International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 29, No. 3, June, 2024, pp. 1161-1174
Journal homepage: http://iieta.org/journals/isi

Node Clone Detection Protocols for Protect the WSNs: A Survey

Karrar Alkhafagee[1*], Aladdin Abbas Alsharifi[2]

[1] Department of Software, College of Information Technology, University of Babylon, Al Hilla 51001, Iraq
[2] Department of Information Networks, College of Information Technology, University of Babylon, Al Hilla 51001, Iraq

Corresponding Author Email: karrarma.sw.msc@student.uobabylon.edu.iq

https://doi.org/10.18280/isi.290333

Received: 14 August 2023
Revised: 21 January 2024
Accepted: 10 April 2024
Available online: 20 June 2024

Keywords:
node clone, cloning attack detection, security attacks, Wireless Sensor Network s(WSNs), static and mobile nodes, centralized and distributed detection protocols

ABSTRACT

The aim of this survey is to limit the largest number of these techniques in one place in the form of tables in order for the researcher to distinguish between them and know the extent of their benefits and disadvantages, as well as in order for the researcher to avoid falling into these defects as much as possible when he makes his own cloned contract detection system. In this paper, we have conducted a comprehensive review of the collection of several techniques for detecting centralized and distributed replication attacks, where nodes can be static or mobile sensor nodes, and tables were made summarizing what was mentioned in these techniques, each according to the results reached by the researchers. A Wireless Sensor Network (WSN) is a system of self-contained sensor nodes that monitor environmental (or physical) parameters with limitations on battery life, memory capacity, and computational power. WSNs are open to several types of attacks due to their use in unmoderated and insecure contexts. Cloning attacks, or (replication attacks), are a type of physical attack. A network adversary can quickly control a single node and collect data from it. Then reprogram it to make a copy of the captured node. Identifying a duplicate node becomes difficult once these clones are spread throughout the network and are accepted as original nodes. A technology or (protocol) must be found that ideally prevents the node from being cloned, as researchers have not been able to create a 100% secure system to prevent the effects of node cloning, which include network traffic monitoring, sensor spoofing, mock data injection, sabotage of data collection, signal jamming, denial-of-service attacks, and disrupting network tasks. Creating a comparison table between techniques for preventing node cloning provides many benefits, including quickly finding the appropriate technique. It is considered a comprehensive and quick-access reference. It facilitates the decision-making process and prevents making mistakes that researchers made previously. It provides visual assistance for analyzing the strengths and weaknesses of each technique in an easier and faster way. The researcher was able to choose the most appropriate technology to develop and improve the quality of its performance to reach the ideal technology in future works.

1. INTRODUCTION

The main security targets of WSNs include confidentiality, authenticity, data integrity, and availability [1]. The network is unreliable and unsuitable for further connections when the enemy launches node-clone attacks, as all of these security objectives are affected. This is due to two reasons, the first of which is that proper detection protocols are not available and are not effective for identifying and nullifying attacks. Secondly, the probability offered by some detection systems is negligible [2]. Much damage to the network due to a node cloning attack since it is considered a real node by its neighbor and can participate in network operations using encryption keys. The major purpose of the adversary's creation of these clones is to perform a variety of insider attacks, including network traffic monitoring, sensor spoofing, mock data injection, sabotage of data collection, signal jamming, denial-of-service attacks, and disrupting network tasks [3].

The cloned node initially launches a variety of malicious attacks (also called malicious nodes) into the network. The cloned node contains its legitimate information (identifier and encryption keys) and is involved in network operations being a non-compromised node [4]. Figure 1 shows the details [5].

To evaluate the performance of various node-clone detection protocols, many items are involved in the evaluation process. The main items include connection costs, storage expenses, security of data, probability and time-detection, cost and maintenance, power level and utilization, delivery-rate, end-to-end delay, service quality, packet loss, and so on. They are the following [4]:

(1) Communication cost: It is the average number of messages sent by nodes when verifying site claims.

(2) Storage cost: It is calculated by the sensor node by the number of stored location claims.

(3) Data security: This refers to preventing unauthorized users from illegally using data.

(4) Likelihood of detection: How much a measure of the accuracy of a detection protocol in identifying and detecting

clones.

(5) Discovery time: It is the rate of time that passes between the publication of a clone and its discovery in the network.

(6) Data Delivery Cost: It is the cost factor incurred to deliver the packet from the source node to the destination.

(7) Energy efficiency: It is the minimum amount of energy used by a node to direct the beam to the desired location.

(8) Rate of Delivery: It is calculated by dividing the ratio of the number of packets received by total number of packets sent.

(9) Amount of lost packets: Due to congestion or network failure, some of the packets are lost. The number of packets that failed to arrive at the destination.

(10) Avoidance: the canceling of something by an authority [4].

These selection criteria are based on their relevance to node-clone detection protocol performance and their potential to highlight the advantages and disadvantages of various strategies. Considerations such as communication and storage costs are critical when examining a protocol's scalability, and data security and detection probability are essential for determining a protocol's efficacy in thwarting node-clone attacks. In a similar vein, assessing a protocol's performance with regard to power consumption and data transfer requires consideration of energy efficiency and delivery rate. All things considered, the assessment items offer a thorough framework for evaluating the efficacy of node-clone detection procedures and can aid in directing the choice and application of suitable strategies for thwarting node-clone attacks in WSNs.

The Wireless Sensor Networks (WSNs) security objectives are as follows [4]:

(1) Availability: It ensures that network services are accessible even while under assault. The enemy attempts to undermine Provides network services by disrupting its operations due to a node-cloning attack.

(2) Authenticity: This term typically specifies the identities of the nodes taking part in network communication. It is challenging to recognize between a clone and an original/legitimate node as a result of a node clone attack because the clone has the same basic information as the parent node.

(3) Confidentiality: guarantees safe data transfer between trusted nodes. Due to node clone attacks, where the cloned-node mimics the behavior of a normal node, people attempt to abuse the data carried through networks, turning private information into public information.

(4) Data integrity: It gives a guarantee of data reliability and immutability it is used to communicate between nodes. Because of the node-clone attack, the enemy can cram wrong data, reprogram node code, forge data, and so on, which makes the data unreliable for transmission [4].

Node cloning compromises the security objectives of WSNs in several cases:

a. It undermines the availability of network services by disrupting its operations due to a node-cloning attack.

b. It challenges the authenticity of the identities of the nodes taking part in network communication, making it difficult to differentiate between a clone and an original/legitimate node.

c. It compromises the confidentiality of data transfer between trusted nodes, as node clone can mimic the behavior of a normal node and abuse the data carried through networks, turning private information into public information.

d. It impacts the data integrity of the network by cramming wrong data, reprogramming node code, forging data, and so on, which makes the data unreliable for transmission.

