N/A	Location dependent
	RDE [40]	$O(d.n.\sqrt{n})$	$O(d)$	Lower memory overhead	Not suitable for dynamic topological scenarios
	Chano KIM [41]	$O(\sqrt{n})$	$O(\sqrt{n})$	Reduces the number of communication messages	Not having promising results in detecting node replication attack
	RAWL [42]	$O(\sqrt{n}log(n))$	$O(\sqrt{n}log(n))$	High detection probability	Higher memory and communication cost
	TRAWL [42]	$O(\sqrt{n}log(n))$	$O(1^2)^2$	High detection probability	Higher communication cost
	NRDP [43]	$O(N.g\sqrt{N})$	$O(g)$	The simplest method for exchanging group membership information	It has an extra overhead of choosing reporter nodes
	DHT [44]	$O(logn\sqrt{n})$	$O(d)$	Providing efficient clone detection probability	Higher communication cost
	GDL and RMC [45]	$O(\sqrt{1} \times \sqrt{m}/2)$	$O(\sqrt{n})$	To deliver a higher level of compromise-resilience random verification is used	Due to its deterministic verification process, it is not robust to a smart node replication attack
	RWND [46]	N/A	N/A	High probability of detection, with high security of witness nodes	High communication, memory and energy cost in case of more areas
	SSRWND [47]	N/A	N/A	High probability of detection, with high security of witness nodes	High communication, memory and energy cost in case of more areas
	ERCD [48]	$O(h\sqrt{h})$	$O(h)$	High detection probability with random witness selection	To store witnesses it requires a small ring routing, this reduces the storage requirements of the nodes
	PAWS [49]	$O(3\sqrt{n}log(n))$	$O(1)^2$	Energy consumption, detection probability, and resiliency	Limited redundancy
	RE-GSASA [50]	$O(n\sqrt{n})$	$O(n)$		Messages overhead are high
Generation or group based	Bekara et al [51], [52].	$O(n)$	$O(1)$	This scheme is simple, incurs less communication overhead	Nodes are bound to their groups and geographic locations
	Basic Scheme [53]	$O(m)$	$O(m)$	The communication, computational and memory overhead is lower	The network is poorly connected making it unsuitable for high robust applications
	Location Claim Base Scheme [53]	$O(m + d)$	$O(d + 2m)$	High detection capability, less communication, computational and storage overhead	Flooding fake claims due to DoS risk
	Multi-Group Base Scheme [53]	$3xO(m + d)$	$O(d + 2xm(1$ +Dmax))	Robust to node compromise ever since an adversary wishes to compromise several groups	Higher communication overhead
	Yuichi Sei [54]	$O(r)$	$O(r.\sqrt{n})$	No trusted entity, more resilient	Higher communication cost, built-in detection start time
Neighbor based	NBDS [55]	$O(r.\sqrt{n})$	$O(r)$	Location independent	Messages overhead are high
Clustering based	NI-LEACH [56]	$O(l(1 + m'2))$	$O(k.e)$	Balanced throughput, less delay	Lower detection rate (in case of multiple adversaries)
Witness path based	LSCD [57]	$O(n\sqrt{n})$	$O(l/r)$	The dynamic mechanism in detection route establishment ensures the high detection probability, storage overhead of nodes is relatively low	The communication cost is high
Cluster head based	LTBRD [58]	N/A	N/A	Energy consumption and memory occupancy is low	Detection probability is low
	PRCD [59]	$O(Np)$	$O(1/p)$	Low computing complexity, long network lifetime	N/A

TABLE 3. String searching.

S.No	Digital Library Searched	URL	Search String (Track)
1	Science Direct	http://www.sciencedirect.com/	"Clone Node Detection" OR "Replica Node Detection" OR "Node Compromise Attack" AND "Centralized Approach" OR "Centralized Technique" OR "Centralized Scheme" OR "Centralized Method" AND "Distributed Approach" OR "Distributed Technique" OR "Distributed Scheme" OR "Distributed Method"
2	IEEE Xplore	http://ieeexplore.ieee.org/	
3	Google Scholar	https://scholar.google.com.pk	
4	Springer Link	http://link.springer.com/	
5	ACM	https://dl.acm.org/	

TABLE 4. Track result.

Search String	Digital Libraries Searched				
	Science Direct	IEEE Xplore	Google Scholar	Springer Link	ACM
Track	1,555	14,854	16,900	69	66

TABLE 5. Inclusion/exclusion criteria.

Inclusion criteria
a) Research studies and articles that are relevant to formulated RQ are included in the final list. b) Research work having the keywords "Wireless Sensor Network, Clone Node Detection, Centralized Approach, and Distributed Approaches" is included in the final list. c) The research papers/articles/books/review papers written in the English language only are included. d) The articles/papers that are published online are included in the list.
Exclusion criteria
a) Literature that does not fulfill the above mentioned criteria ha been excluded. b) The researchers excluded all the duplicate papers. c) The papers reporting table of contents or the information regarding the proceedings of conferences, workshops are not included.

positions in the network are involved in this process. Focusing on the Static WSNs, there are seven different types of detection techniques, which are node to network broadcasting (N2N), witness node-based, group or generation-based, neighbor-based, clustering-based, witness path-based and cluster head-based techniques [36]–[59] and their comparison is shown in Table 2.

III. SYSTEMATIC LITERATURE REVIEW

We conducted a SLR to find the challenges and answer the questions raised in our research domain. SLR is a protocol based research approach conducted to shortlist and assess the most relevant studies used to answer RQs. In case of the WSNs security domain, SLR is a stimulating research method for data collection. For this, we followed SLR guidelines [60]–[62]. Detailed steps are as given in following subsections.

A. SEARCH STRING FORMATION

The most important step in SLR is the searching and filtering process [63]–[66]. Following Search Filters (SF) have been used in our study for the creation of customized Search Questions (RQs).

SFs 1: We derived the major search terms from the RQs. These terms are (1) Clone Node Detection (2) Centralized Approach (3) Distributed Approach.

SFs 2: Identification of synonyms for the significant terms. clone node detection: (‘‘clone node detection’’ OR ‘‘replica node detection’’ OR ‘‘node compromise attack’’), centralized approach: (‘‘centralized approach’’ OR ‘‘centralized technique’’ OR ‘‘centralized scheme’’ OR ‘‘centralized method’’), distributed approach: (‘‘distributed approach’’ OR ‘‘distributed technique’’ OR ‘‘distributed scheme’’ OR ‘‘distributed method’’).

SFs 3: Verification of the keywords in the relevant papers. (‘‘Clone node detection’’, ‘‘replica node detection’’, ‘‘node compromise attack’’).

SFs 4: The operator AND, OR are used along with search strings. Track: (‘‘clone node detection’’ OR ‘‘replica node detection’’ OR ‘‘node compromise attack’’) AND (‘‘centralized approach’’ OR ‘‘centralized technique’’ OR ‘‘centralized scheme’’ OR ‘‘centralized method’’) AND (‘‘distributed approach’’ OR ‘‘distributed technique’’ OR ‘‘distributed scheme’’ OR ‘‘distributed method’’), where Track denotes a search string that is intended to search the literature specific to clone node detection in the context of WSNs security.

B. ONLINE SEARCH VENUES (DIGITAL LIBRARIES)

Based on SF4, Table 3 shows selected digital libraries for searching the relevant studies. Tables 3,4 and 6 depict the details of the digital libraries. A total of 33,444 research articles have been retrieved and six papers are identified via a snowballing method. By adopting the Tollgate approach, we selected 123 papers in the first phase based on the research title and abstract via inclusion/exclusion criteria. In phase 2, we reviewed these research articles and refined them to 37 articles.

C. INCLUSION/EXCLUSION CRITERIA

The findings of the search string Track are further evaluated to confirm that the filtered research articles meet the inclusion and exclusion principle defined in Table 5.

TABLE 6. Publication search details in various digital libraries.

Digital Library	Total Papers Found	1st Level of Inclusion/Exclusion	2nd Level of Inclusion/Exclusion	3rd Level of Inclusion/Exclusion
Science Direct	1,555	10/1,545	0/1,555	37/33,413
IEEE Xplore	14,854	33/14,821	20/14,834	
Google Scholar	16,900	45/16,855	4/16,896	
Springer Link	69	21/48	7/62	
ACM	66	8/58	1/65	
Publications through snowballing technique	6	6/0	5/1	
Total	33,450	123/33,327	37/33,413	37/33,413

TABLE 7. Publication quality assessment.

S.No Quality Assessment Standards	Value/Score
QA1: Checked appropriateness of aims and objectives of selected research paper	Yes = 1, Partial = 0.5 No = 0
QA2: Checked whether the conclusion matches with defined objectives of the research	Yes = 1, Partial = 0.5 No = 0
QA3: Checked the core terms of the research, i.e. Clone Node Detection. Additionally, check whether these terms are defined and discussed clearly.	Yes = 1, Partial = 0.5 No = 0
QA4: Checked the appropriateness of how the clone node detection scheme has been identified in the selected papers. Note: QA4 intends to seek the method(s), through which the reported clone detection scheme has been identified. If the method(s) is clearly mentioned, then it is marked as Yes = 1; otherwise, No = 0.	Yes = 1, Partial = 0.5 No = 0

D. PUBLICATION QUALITY ASSESSMENT

Every paper was tested against the Quality Assessment (QA) standards shown in Table 7 along-with scores. The aim of the QA was to know the quality of the research papers selected. We performed the QA during the data extraction phase. Every QA criterion has 3 possible values: Yes, Partial and No with marks of 1, 0.5, and 0, respectively. Detailed scores of the 37 papers finally selected are given in Appendix, where R1 and R2 represent the respondent's Author 2 and 3 respectively.