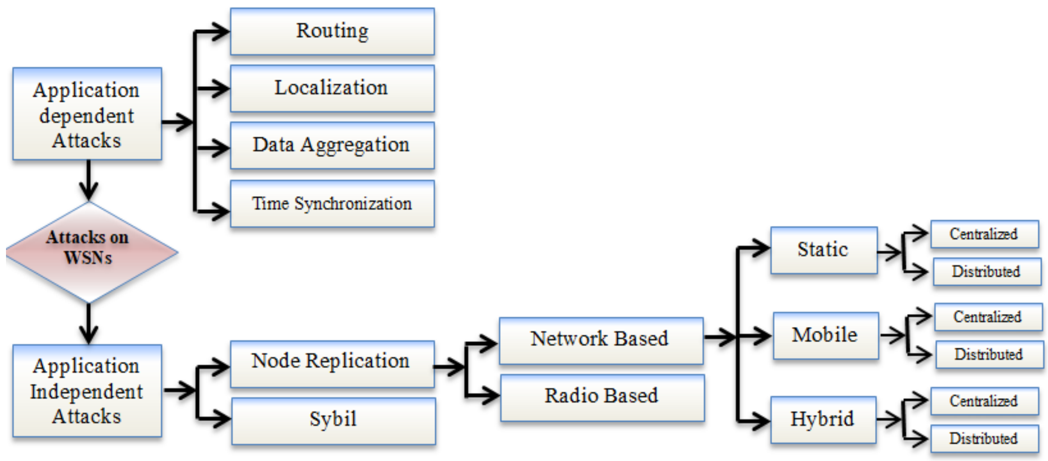

Figure 1. Taxonomy of attacks on WSNs [5]

2. CATEGORY OF SELECTION CRITERIA

The four types of detection systems are used to gather and validate clone evidence. These are the type of device, the mechanism of detection, the deployment techniques, and the detection range. Each was grouped as depicted in Figure 2 [6]. The type of device is further divided into (static, mobile, and hybrid) in the selection criteria, while the detection mechanism is divided into (centralized, distributed, and hybrid). Finally, deployment tactics are once more divided into two categories: random uniform and grid. The detecting range is finally divided into entire and local categories [6]. Figure 2 shows the details.

2.1 Type of devices (Static, Mobile, Hybrid)

The sensor network is classified according to the type of devices as static, mobile, and hybrid in nature. Sensor nodes are randomly deployed in the static state, and their location does not change after deployment and is called (static). As for the mobile, the sensor nodes move on their own even after they are deployed, and by controlling their movement, they interact with the physical environment [6]. From my point of view and other reverences such as [7], a third type can be created, which is a hybrid WSN, which is a mixture of static and mobile devices in the same network. It can be used in a single network if the environment is a forest where the network monitors fire occurrences, or in a battle environment that requires, for example, a temperature sensor. Additionally, we might need a mobile drone equipped with a camera to film the scene and send the footage to the server, resulting in a hybrid Wireless Sensor Network (WSN). Static devices have the advantage of being more accurate and dependable than mobile ones. A mobile gadget, on the other hand, is more adaptable and location-neutral. The benefits of both stationary and mobile devices are combined in a hybrid device. Using a stationary device has the drawback of being less flexible than using a mobile one. Because of its mobility, a mobile device might be less accurate, and because of its complexity, a hybrid device might be more expensive.

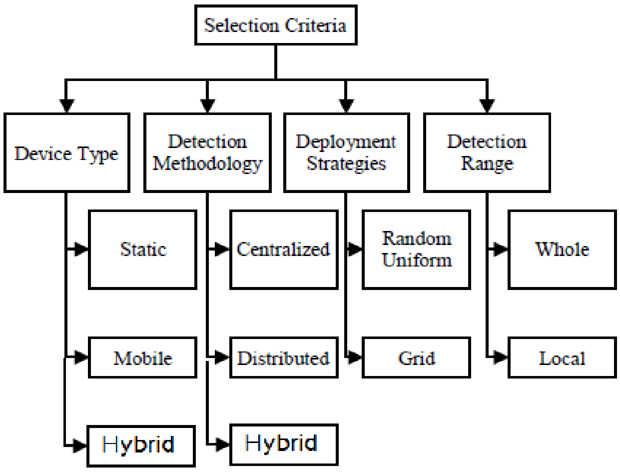

Figure 2. Taxonomy of selection criteria [6]

2.2 Methodology of detection (centralized, distributed and hybrid)

In the centralized network, a node is responsible for the security of the network, but in the distributed network, each node is responsible for its security. The above two types can be combined into one network called a hybrid [8]. Using a centralized system has the benefit of being simpler to administer and control. On the other hand, a distributed approach can manage large-scale systems and is more fault-tolerant. The benefits of both distributed and centralized methods are combined in a hybrid mechanism. A centralized method may have a single point of failure, which is a drawback. There could be more complexity and communication overhead in a distributed system. In previous research, comparisons were made between centralized and distributed technologies in terms of: cost, power consumption, Accuracy, Dependency on additional hardware and Deployability [9]. A hybrid system combines the benefits of distributed and centralized systems. In some situations, it may be more efficient than a distributed or centralized system, including:

(1) Constraints on resources: A hybrid system can effectively spread the load between its dispersed and centralized components in Wireless Sensor Networks (WSNs) with limited resources.

(2) Scalability: Due to its capacity to split the workload among several nodes and lessen the stress on individual nodes, a hybrid system can scale more effectively than a centralized or distributed system.

(3) Fault tolerance: Because a hybrid system can keep running even if some of its nodes or components fail, it can offer superior fault tolerance than a centralized or distributed system.

(4) Energy efficiency: Because a hybrid system may optimize each node's energy usage while lowering overall energy consumption, it may be more energy-efficient than a centralized or dispersed system.

2.3 Deployment strategies (Random, Grid)

The grid will perform better upon deployment than the random. The grid deployment ensures non-determinism and is useful in shielding the enemy from intelligent attack. The study is made simpler by the grid-based torus structure; It is a network diagram that dominates all directions north, south, east and west. A grid-based implementation offers great connectivity and resilience. The random deployment situation in some protocols results in significant collision probability and consequently somewhat high storage costs [6]. Using a random uniform deployment strategy has the benefit of being straightforward and simple to put into practice. On the other side, a grid deployment strategy is more organized and has a wider coverage area. A random uniform deployment strategy has the drawback of potentially missing some places. A grid rollout strategy could be more expensive and complicated. A random uniform deployment approach could be preferable to a grid deployment approach in specific circumstances. For instance, a random uniform deployment approach might be more successful in covering all areas if the deployment area involves obstacles or is shaped unevenly. Furthermore, compared to a grid deployment method, a random uniform deployment technique might be more affordable and simpler to execute. Nonetheless, a grid deployment method might outperform a random uniform deployment strategy when it comes to preventing node clones. This is so that node clones may be detected and prevented more successfully. A grid deployment method offers improved coverage and connection. Furthermore, because a grid deployment method is less susceptible to sophisticated attacks and more structured, it can offer greater resilience against them.