For each given item QA1 to QA4 the evaluation is performed as follows:

- The research article that answers to the checklist queries are assigned 1 point.
- The research articles containing some of the answers to the checklist questions were assigned 0.5 points.
- If there is no answer to the checklist, queries were assigned 0 points.

Question 4 intends to seek the method(s), through which the reported challenges have been identified. If the method(s) is clearly mentioned, then it is marked as Yes $= 1$; otherwise marked as Partial $= 0.5$ or No $= 0$. Similar criteria are used by [67], [68].

E. DATA EXTRACTION PROCESS

This is an important step in SLR, in which the data is extracted from already selected research articles. The criteria adopted for extraction are purely based on RQs. The predefined rules for data extraction are paper ID, title, reference, year, research database, quality of the publication, the country where the research was performed, context, schemes, methods and also pros and cons of each technique.

F. DATA SYNTHESIS

As per the SLR protocol, we performed a synthesis of the data extracted from already filtered research articles and created different categories of the challenges. Initially, we identified 14 challenges, but the further classification was performed and few challenges were merged. Finally, a list of 6 challenges were identified which are discussed in Table 8. Out of these 6 challenges, 4 challenges are considered as critical with a frequency of more than 10% while the remaining 2 having a frequency of less than 10% are considered non-critical.

G. RESULTS

Table 8, discusses the challenges along with frequency range. As discussed earlier, critical challenges are the ones whose frequency range is more than 10%. The formula for finding frequency is the total number of challenges identified in the 34 papers finally selected, multiplied with 100 and divided by the total number of papers, i.e., 34.

H. CHALLENGES IDENTIFICATION VIA THE SLR PROCESS RQ

A final sample of 34 papers are selected and data is summarized from them. A list of 6 challenges, as depicted in Table 8,

TABLE 8. List of the identified challenges.

S.No	Challenges	Frequency Out of N out of 34	%
1	Communication cost	16	47.06
2	Single point of failure	12	35.29
3	Detection probability	7	20.59
4	Memory or Storage Cost	5	14.71
5	Deterministic	3	8.82
6	Redundancy	1	2.94

were shortlisted through the SLR from that summarized data. Out of these 6 challenges, 4 were identified as critical according to 10% frequency criteria. Following is the description of those 6 challenges:

1) COMMUNICATION COST

Communication costs can be defined as the average number of location claims sent and received by every node during each iteration of a clone detection protocol. Communication cost is the most essential and important performance metric of clone detection protocols because during communication, sensors nodes consume more energy than any other operations in WSN's [69]. Table 8 indicates that ''Communication Cost'', having the highest frequency of 47.06% and can be labeled as the first challenge. Moreover, this research found that various detection protocols [27], [30], [32], [35], [36], [38], [42]–[44], [46], [47], [50], [53]–[55], [57] suffer from the challenge of high communication cost during the clone nodes detection process.

2) SINGLE POINT OF FAILURE

In a centralized scheme, all nodes in the network send their ID and location to a single trusted node (e.g., base station or sink), which checks for the conflict (i.e., the same ID with different locations) to detect the clone nodes in the network. The single trusted node introduces many challenges as it's neighboring nodes suffer from high communication cost and due to its important role in clone detection, this node becomes the prime target of the attackers. Therefore, failure of the single trusted node results in a single point of failure and most of the proposed centralized clone detection schemes are suffering from this challenge [2], [22], [25], [27]–[35]. According to Table 8, ''Single Point of Failure'', is found to be the second most quoted challenge having the frequency of 35.29%.

3) DETECTION PROBABILITY

Detection probability is defined as the total number of successful detection of clone nodes during each iteration of the protocol, divided by the total number of iterations of the protocol. High and successful detection probability is the most significant performance metric for any clone detection protocol. However, most of the proposed clone detection protocols suffer from low detection probability with high cost in terms of communication and memory [29], [33], [36], [38], [41], [56], [58]. This study concludes that ''Detection Probability'', with a frequency of 20.59%, can be regarded as the third-significant challenge in the clone node detection mechanism.

4) MEMORY/STORAGE COST

Memory cost can be described as the total number of location claims, that are stored by every node in the network during each iteration of the clone detection protocol. The low-cost wireless sensor nodes have limited resources in terms of energy and storage but on the other hand, for achieving a high clone detection rate, the clone detection protocols require large memory to store location claims. The fourth challenge, according to Table 8, is ''Memory or Storage Cost'', with a frequency of 14.71%. Therefore achieving high detection probability with lower memory cost is challenging and most of the current clone detection protocols suffer from high memory costs [27], [28], [42], [46], [48].