2.4 Detection range (whole, local)

Since location claims are relayed to many zones and a strong attacker could corrupt an entire zone, the WSN network necessitates a higher communication cost. The localization strategy necessitates focused attention on the local area with no need to consider the network as a whole. Thus, the cost of communication and computation may be decreased [6]. It can cover a bigger area and detect more clones when the entire detection range is used. In contrast, a local detection range can yield more precise results because it is more targeted. Using the whole detection range has the potential drawback of increased complexity and expense. Certain clones outside of a local detection range may go unnoticed by the range. There is a risk of missing localized or specific events, as the detection range may not be focused on specific target locations [10]. In WSNs, there are trade-offs between whole-network and local detection algorithms in terms of resource consumption, accuracy, and scalability. Although whole-network detection techniques might offer more thorough coverage, they might not scale well for big WSNs and might need more resources. Although local detection techniques might not cover the whole network, they might yield more accurate results and aid in resource conservation. The particulars of the application and the resources at hand determine which of these approaches is best.

3. CLONE DETECTION PROTOCOLS

In this study, we will discuss the detection methodology of protection (sometimes called techniques, methodologies, or schemes) from node cloning attacks in WSNs from literature, which are of two types, central and distributed, as follows:

3.1 Clone-detection protocols in static WSNs

There are many protocols designed to detect replication of nodes in static WSNs that can be classified into work-centric and distributed-work protocols [5].

3.1.1 Centralized clone detection protocols in static WSNs

These technologies rely mainly on a strong base station “BS” regardless of being complex and having low overhead costs, for decision-making and information convergence, nodes send their location claims to the base station with the help of their neighbors. If a single identifier is found in more than one location and when the base station verifies the node identifiers, a cloning attack alert message is generated. These protocols are able to discover cloned nodes. But the sensor information remains unsecured, as the enemy can perform sabotage operations and spy on the information transmitted between the sensor node and the sink. In addition, the life of the network ends quickly because the nodes close to the basin node lose their energy quickly, depending on the capacity of their battery. Central detection techniques for static WSNs can be classified into one of the categories listed below, and their comparison is shown in Table 1 [5].

3.1.2 Distributed clone detection protocols in static WSNs

Replication detection differs from centralization in that each node in the network is responsible for its own security, which means that there is no central node of the authority designated to do the work. Even nodes in remote locations in the network participate in this task. Focusing on static wireless networks, there are several different types of detection techniques or schemes that we will mention in detail below and their comparison is shown in Table 1 [5], and Figure 3 shows the details of protocols.

Table 1 explains the details of Figure 3, which includes some of the protocols proposed by the researchers within the mentioned sources, each according to his calculations for the purpose of preventing or repelling exposure to the attack of cloning nodes in WSNs, which we highlighted some of the important ones, as well as we mentioned their costs, advantages and disadvantages, so that the researcher does not make mistakes and also develops Its work is based on it, and it includes protocols for static node networks.

3.2 Clone detection protocols in mobile WSNs

Recently, mobile nodes have been used significantly within WSN. Because it plays a major role in implementing some needs in the network, in which it is needful for the nodes to be mobile to solve problems and provide many advantages over static wireless networks. Since static network protocols are not feasible and ineffective for detecting clones in mobile nodes, it has become necessary to develop and study some techniques for mobile WSNs to detect cloned nodes. These technologies are categorized into two main categories, centralized and distributed, and are detailed in Table 2.

3.3 Other clone detection protocols in WSNs

The way these protocols work is hybrid (centralized and distributed at the same time) and does not depend on any of the rules that we have discussed previously. Table 3 below explains more.

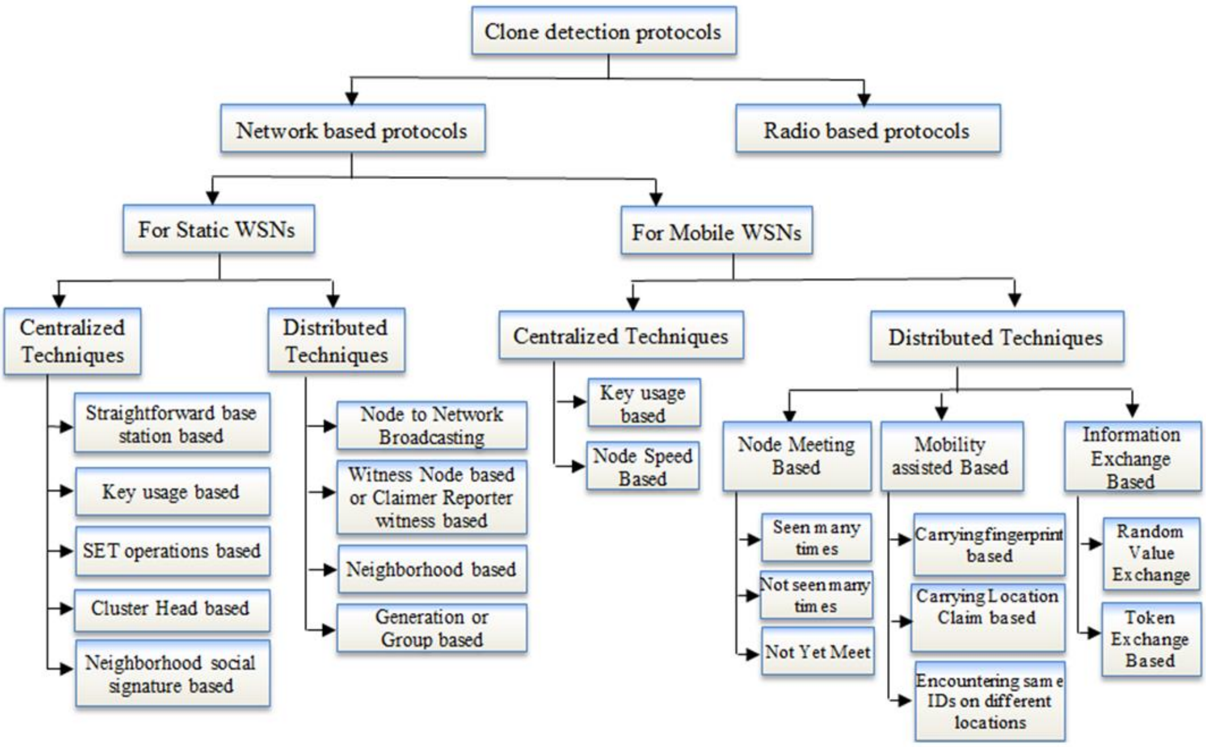

Figure 3. Taxonomy of clone detection protocols [11]

Table 1. Node clone detection protocols in static WSNs [5]

Protocol-based	Protocol Name	Cost of Communication	Cost of Memory	Its Advantages	Its Drawbacks	Detection Methodology
Key-usage based	Bloom Filter (PF) or called (Brooks et al. [12])	O (n log (n))			The high rate of false positives and negatives, and how to ensure that cloned nodes do not reliably communicate their credentials to the base station.	Centralized
Base station based	SET [13]	O (n)	O (d)	Independent site, low general memory	Single point of failure, Costly. This protocol is very complex because its components are complex. The enemy can cancel the original nodes with this protocol [14].	Centralized
	RED [15-19, 20]	O ($\sqrt{n}$)	O ($d\sqrt{n}$)	High detection ratio, low memory cost, unified Uniform distribution of witnesses due to "pseudo-random selection of witnesses contract"	Deterministic, Need a trusted entity.	Centralized
	CSI-1 [11, 21]	O (n log (n))	O (log (n))	High probability of detecting cloned nodes	Suffers from high communication and storage costs	Centralized
	CSI-2 [21]	O (n)	O (1)	It has low communication and storage costs less than CSI-1.	The detection probability of clone nodes is low.	Centralized
	Kenaza et al. [22]	Summation of (BS*NS) to Trans & Response	Two keys.	A clone detection rate is high.	It is not scalable and has other common drawbacks of centralized solutions.	Centralized
	PVM-MVP [23]	O (N^2)	O (N)	Its accuracy is high in detecting cloned nodes.	Network throughput is higher due to lower network life, time consuming and cost-effective.	Centralized
Neighborhood social signature-based	Real-time detection Scheme (RTD) by: Xing et al. [24]	C. (1 + ratio)	O (d) + min (M, w.log2 M)	Computational cost is low.	It could check itself for a fingerprint that matched the area in its vicinity because it couldn't handle an advanced clone [14].	Centralized
Cluster head based	LNCA and Bloom Filter [6]	O (t^2)	O (t)	Lower communication overhead	Lower detection probability.	Centralized
	ABCD [25]	O (n log (n))	O (n)	The detection rate of cloned nodes is high.	High communication cost, single point of failure, reduces network life-time.	Centralized
	SWBC [26]			Communication overhead is reduced. The detection rate is successful.	It needs a lot of storage space because the number of saved messages after detecting the enemy attack rate is greater when compared to RED and LSM.	Centralized
Zone based	ZBNRD [20]	O ($N \cdot \sqrt{nZ}$)+ O ($N z \cdot \sqrt{N}$)	O (d) / O (nZ)	The detection of cloned nodes is dynamic.	Be deterministic.	Centralized
Neighbor ID based	X-RED [27]	O (n log (n))	O (n)	Higher detection probability, and low memory cost.	The traffic overhead is large.	Centralized
Node to network broadcasting	N2NB [28] or called Broadcast protocol (BP) [14]	O (n^2)	O (d)	Relatively acceptable communication cost if the network is small and provides a more efficient detection	The larger the network, the greater the communication cost.	Distributed

				amount than centralized methods.		
Witness node-based	DM [11, 28]	O (g log($\sqrt{n}$ / d)	O (g)	Lowers communication costs	Less security.	Distributed
	RM [11, 20, 28]	O (n^2)	O ($\sqrt{n}$)	With enhanced flexibility, witnesses are difficult to predict.	It has lower detection probability, and high communication cost as well.	Distributed
	LSM [11, 20, 28]	O ($n\sqrt{n}$)	O ($\sqrt{n}$)	- Better detection probability - Improved communication cost - It is distinguished from RM by lower connection cost and better memory efficiency.	He has two problems, the crowded center problem, and the crossover problem.	Distributed
	LM [6]: (SDC & P-MPC [29, 30])	O (r.$\sqrt{n}$) + O(s)	O (ω) Or: O(1) [30]	More efficient discovery than LSM and low memory	Its reliance on the trusted entity and the amount of cell size. Communication cost (when the size of the cell is larger because if the size of the cell is smaller the node can be hacked easily).	Distributed
	B-MEM [11, 29]	O ($k.n.\sqrt{n}$)	O (tk + t′ k$\sqrt{n}$)	Good detection probability, less memory	Location dependent.	Distributed
	BC-MEM [11, 29]		O (tk + t′ k $\sqrt{n'}$)	Solve the problems of crowded centers and crossover that LSM was suffering from. Less storage space, and a high probability of detection	Location dependent.	Distributed
	C-MEM [11, 29]		O (t + t′ $\sqrt{n}$)		Location dependent.	Distributed
	CC-MEM [11, 29]		O (t + t′ $\sqrt{n}$)		Location dependent.	Distributed
	RDE [11, 31]	O ($d.n.\sqrt{n}$)	O (d)	Less memory consumption	It is not suitable for dynamic topological scenarios.	Distributed
	Chano KIM [32]	O ($\sqrt{n}$)	O ($\sqrt{n}$)	The number decreases in contact messages.	No promising results in node cloning attack detection.	Distributed
	RAWL [11, 19, 33]	O ($\sqrt{n}$ log (n)) or O (n$\sqrt{n}$) if a large network	O ($\sqrt{n}$ log(n)) or O($\sqrt{n}$) if a large network	High detection probability	Memory and communication costs are large.	Distributed
	TRAWL [11, 19]	O ($\sqrt{n}$ log(n))	O ($(1^2)^2$)	High detection probability	High connection cost.	Distributed
	NRDP [11, 17]	O (N.g($\sqrt{N}$)	O (g)	Share group membership information most simply.	Choosing a correspondent contract costs additional expenses.	Distributed
	DHT [33, 34]	O (log n $\sqrt{n}$)	O (d)	Provides effective clone detection probability.	Higher communication cost.	Distributed
	GDL and RMC [35]	O ($\sqrt{1}$×$\sqrt{m}$ /2)	O ($\sqrt{n}$)	To provide a better level of use random validation and resilience.	Not resistant to smart node cloning attack due to determinism verification process.	Distributed
	RWND [36]			Witness contract well insured, high probability of detection.	High connection, memory, and power cost when there are more regions.	Distributed
	SSRWND [37]			Witness contract well insured, high probability of detection.	High connection, memory, and power cost when there are more regions.	Distributed
	ERCD [38]	O (h$\sqrt{h}$)	O (h)	High detection probability with	Storing witnesses requires little routing of the node	Distributed