5) DETERMINISTIC SELECTION OF WITNESS NODES

The witness nodes are the most significant and fundamental elements in Claimer-Reporter-Witness based clone detection techniques as they are responsible for detecting clones in the network. The selection of these witness nodes is a very important and challenging task. If the selection of witnesses is deterministic, an enemy can easily identify, locate and comprise them to neutralize the detection process. In the literature, the selection of witness nodes in many proposed witness node based distributed schemes, [25], [34], [45] is deterministic. The study shows that ''Deterministic'' with a frequency of 8.82% is identified as a serious challenge in clone node detection techniques.

6) REDUNDANCY

In WSNs, nodes are heavily deployed in the area of interest to gather the required information. Sensors detect similar data and forward it to the sink. The reliable data is needed in the analysis, evaluation and predicting of system behavior while bad quality data can lead to inaccurate results in decision making. Such similar data can produce redundancy at the sink. The outcome of redundant data results in more accuracy, reliability and safety while elimination helps in energy saving, as most of the energy of the sink node, is wasted in dealing with the redundant data. However, data accuracy still needs to be well-kept even if there is an increase in network cost and/or time. Another challenge in the clone node detection technique is ''Redundancy'' with a frequency of 2.94% which is the absence of redundant data for the purpose of decision making [49].

IV. CONCLUSION

In this article, a systematic review of clone detection techniques was conducted. From the literature, it was found that due to the characteristics of the WSNs such as limited processing, memory, battery, lack of tamper resistance hardware etc., the sensor nodes are prone to various attacks such as

Papers	References	Respondents(R)	QA1	QA2	QA3	QA4	Points	Mean
P1	[2]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P2	[22]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P3	[25]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P4	[27]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P5	[28]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P6	[29]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P7	[30]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P8	[31]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P9	[32]	R1	0.5	1	0.5	1	3	3
		R2	0.5	1	1	0.5	3	
P10	[33]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P11	[34]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P12	[35]	R1	0.5	1	0.5	0.5	2.5	2.75
		R2	0.5	1	0.5	1	3	
P13	[36]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P14	[38]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P15	[39]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P16	[40]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P17	[41]	R1	1	1	0.5	1	4	3.5
		R2	1	1	0.5	1	4	
P18	[42]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P19	[43]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P20	[44]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P21	[45]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P22	[46]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P23	[47]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P24	[48]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P25	[49]	R1	0.5	1	1	1	3.5	3.5
		R2	1	1	1	0.5	3.5	
P26	[50]	R1	0.5	1	0.5	1	3	2.75
		R2	0.5	1	1	1	3.5	
P27	[52]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P28	[53]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P29	[54]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P30	[55]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P31	[56]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P32	[57]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P33	[58]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	
P34	[59]	R1	1	1	1	1	4	4
		R2	1	1	1	1	4	

clone node or node replication attack. To counter clone node attacks, different techniques such as network-based detection techniques, centralised based detection and distributed based detection techniques have been proposed. Some of the sub-techniques within centralised detection approach include key usage, base station, neighbourhood social signature, cluster head, zone and neighbour based techniques. Similarly, few potential clone detection techniques under a distributed based approach include node to network broadcasting, witness node, generation based techniques etc. Finally, the key challenges with respect to clone detection were highlighted.

APPENDIX
POINT TABLE OF QUALITY ASSESSMENT CRITERIA

Detailed scores of each selected paper of SLR against the questions of quality assessment criteria.

REFERENCES

[1] A. Kurniawan, "Introduction to wireless sensor networks," in *Practical Contiki-NG*. Berkeley, CA, USA: Springer, 2018, pp. 1–46.

[2] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir, "On the detection of clones in sensor networks using random key predistribution," *IEEE Trans. Syst., Man, Cybern. C, Appl. Rev.*, vol. 37, no. 6, pp. 1246–1258, Nov. 2007.

[3] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102–114, Aug. 2002.

[4] A. Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.

[5] J. R. Douceur, "The sybil attack," in *Proc. Int. Workshop Peer-to-Peer Syst.* Berlin, Germany: Springer, 2002, pp. 251–260.

[6] J. Newsome, E. Shi, D. Song, and A. Perrig, "The sybil attack in sensor networks: Analysis & defenses," in *Proc. 3rd Int. Symp. Inf. Process. sensor Netw. (IPSN)*, 2004, pp. 259–268.

[7] M. Demirbas and Y. Song, "An RSSI-based scheme for sybil attack detection in wireless sensor networks," in *Proc. Int. Symp. World Wireless, Mobile Multimedia Netw. (WoWMoM)*, 2006, p. 5.

[8] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. 19th Int. Conf. Data Eng.*, 2003, pp. 197–213.

[9] M. Conti, R. Di Pietro, and L. V. Mancini, "Secure cooperative channel establishment in wireless sensor networks," in *Proc. 4th Annu. IEEE Int. Conf. Pervas. Comput. Commun. Workshops (PERCOMW)*, Mar. 2006, p. 5.