				random witness selection.	ring, which reduces storage costs.	
	SBEA [39]	High complexity	Best	Improvement of the ERCD protocol by the added routing algorithm to give improvement to network lifetime and increase the performance of sensor nodes.	The arrival of data to the target is not guaranteed, The scattering density is high even if the active data node is far from the source and will not be affected by the resource-target node. Not useful if you need a contract.	Hybrid
	PAWS [40]	O ($3\sqrt{n}$ log(n))	O $(1)^2$	Detection probability, energy consumption, and flexibility are good.	Limited redundancy.	Distributed
	RE-GSASA [41]	O (n $\sqrt{n}$)	O (n)	Improves the probability of detecting a clone attack by reducing the time to detect a clone attack and optimizing power consumption.	Messages overhead are high.	Distributed
	ACTIVE [42]	O ($\sqrt{n}$)	O (1)	Good memory cost and the protocol tests nodes using relays to test whether randomly selected nodes are cloned.	Communication cost.	Distributed
Generation or group based	Bekara and Laurent [43, 44]	O (n)	O (1)	Simple protocol and its communication cost are lower.	The nodes in it are linked to their geographical locations and groups.	Distributed
	Basic Protocol [45]	O (m)	O (m)	less communication, Arithmetic operations and memory overhead are also lower.	It suffers from poor network connectivity so high-power applications cannot use it.	Distributed
	Location Claim Base Protocol [45]	O (m+d)	O (d+2m)	Strong detection ability, appropriate communication cost, and lower computational and storage burdens.	Dumping bogus claims due to DoS risks.	Distributed
	Multi-Group Base Protocol [45]	3xO(m + d)	O (d + 2xm(1 + Dmax)	A solid compromise to knots since the opponent wants to settle several sets.	High connection cost.	Distributed
	Sei and Honiden [17]	O (r)	O (r. $\sqrt{n}$)	There is no entity more reliable, and more flexible.	large communication costs, The start time of the built-in detection.	Distributed
	CINORA [46]	O (M ∗√W) thus involved is O(M ∗W)		It does not conclusively determine the identity of a node to a cell, which helps us to make node anonymous for increased security.	The effect on detection accuracy is unknown when adversary nodes form a community to exploit the network and disrupt the communication process, and the Effect of symmetric and asymmetric switches on communication and memory overheads also.	Distributed
Neighbor based	HIP/HOP [42, 47]			Low communication cost	High Memory cost.	Distributed
Clustering based	LEACH [48, 49]			1. LEACH schedule-based protocols addressing idle listening avoidance using TDMA schemes. 2. Explicitly define the sending and receiving opportunities of the nodes and allow them to rest when they are not needed.	1. When faced with a changing topology, setting and maintaining tables requires signaling. 2. The time is divided into relatively small slots if the TDMA variant is used, and the sender and receiver must agree on the limits of the slots to meet each other and also avoid interference with	Distributed

				3. It calculates transmission schedules in such a way that no collisions occur at receivers. 4. There is therefore no need to use special mechanisms to avoid hidden end positions.	other slots, which may lead to collisions. However, solving the time synchronization problem involves some additional signaling traffic. 3. Despite the small date ranges, these schedules do not easily adapt to different pregnancies. 4. A node has difficulty giving unused bits of time to its neighbors. 5. The schedule of the node needs a large amount of memory and the nodes with weak capabilities cannot handle it.	
	NI LEACH [50]	O (l (1+m'2))	O (k. e)	Less delay, balanced productivity.	It is not useful to use it in the case of multiple opponents, because its detection rate is lower.	Distributed
	MMF – CND using LEACH Protocol [51]	CND: O(n) MMF: O (c^2n)	CND O (n)	Add new security to LEACH protocol by MMF algorithm and node clone detection by CND algorithm.	Communication and memory costs are high.	Centralized
	Hierarchical Distributed Algorithm (HDA) [14]	O (N^2)	O (N)	Transmitter by sensor nodes only to its cluster headers. Then the cluster head sends the data to the base station.	High communication and memory cost.	Distributed
	NBCAD [42, 52]	Less than SET, RED Protocols		High Detection ratio and higher probability. Less memory and power consumption of nodes as well as reduced transmission range.		Distributed
Witness path based	LSCD [53]	O (n$\sqrt{n}$)	O (l/ r)	High probability of detection, and node storage is suitably low.	The communication cost is High.	Distributed
	TAWS [6]	O ($\sqrt{n}$ log(n))	O $(1)^2$	The witness nodes are selection of in a random manner using a random walk table.	Relatively high memory cost due to the random walk table.	Distributed
Cluster head based	LTBRD [54]			Less memory and power consumption.	The detection probability is low.	Distributed
	PRCD [55]	O (Np)	O (1 / p)	Long network life and adequate computing complexity.		Distributed
Base station Based	DNCA (Detection of Node Capture Attack) [56]	O (n $\sqrt{n}$)	O (n)	The captured nodes did not participate during this period in any network operation.	The communication and memory costs are high.	Distributed

Table 2. Clone node detection protocols in mobile WSNs

Type of Protocol	The Name	Communication Cost	Memory Cost	Advantages	Drawbacks	Detection Methodology
Node speed based [11]	Fast [14] by: Ho et al. Scheme [11]	O($n\sqrt{n}$)	O(n)	A mobile node should never move at speeds greater than the maximum speed configured by the system.	This protocol does not carry the costs of the current generation of Wireless Sensor Networks because it uses much more expensive equipment called GPS [14].	Centralized

Information exchange based [11] or Conflict based [14] Witness based detection probability, time-based [42]	XED [14]	O(1)	O(4 . v . E(X))	Low memory cost because sensor node location information is not needed, only persistent communication is required [42].	If cloned nodes communicate with each other, they can create secret channels and can easily fool detection technology [14].	Distributed
	Zhu et al. [57] by Token Based	-	-	Used two algorithms: token and seen many time based.	Clone nodes can share tokens and make the protocol exist in name only. This protocol fails when a clever attacker creates secret channels between cloned nodes.	Distributed
Node meeting based [11] or Node mobility [14, 39]	NBDS [14]	$O(r\sqrt{n})$	O(r)	Independent of location.	The cost of messages is high.	Distributed
	EDD Protocol [14]	O(1) / O(n)	O(n)	Composed of two phases: the offline phase and the online phase.	Inapplicable due to the high storage overhead for large-scale WSNs [11, 14].	Distributed
	SDD/CDD by Conti et al. [58]			Both proposed algorithms are based on the simple observation that "If node a does not return node b within a certain period, node b may have been captured".	Any sensor node can flood the entire mobile WSN with a broadcast message which is not possible in reality. There is no change in membership in the network and this is not the case in reality.	
	SEDD [11]	O(n)	$O(\xi)$	Instead of monitoring all nodes in EDD, each node only monitors a subset of nodes	Memory and communication cost is high stilled but it is better than EDD.	Distributed
Mobility assisted based [11] or Time location-based	PDRA [59] Wang and Shi Protocol with Base Station [11, 14]	O(n)		If the answers of the cloned nodes are collected by different patrol nodes, they will be discovered by exchanging messages with the patrol guards after the round, or by the base station.		Distributed
	PDRA [59] Wang and Shi Protocol Without Base Station [11, 14]	$O(n * \sqrt{u})$		If cloned nodes are deployed in an area where a periodic node collects its answer message in a periodic period, the sentinel can invalidate it immediately upon receiving the second answer and overstepping the distance between the two locations.		Distributed
	UTLSE [11, 14]	O(n)	$O(\sqrt{n})$	- Each node is configured with a unique tracking group. - Statements of claims are only exchanged when appropriate witnesses meet each other.	High communication cost.	Distributed
	MTLSD [11]	O(n)	$O(\sqrt{n})$	- Statements of claims are only exchanged when appropriate witnesses have met each other. - MTLSD has a higher detection power than UTLSE.	High communication cost.	Distributed
Neighbor based	SHD [14]			It uses the fingerprint for each node, as well as the decision of the witness node.	High communication cost.	Distributed

Key usage-based	Deng and Xiong Protocol [11]	O(n log n)		Polynomial-based pair-wise key pre-distribution and Bloom Filters.	There is no evidence that a participating cloned node will faithfully report its keys to the base station. The number of the parent node of pair switches may exceed a threshold value due to their connectivity. The dependence of centralized detection protocol operations on base station participation leads to singlepoint failure and rapid depletion of power for sensor nodes around the base station.	Centralized
Detection rate Detection probability [42]	CLONE WARS [42, 47]			High detection rate. Communication cost is reduced.		Distributed