[10] M. Conti, R. Di Pietro, and L. V. Mancini, "ECCE: Enhanced cooperative channel establishment for secure pair-wise communication in wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 49–62, Jan. 2007.

[11] R. D. Pietro, L. V. Mancini, and A. Mei, "Energy efficient node-to-node authentication and communication confidentiality in wireless sensor networks," *Wireless Netw.*, vol. 12, no. 6, pp. 709–721, Dec. 2006.

[12] R. di Pietro, L. V. Mancini, A. Mei, A. Panconesi, and J. Radhakrishnan, "Sensor networks that are provably resilient," in *Proc. Securecomm Workshops*, Aug. 2006, pp. 1–10.

[13] C. Hartung, J. Balasalle, and R. Han, "Node compromise in sensor networks: The need for secure systems," Dept. Comput. Sci., Univ. Colorado Boulder, Boulder, CO, USA, Tech. Rep. CU-CS-990-05, 2005.

[14] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," in *Proc. 1st IEEE Int. Workshop Sensor Netw. Protocols Appl.*, Sep. 2003, pp. 113–127.

[15] B. Parno, M. Luk, E. Gaustad, and A. Perrig, "Secure sensor network routing: A clean-slate approach," in *Proc. ACM CoNEXT Conf. (CoNEXT)*, 2006, p. 11.

[16] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in *Proc. IEEE Symp. Secur. Privacy*, May 2004, pp. 259–271.

[17] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 23, no. 4, pp. 839–850, Apr. 2005.

[18] L. Yu and J. Li, "Grouping-based resilient statistical en-route filtering for sensor networks," in *Proc. IEEE 28th Conf. Comput. Commun. (INFOCOM)*, Apr. 2009, pp. 1782–1790.

[19] C. Karlof, N. Sastry, and D. Wagner, "TinySec: A link layer security architecture for wireless sensor networks," in *Proc. 2nd Int. Conf. Embedded networked sensor Syst. (SenSys)*, 2004, pp. 162–175.

[20] A. Perrig, R. Szewczyk, J. D. Tygar, V. Wen, and D. E. Culler, "SPINS: Security protocols for sensor networks," *Wireless Netw.*, vol. 8, no. 5, pp. 521–534, Sep. 2002.

[21] S. Zhu, S. Setia, and S. Jajodia, "LEAP+: Efficient security mechanisms for large-scale distributed sensor networks," *ACM Trans. Sensor Netw.*, vol. 2, no. 4, pp. 500–528, Nov. 2006.

[22] H. Choi, S. Zhu, and T. F. La Porta, "SET: Detecting node clones in sensor networks," in *Proc. 3rd Int. Conf. Secur. Privacy Commun. Netw. Workshops (SecureComm)*, 2007, pp. 341–350.

[23] S. G. Thakur, "Cinora: Cell based identification of node replication attack in wireless sensor networks," in *Proc. IEEE Int. Conf. Commun. Syst. (ICCS)*, Dec. 2008, pp. 1–8.

[24] H. R. Shaukat, F. Hashim, A. Sali, and M. F. Abdul Rasid, "Node replication attacks in mobile wireless sensor network: A survey," *Int. J. Distrib. Sensor Netw.*, vol. 10, no. 12, Dec. 2014, Art. no. 402541.

[25] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "Distributed detection of clone attacks in wireless sensor networks," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 5, pp. 685–698, Sep. 2011.

[26] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, "A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks," in *Proc. 8th ACM Int. Symp. Mobile Ad Hoc Netw. Comput. (MobiHoc)*, 2007, pp. 80–89.

[27] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "CSI: Compressed sensing-based clone identification in sensor networks," in *Proc. IEEE Int. Conf. Pervas. Comput. Commun. Workshops*, Mar. 2012, pp. 290–295.

[28] T. Kenaza, O. N. Hamoud, and N. Nouali-Taboudjemat, "Efficient centralized approach to prevent from replication attack in wireless sensor networks," *Secur. Commun. Netw.*, vol. 8, no. 2, pp. 220–231, Jan. 2015.

[29] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, "Compressed sensing-based clone identification in sensor networks," *IEEE Trans. Wireless Commun.*, vol. 15, no. 4, pp. 3071–3084, Apr. 2016.

[30] P. Uma Maheswari and P. Ganesh Kumar, "Dynamic detection and prevention of clone attack in wireless sensor networks," *Wireless Pers. Commun.*, vol. 94, no. 4, pp. 2043–2054, Jun. 2017.

[31] K. Xing, F. Liu, X. Cheng, and D. H. C. Du, "Real-time detection of clone attacks in wireless sensor networks," in *Proc. 28th Int. Conf. Distrib. Comput. Syst.*, Jun. 2008, pp. 3–10.

[32] W. Naruephiphat, Y. Ji, and C. Charnsripinyo, "An area-based approach for node replica detection in wireless sensor networks," in *Proc. IEEE 11th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Jun. 2012, pp. 745–750.

[33] W. Znaidi, M. Minier, and S. Ubéda, "Hierarchical node replication attacks detection in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 9, no. 4, Apr. 2013, Art. no. 745069.

[34] A. K. Mishra and A. K. Turuk, "A zone-based node replica detection scheme for wireless sensor networks," *Wireless Pers. Commun.*, vol. 69, no. 2, pp. 601–621, Mar. 2013.

[35] P. Abinaya and C. Geetha, "Dynamic detection of node replication attacks using X-RED in wireless sensor networks," in *Proc. Int. Conf. Inf. Commun. Embedded Syst. (ICICES)*, Feb. 2014, pp. 1–4.

[36] B. Parno, A. Perrig, and V. Gligor, "Distributed detection of node replication attacks in sensor networks," in *Proc. IEEE Symp. Secur. Privacy*, Oakland, CA, USA, 2005, pp. 49–63.

[37] B. Zhu, V. G. K. Addada, S. Setia, S. Jajodia, and S. Roy, "Efficient distributed detection of node replication attacks in sensor networks," in *Proc. 23rd Annu. Comput. Secur. Appl. Conf. (ACSAC)*, Dec. 2007, pp. 257–267.

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

[39] M. Zhang, V. Khanapure, S. Chen, and X. Xiao, "Memory efficient protocols for detecting node replication attacks in wireless sensor networks," in *Proc. 17th IEEE Int. Conf. Netw. Protocols*, Oct. 2009, pp. 284–293.

[40] Z. Li and G. Gong, "Randomly directed exploration: An efficient node clone detection protocol in wireless sensor networks," in *Proc. IEEE 6th Int. Conf. Mobile Adhoc Sensor Syst.*, Oct. 2009, pp. 1030–1035.

[41] C. Kim, S. Shin, C. Park, and H. Yoon, "A resilient and efficient replication attack detection scheme for wireless sensor networks," *IEICE Trans. Inf. Syst.*, vols. E92–D, no. 7, pp. 1479–1483, 2009.