Table 3. Node clone detection protocols in hybrid [11] (from static & mobile) in WSNs

Type of Protocol	Name	Communication Cost	Memory Cost	Advantages	Drawbacks	Detection Methodology
Topology distortion	MDS [11]	affordable	O(1)	High detection rate.	Communication overhead on the network in the case of dense network topologies.	Hybrid
Danger theory (DT)	DT [12]	O(N)	O(N)	It works way better than XED and SPRT as it exceeds false negative rates.	Getting started with learning in neural networks takes time.	Hybrid
Artificial intelligence-based	AI-DNN [60]			Corrective and perimeter defensive copy attacks based on hardware and perimeter defense systems (IDS/IPS) generating a high false positive rate can be reduced.	Expensive design and implementation costs.	Hybrid
Witness-based and multiple machine learning algorithms	Multiple machine learning models (MMLM) [61]	Ctot = Csn + Cw	Cm = Nn. L	Processing speed uses some machine learning algorithms and does not require additional memory.		Centralized
Context information sensed	Extended elliptic curve digital signature technique ECDSA [62]	O(N)	O($\sqrt{N}$)	Use three algorithms to location proof, Three algorithms work in this protocol, the site computation algorithm, the site proof creation algorithm, and the site verification algorithm, and this enhances the work of the protocol.		Distributed
Combine more than schemes	TDD/SDD [63]	-	-	There are no restrictions on the number and distribution of cloned nodes, and it incurs low computation and communication costs. TDD and SDD provide high detection accuracy and excellent resilience against cloned, collusive, smart nodes.		Distributed

4. THE POTENTIAL IMPACT OF THESE PROTOCOLS ON THE LIFESPAN OF A MOBILE WSN AND THEIR COMPATIBILITY WITH EXISTING NETWORK INFRASTRUCTURES

Node-clone detection algorithms have the potential to significantly affect how long a mobile WSN lasts. In the context of mobile WSNs, a number of protocols and procedures have been proposed to increase the network lifetime. To extend the lifespan of a network, these techniques include the usage of mobile relays, mobile sinks, and mobile sensor relocation [64]. One way to extend the lifetime of a network is to deploy mobile nodes to take over the sensing and relaying duties of bottleneck nodes. For example, when a mobile node travels to co-locate with a bottleneck node and handles the bottleneck node's transmission and reception activities, the bottleneck node can sleep to conserve energy, extending its lifetime and enhancing the longevity of the network as a whole. To extend the lifespan of mobile WSNs, dynamic optimization of sensor node communication activity has also been investigated. Moreover, strategies to balance energy consumption and increase network lifetime have been studied, including the use of multi-path routing techniques and the exploitation of node mobility in mobile WSNs [65]. The problem is that most research is not tested protocols within real WSN environments as a testbed or publishing operations, but only simulation, we hope in the future the testing should be real instead of using simulation.

5. CONCLUSION

This paper presents a review of previous research to compare and categorize some of the detection protocols for cloned nodes, highlighting their advantages and disadvantages, as well as costs in terms of memory, connectivity, and detection methodology. We have added new protocols alongside the previous ones, extracted their advantages and disadvantages through the three tables, and classified them according to the common classification in previous research. The classification was modified with simple additions from previous research as well, and this is what distinguishes our review from previous reviews. We have added new protocols alongside the protocols. We extracted its advantages and disadvantages through the three tables, and classified them according to the unified classification, and this is what distinguishes our review from previous reviews. We found that almost all detection schemes suffer from high communication and storage costs, but they still provide a high detection rate because such large costs affect the life of the network, especially when nodes do not have many capabilities to bear it. The types of sensors were also highlighted, which are central, distributed, and hybrid (a mixture of the two types). In static nodes, a node can be located once during initialization when sensor nodes are statically deployed. But, when the sensor nodes are mobile, they must periodically obtain their locations as they travel and this is one of the challenges faced by the mobile nodes. Therefore, they need to increase the time, energy, and speed of speed of execution. Presenting the significance of these findings for further study, the creation of fresh detection algorithms, or the area of mobile WSNs in general could improve the survey. For instance, the survey can go over how to overcome the difficulties found by creating new detection techniques or enhancing the ones that already exist. The impact of the results on the design of mobile WSNs and their applications might also be covered in the survey. By outlining these ramifications, the survey may offer a more thorough comprehension of the importance of the issues raised and their possible influence on the area of mobile WSNs. In the future, it is anticipated that the issues of high prices and network life impact in WSNs will be resolved by future technological developments in areas like energy efficiency, sustainability, and integration with edge computing and artificial intelligence. These advancements will support WSNs' long-term viability, sustainability, and efficiency, opening the door for further development and broad use. Including such research will affect the quality of future research, and benefiting from previous mistakes and not falling into them will enhance the improvement of energy use and speed of communication between nodes, and most importantly, it will increase the security of the network from cloning, due to the great need people have for Internet of Things networks, the most important of which are the medical, industrial, agricultural, and military fields in Nowadays, it is necessary to pay attention to its security in order to further enhance its quality in industries.

ACKNOWLEDGEMENT

All thanks and appreciation to the supervising doctor, Aladdin Alsharifi, for scientific support for me. With the offer, there is no financial support from any institution for this research.

REFERENCES

[1] Zhou, Y., Fang, Y., Zhang, Y. (2008). Securing Wireless Sensor Networks: A survey. IEEE Communications Surveys & Tutorials, 10(3): 6-28. https://doi.org/10.1109/COMST.2008.4625802

[2] Zhou, Y., Zhang, Y., Fang, Y. (2007). Access control in Wireless Sensor Networks. Ad Hoc Networks, 5(1): 3-13. https://doi.org/10.1016/j.adhoc.2006.05.014

[3] Deng, X.M., Xiong, Y. (2011). 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. https://doi.org/10.1007/s11390-011-1172-1

[4] Usha, N.S., Anita, E.M. (2018). An elaborate survey on node replication attack in static Wireless Sensor Networks. International Journal of Computer and Information Engineering, 12(10): 797-804. https://doi.org/10.5281/zenodo.1474723

[5] Numan, M., Subhan, F., Khan, W.Z., Hakak, S., Haider, S., Reddy, G.T., Jolfaei, A., Alazab, M. (2020). A systematic review on clone node detection in static Wireless Sensor Networks. IEEE Access, 8: 65450-65461. https://doi.org/10.1109/ACCESS.2020.2983091

[6] Znaidi, W., Minier, M., Ubéda, S. (2013). Hierarchical node replication attacks detection in Wireless Sensor Networks. International Journal of Distributed Sensor Networks, 9(4): 745069. https://doi.org/10.1155/2013/745069

[7] Meghana, S., Srinath, R. (2019). A novel mechanism for clone attack detection in hybrid IoT devices. International Research Journal of Engineering and

Technology, 6(5): 2194-2198.

[8] Shaukat, H.R., Hashim, F., Shaukat, M.A., Ali Alezabi, K. (2020). Hybrid multi-level detection and mitigation of clone attacks in mobile wireless sensor network (MWSN). Sensors, 20(8): 2283. https://doi.org/10.3390/s20082283

[9] Singh, S.P., Sharma, S.C. (2016). Critical analysis of distributed localization algorithms in Wireless Sensor Networks. International Journal of Wireless and Microwave Technologies, 4: 72-83. https://doi.org/10.5815/ijwmt.2016.04.07

[10] Khan, S.A. (2011). Localization and fault detection in Wireless Sensor Networks. Doctoral dissertation, Université Paris-Est.

[11] Khan, W.Z., Aalsalem, M.Y., Saad, M.N.B.M., Xiang, Y. (2013). Detection and mitigation of node replication attacks in Wireless Sensor Networks: A survey. International Journal of Distributed Sensor Networks, 9(5): 149023. https://doi.org/10.1155/2013/149023

[12] Brooks, R., Govindaraju, P.Y., Pirretti, M., Vijaykrishnan, N., Kandemir, M.T. (2007). On the detection of clones in sensor networks using random key predistribution. IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 37(6): 1246-1258. https://doi.org/10.1109/TSMCC.2007.905824

[13] Choi, H., Zhu, S., La Porta, T.F. (2007). SET: Detecting node clones in sensor networks. In 2007 Third International Conference on Security and Privacy in Communications Networks and the Workshops - SecureComm 2007, Nice, France, pp. 341-350. https://doi.org/10.1109/SECCOM.2007.4550353

[14] Anthoniraj, J., Razak, T.A. (2014). Clone attack detection protocols in Wireless Sensor Networks: A survey. International Journal of Computer Applications, 98(5): 43-49.

[15] Conti, M., Di Pietro, R., Mancini, L.V., Mei, A. (2007). A randomized, efficient, and distributed protocol for the detection of node replication attacks in Wireless Sensor Networks. In Proceedings of the 8th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Montreal Quebec, Canada, pp. 80-89. https://doi.org/10.1145/1288107.1288119

[16] Conti, M., Di Pietro, R., Mancini, L., & Mei, A. (2010). Distributed detection of clone attacks in Wireless Sensor Networks. IEEE Transactions on Dependable and Secure Computing, 8(5): 685-698. https://doi.org/10.1109/TDSC.2010.25

[17] Sei, Y., Honiden, S. (2010). Distributed detection of node replication attacks resilient to many compromised nodes in Wireless Sensor Networks. In 4th International ICST Conference on Wireless Internet, Maui, HI, USA. http://doi.org/10.4108/ICST.WICON2008.4796

[18] Meng, X., Lin, K., Li, K. (2010). A note-based randomized and distributed protocol for detecting node replication attacks in Wireless Sensor Networks. In Algorithms and Architectures for Parallel Processing: 10th International Conference, Busan, Korea, pp. 559-570. https://doi.org/10.1007/978-3-642-13119-6_49

[19] Zeng, Y., Cao, J., Zhang, S., Guo, S., Xie, L. (2010). Random-walk based approach to detect clone attacks in Wireless Sensor Networks. IEEE Journal on Selected Areas in Communications, 28(5): 677-691. https://doi.org/10.1109/JSAC.2010.100606

[20] Mishra, A.K., Turuk, A.K. (2013). A zone-based node replica detection scheme for Wireless Sensor Networks. Wireless Personal Communications, 69: 601-621. https://doi.org/10.1007/s11277-012-0592-8

[21] Yu, C.M., Lu, C.S., Kuo, S.Y. (2016). Compressed sensing-based clone identification in sensor networks. IEEE Transactions on Wireless Communications, 15(4): 3071-3084. https://doi.org/10.1109/TWC.2016.2516021

[22] Kenaza, T., Hamoud, O.N., Nouali-Taboudjemat, N. (2015). Efficient centralized approach to prevent from replication attack in Wireless Sensor Networks. Security and Communication Networks, 8(2): 220-231. https://doi.org/10.1002/sec.975

[23] Uma Maheswari, P., Ganesh Kumar, P. (2017). Dynamic detection and prevention of clone attack in Wireless Sensor Networks. Wireless Personal Communications, 94: 2043-2054. https://doi.org/10.1007/s11277-016-3357-y

[24] Xing, K., Liu, F., Cheng, X., Du, D. H. (2008). Real-time detection of clone attacks in Wireless Sensor Networks. In 2008 The 28th International Conference on Distributed Computing Systems, Beijing, China, pp. 3-10. https://doi.org/10.1109/ICDCS.2008.55

[25] Naruephiphat, W., Ji, Y., Charnsripinyo, C. (2012). An area-based approach for node replica detection in Wireless Sensor Networks. In 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Liverpool, UK, pp. 745-750. https://doi.org/10.1109/TrustCom.2012.73

[26] Meenatchi, S., Navaneethan, C., Sivakumar, N., Thanapal, P., Prabhu, J. (2014). SWBC-security in Wireless Sensor Networks by broadcasting location claims. Journal of Theoretical & Applied Information Technology, 64(1): 16-21.

[27] Abinaya, P., Geetha, C. (2014). Dynamic detection of node replication attacks using X-RED in Wireless Sensor Networks. In International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, India, pp. 1-4. https://doi.org/10.1109/ICICES.2014.7033957

[28] Parno, B., Perrig, A., Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. In 2005 IEEE Symposium on Security and Privacy (S&P'05), Oakland, CA, USA, pp. 49-63. https://doi.org/10.1109/SP.2005.8

[29] Zhang, M., Khanapure, V., Chen, S., Xiao, X. (2009). Memory efficient protocols for detecting node replication attacks in Wireless Sensor Networks. In 2009 17th IEEE International Conference on Network Protocols, Plainsboro, NJ, USA, pp. 284-293. https://doi.org/10.1109/ICNP.2009.5339674

[30] Cynthia, J.S., Punithavathani,D. S. (2016). Taws: Table assisted walk strategy in clone attack detection. ICTACT Journal on Communication Technology, 7(4): 1387-1396. https://doi.org/10.21917/ijct.2016.0205

[31] Li, Z., Gong, G. (2009). Randomly directed exploration: An efficient node clone detection protocol in Wireless Sensor Networks. In 2009 IEEE 6th International Conference on Mobile Adhoc and Sensor Systems, Macau, pp. 1030-1035. https://doi.org/10.1109/MOBHOC.2009.5337014

[32] Kim, C., Shin, S., Park, C., Yoon, H. (2009). A resilient and efficient replication attack detection scheme for Wireless Sensor Networks. IEICE Transactions on

Information and Systems, 92(7): 1479-1483. https://doi.org/10.1587/transinf.E92.D.147

[33] Li, Z., Gong, G. (2013). On the node clone detection in Wireless Sensor Networks. IEEE/ACM Transactions on Networking, 21(6): 1799-1811. https://doi.org/10.1109/TNET.2012.2233750

[34] Swathi, P., Vasu, S. (2014): A new approach of node clone detection protocols in Wireless Sensor Networks. International Journal of Innovative Research in Computer and Communication Engineering, 2(7): 5039-5045.