[42] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, "Random-walk based approach to detect clone attacks in wireless sensor networks," *IEEE J. Sel. Areas Commun.*, vol. 28, no. 5, pp. 677–691, Jun. 2010.
[43] X. Meng, K. Lin, and K. Li, "A note-based randomized and distributed protocol for detecting node replication attacks in wireless sensor networks," in *Proc. Int. Conf. Algorithms Archit. Parallel Process.* Berlin, Germany: Springer, 2010, pp. 559–570.
[44] Z. Li and G. Gong, "On the node clone detection in wireless sensor networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 6, pp. 1799–1811, Dec. 2013.
[45] Y. Zhou, Z. Huang, J. Wang, R. Huang, and D. Yu, "An energy-efficient random verification protocol for the detection of node clone attacks in wireless sensor networks," *EURASIP J. Wireless Commun. Netw.*, vol. 2014, no. 1, p. 163, Dec. 2014.
[46] W. Z. Khan, M. Y. Aalsalem, and N. M. Saad, "Distributed clone detection in static wireless sensor networks: Random walk with network division," *PLoS ONE*, vol. 10, no. 5, 2015, Art. no. e0123069.
[47] M. Y. Aalsalem, W. Z. Khan, N. M. Saad, M. S. Hossain, M. Atiquzzaman, and M. K. Khan, "A new random walk for replica detection in WSNs," *PLoS ONE*, vol. 11, no. 7, 2016, Art. no. e0158072.
[48] Z. Zheng, A. Liu, L. X. Cai, Z. Chen, and X. Shen, "Energy and memory efficient clone detection in wireless sensor networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 5, pp. 1130–1143, May 2016.
[49] J. S. Cynthia and D. S. Punithavathani, "Clone attack detection using pair access witness selection technique," *Int. J. Comput. Netw. Appl.*, vol. 3, no. 5, pp. 118–128, 2016.
[50] D. R. Kumar and A. Shanmugam, "A hyper heuristic localization based cloned node detection technique using gsa based simulated annealing in sensor networks," in *Cognitive Computing for Big Data Systems Over IoT*. Cham, Switzerland: Springer, 2018, pp. 307–335.
[51] C. Bekara and M. Laurent, "Defending against nodes replication attacks on wireless sensor networks," in *Proc. 2nd Conf. Secur. Netw. Archit. Inf. Syst. (SAR-SSI)*. Lyon, France: Université Jean Moulin, 2007, pp. 31–40.
[52] C. Bekara and M. Laurent-Maknavicius, "A new protocol for securing wireless sensor networks against nodes replication attacks," in *Proc. 3rd IEEE Int. Conf. Wireless Mobile Comput., Netw. Commun. (WiMob)*, Oct. 2007, p. 59.
[53] 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 Netw.*, vol. 7, no. 8, pp. 1476–1488, Nov. 2009.
[54] Y. Sei and S. Honiden, "Distributed detection of node replication attacks resilient to many compromised nodes in wireless sensor networks," in *Proc. 4th Int. ICST Conf. Wireless Internet*, 2008, p. 28.
[55] L.-C. Ko, H.-Y. Chen, and G.-R. Lin, "A neighbor-based detection scheme for wireless sensor networks against node replication attacks," in *Proc. Int. Conf. Ultra Modern Telecommun. Workshops*, Oct. 2009, pp. 1–6.
[56] G. Cheng, S. Guo, Y. Yang, and F. Wang, "Replication attack detection with monitor nodes in clustered wireless sensor networks," in *Proc. IEEE 34th Int. Perform. Comput. Commun. Conf. (IPCCC)*, Dec. 2015, pp. 1–8.
[57] M. Dong, K. Ota, L. T. Yang, A. Liu, and M. Guo, "LSCD: A low-storage clone detection protocol for cyber-physical systems," *IEEE Trans. Comput.-Aided Design Integr. Circuits Syst.*, vol. 35, no. 5, pp. 712–723, May 2016.
[58] G. Amudha and P. Narayanasamy, "Distributed location and trust based replica detection in wireless sensor networks," *Wireless Pers. Commun.*, vol. 102, no. 4, pp. 3303–3321, Oct. 2018.
[59] F. Pan, Z. Pang, M. Xiao, H. Wen, and R.-F. Liao, "Clone detection based on physical layer reputation for proximity service," *IEEE Access*, vol. 7, pp. 3948–3957, 2019.
[60] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," EBSE, Durham, U.K, Tech. Rep., 2007.
[61] M. Salam and S. U. Khan, "Systematic literature review protocol for green software multi-sourcing with preliminary results," *Proc. Pakistan Acad. Sci.*, vol. 52, no. 52, pp. 285–300, 2015.
[62] M. Yaseen, S. U. Khan, and A. U. Alam, "Software multi-sourcing risks management from vendor's perspective: A systematic literature review protocol," *Gomal Univ. J. Res.*, vol. 29, no. 2, pp. 1–8, 2013.
[63] M. Staples and M. Niazi, "Experiences using systematic review guidelines," *J. Syst. Softw.*, vol. 80, no. 9, pp. 1425–1437, Sep. 2007.
[64] M. Niazi, S. U. Khan, S. Imtiaz, M. Bano, and N. Ikram, "Establishing trust in offshore software outsourcing relationships: An exploratory study using a systematic literature review," *IET Softw.*, vol. 7, no. 5, pp. 283–293, Oct. 2013.
[65] M. Ilyas and S. U. Khan, "Software integration in global software development: Success factors for GSD vendors," in *Proc. IEEE/ACIS 16th Int. Conf. Softw. Eng., Artif. Intell., Netw. Parallel/Distrib. Comput. (SNPD)*, Jun. 2015, pp. 1–6.
[66] W. Alsaqaf, M. Daneva, and R. Wieringa, "Quality requirements in large-scale distributed agile projects—A systematic literature review," in *Proc. Int. Work. Conf. Requirements Eng., Found. Softw. Qual.* Cham, Switzerland: Springer, 2017, pp. 219–234.
[67] S. Mahmood, S. Anwer, M. Niazi, M. Alshayeb, and I. Richardson, "Identifying the factors that influence task allocation in global software development: Preliminary results," in *Proc. 19th Int. Conf. Eval. Assessment Softw. Eng.*, 2015, p. 31.
[68] S. U. Khan, M. Niazi, and R. Ahmad, "Barriers in the selection of offshore software development outsourcing vendors: An exploratory study using a systematic literature review," *Inf. Softw. Technol.*, vol. 53, no. 7, pp. 693–706, Jul. 2011.
[69] D. Estrin, R. Govindan, J. Heidemann, and S. Kumar, "Next century challenges: Scalable coordination in sensor networks," in *Proc. 5th Annu. ACM/IEEE Int. Conf. Mobile Comput. Netw. (MobiCom)*, 1999, pp. 263–270.

MUHAMMAD NUMAN received the B.S.C.S. degree from Shaheed Benazir Bhutto University, Sheringal, Dir Upper, Pakistan, in 2015, and the M.S.C.S. degree from the National University of Modern Languages, Islamabad, Pakistan, in 2020. He worked as a Research Assistant with Dr. F. Subhan, where he was involved with advanced research projects. His current research interests include wireless sensor networks, the Internet of Things (IoT), and the Internet of robotic things (IoRT) and its security.

FAZLI SUBHAN received the M.Sc. degree in computer science from the University of Peshawar, Pakistan, in 2003, and the Ph.D. degree in information technology from Universiti Teknologi PETRONAS, Malaysia, in 2012. He is currently working as an Assistant Professor with the Department of Computer Science, National University of Modern Languages (NUML), Islamabad, Pakistan. His research interests include indoor positioning systems, wireless sensor networks, machine learning, and software engineering.

WAZIR ZADA KHAN (Senior Member, IEEE) received the bachelor's and master's degrees in computer science from COMSATS University Islamabad, Wah Campus, in 2004 and 2007, respectively, and the Ph.D. degree from the Electrical and Electronic Engineering Department, Universiti Teknologi PETRONAS, Malaysia, in 2015. He is currently working with the Farasan Networking Research Laboratory, Faculty of CS and IT, Jazan University, Saudi Arabia. His current research interests include wireless sensor networks, security and privacy, and the IoT.

SAQIB HAKAK received the bachelor's degree in computer science engineering from the University of Kashmir, India, in 2010, and the master's degree in computer and information engineering from IIUM, Malaysia, and the Ph.D. degree from the Faculty of Computer Science and Information Technology, University of Malaya, Malaysia. He is currently working as an Assistant Professor with the University of Northern British Columbia, Canada. Prior to this designation, he worked as a Postdoctoral Research Fellow with the prestigious Canadian Institute for Cyber-Security. His research interests include information security, natural language processing, cyber security, artificial intelligence, and wireless networks.

SAJJAD HAIDER is currently working as an Assistant Professor with the Department of Computer Science, National University of Islamabad, Pakistan. He has authored or coauthored many publications in prominent journals. His research interests include parallel and distributed computing, the IoT, and wireless sensor networks.

G. THIPPA REDDY received the B.Tech. degree in CSE from Nagarjuna University, the M.Tech. degree in CSE from Anna University, Chennai, India, and the Ph.D. degree from VIT, Vellore, India. He is currently working as an Assistant Professor (Senior) with the School of Information Technology and Engineering, VIT. He has 14 years of experience in teaching. He produced more than 25 international/national publications. He is currently working in the area of machine learning, deep neural networks, the Internet of Things, and blockchain.

ALIREZA JOLFAEI (Senior Member, IEEE) received the Ph.D. degree in applied cryptography from Griffith University, Gold Coast, Australia. He is currently a Lecturer (Assistant Professor in North America) and a Program Leader of cyber security with Macquarie University, Sydney, Australia. Prior to this appointment, he worked as an Assistant Professor with Federation University Australia and Temple University, Philadelphia, USA. His current research interests include cyber security, the IoT security, human-in-the-loop CPS security, cryptography, AI, and machine learning for cyber security. He has authored over 60 peer-reviewed articles on topics related to cyber security. He has received multiple awards for Academic Excellence, University Contribution, and Inclusion and Diversity Support. He received the prestigious IEEE Australian Council Award for his research article published in the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He received the recognition diploma with Cash Award from the IEEE Industrial Electronics Society for his publication at the 2019 IEEE IES International Conference on Industrial Technology. He is the Founding Member of Federation University IEEE Student Branch. He served as the Chairman of Computational Intelligence Society in IEEE Victoria Section and the Chairman of Professional and Career Activities for the IEEE Queensland Section. He has served as the Guest Associate Editor of the IEEE journals and Transactions, including the IEEE IoT JOURNAL, the IEEE SENSORS JOURNAL, the IEEE TRANSACTIONS ON INDUSTRIAL APPLICATIONS, the IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, and the IEEE TRANSACTIONS ON EMERGING TOPICS IN COMPUTATIONAL INTELLIGENCE. He has served over ten conferences in leadership capacities, including a Program Co-Chair, a Track Chair, a Session Chair, and a Technical Program Committee Member, including the IEEE TrustCom and the IEEE INFOCOM. He is an ACM Distinguished Speaker on the topic of Cyber-Physical Systems Security.

MAMOUN ALAZAB (Senior Member, IEEE) received the Ph.D. degree in computer science from the School of Science, Information Technology, and Engineering, Federation University of Australia. He is currently an Associate Professor with the College of Engineering, IT, and Environment, Charles Darwin University, Australia. He is currently a Cyber Security Researcher and a Practitioner with industry and academic experience. His research is multidisciplinary that focuses on cyber security and digital forensics of computer systems with a focus on cybercrime detection and prevention, including cyber terrorism and cyber warfare. He has more than 100 research articles. He delivered many invited and keynote speeches, 22 events, in 2018 alone. He convened and chaired more than 50 conferences and workshops. He works closely with government and industry on many projects, including Northern Territory (NT) Department of Information and Corporate Services, IBM, Trend Micro, the Australian Federal Police (AFP), the Australian Communications and Media Authority (ACMA), Westpac, United Nations Office on Drugs and Crime (UNODC), and the Attorney General's Department. He is the Founder and a Chair of the IEEE Northern Territory (NT) Subsection.