[35] Zhou, Y., Huang, Z., Wang, J., Huang, R., Yu, D. (2014). An energy-efficient random verification protocol for the detection of node clone attacks in Wireless Sensor Networks. EURASIP Journal on Wireless Communications and Networking, 2014: 163. https://doi.org/10.1186/1687-1499-2014-163

[36] Khan, W.Z., Aalsalem, M.Y., Saad, N.M. (2015). Distributed clone detection in static Wireless Sensor Networks: Random walk with network division. PloS One, 10(5): e0123069. https://doi.org/10.1371/journal.pone.0123069

[37] Aalsalem, M.Y., Khan, W.Z., Saad, N.M., Hossain, M.S., Atiquzzaman, M., Khan, M.K. (2016). A new random walk for replica detection in WSNs. PloS One, 11(7): e0158072. https://doi.org/10.1371/journal.pone.0158072

[38] Zheng, Z., Liu, A., Cai, L. X., Chen, Z., Shen, X. (2015). Energy and memory efficient clone detection in Wireless Sensor Networks. IEEE Transactions on Mobile Computing, 15(5): 1130-1143. https://doi.org/10.1109/TMC.2015.2449847

[39] Sathya, V., Kannan, D.S. (2022). Lifetime escalation and clone detection in Wireless Sensor Networks using snowball endurance algorithm (SBEA). KSII Transactions on Internet and Information Systems (TIIS), 16(4): 1224-1248. https://doi.org/10.3837/tiis.2022.04.008

[40] Cynthia, J.S., Punithavathani, D.S. (2016). Clone attack detection using pair access witness selection technique. International Journal of Computer Networks and Applications, 3(5): 118-128. https://doi.org/10.22247/ijcna/2016/48862

[41] Rajesh Kumar, D., Shanmugam, A. (2018). A hyper heuristic localization based cloned node detection technique using GSA based simulated annealing in sensor networks. Cognitive Computing for Big Data Systems Over IoT: Frameworks, Tools and Applications, pp. 307-335. https://doi.org/10.1007/978-3-319-70688-7_13

[42] Cynthia, J.S., Punithavathani, D.S. (2016). Perlustrate of detection methodology against clone attacks in Wireless Sensor Networks. International Journal of Computational Intelligence and Informatics, 6(2): 94-107.

[43] Bekara, C., Laurent, M. (2007). Defending against nodes replication attacks on Wireless Sensor Networks. In SAR-SSI 2007: 2nd Conference on Security in Network Architectures and Information Systems, Annecy, France, pp. 31-40.

[44] Bekara, C., Laurent-Maknavicius, M. (2007). A new protocol for securing Wireless Sensor Networks against nodes replication attacks. In Third IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007), White Plains, NY, USA, pp. 59-59. https://doi.org/10.1109/WIMOB.2007.4390853

[45] Ho, J. W., Liu, D., Wright, M., Das, S.K. (2016). Distributed Detection of Replica Node Attacks. In Distributed Sensor Networks, pp. 540-561.

[46] Lou, Y., Zhang, Y., Liu, S. (2012). Single hop detection of node clone attacks in mobile Wireless Sensor Networks. Procedia Engineering, 29: 2798-2803. https://doi.org/10.1016/j.proeng.2012.01.393

[47] Conti, M., Di Pietro, R., Spognardi, A. (2014). Clone wars: Distributed detection of clone attacks in mobile WSNs. Journal of Computer and System Sciences, 80(3): 654-669. https://doi.org/10.1016/j.jcss.2013.06.017

[48] Tandel, R.I. (2016). Leach protocol in wireless sensor network: A survey. International Journal of Computer Science and Information Technologies, 7(4): 1894-1896.

[49] Bodhana. (2022). LEACH- (Low Energy Adaptive Clustering Hierarchy) protocol - Schedule based protocol (EC8702-UNIT-3). https://www.youtube.com/watch?v=SWOAeJM7xgs.

[50] Cheng, G., Guo, S., Yang, Y., Wang, F. (2015). Replication attack detection with monitor nodes in clustered Wireless Sensor Networks. In 2015 IEEE 34th International Performance Computing and Communications Conference (IPCCC), Nanjing, China, pp. 1-8. https://doi.org/10.1109/PCCC.2015.7410341

[51] Sankar Chatterjee, P., Roy, M. (2018). Lightweight cloned-node detection algorithm for efficiently handling SSDF attacks and facilitating secure spectrum allocation in CWSNs. IET Wireless Sensor Systems, 8(3): 121-128. https://doi.org/10.1049/iet-wss.2016.0065

[52] Anthoniraj J., Razak, T.A. (2015). NBCAD: Neighbor based clone attack detection in cluster based static Wireless Sensor Networks.International of Engineering and Technology (IJET), 7(3): 912- 921.

[53] Dong, M., Ota, K., Yang, L.T., Liu, A., Guo, M. (2016). LSCD: A low-storage clone detection protocol for cyber-physical systems. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 35(5): 712-723. https://doi.org/10.1109/TCAD.2016.2539327

[54] Amudha, G., Narayanasamy, P. (2018). Distributed location and trust based replica detection in Wireless Sensor Networks. Wireless Personal Communications, 102: 3303-3321. https://doi.org/10.1007/s11277-018-5369-2

[55] Pan, F., Pang, Z., Xiao, M., Wen, H., Liao, R. F. (2018). Clone detection based on physical layer reputation for proximity service. IEEE Access, 7: 3948-3957. https://doi.org/10.1109/ACCESS.2018.2888693

[56] Ho, J.W. (2010). Distributed detection of node capture attacks in Wireless Sensor Networks. In Smart Wireless Sensor Networks, pp. 345-360.

[57] Zhu, W.T., Zhou, J., Deng, R.H., Bao, F. (2012). Detecting node replication attacks in mobile sensor networks: Theory and approaches. Security and Communication Networks, 5(5): 496-507. https://doi.org/10.1002/sec.338

[58] Conti, M., Di Pietro, R., Mancini, L.V., Mei, A. (2008). Emergent properties: detection of the node-capture attack in mobile Wireless Sensor Networks. In Proceedings of the First ACM Conference on Wireless Network Security, Alexandria, USA, pp. 214-219. https://doi.org/10.1145/1352533.1352568

[59] Wang, L.M., Shi, Y. (2011). Patrol detection for replica

attacks on Wireless Sensor Networks. Sensors, 11(3): 2496-2504. https://doi.org/10.3390/s110302496

[60] Morales-Molina, C.D., Hernandez-Suarez, A., Sanchez-Perez, G., et al. (2021). A dense neural network approach for detecting clone ID attacks on the RPL protocol of the IoT. Sensors, 21(9): 3173. https://doi.org/10.3390/s21093173

[61] Ahmad, U. (2022). A node pairing approach to secure the Internet of Things using machine learning. Journal of Computational Science, 62: 101718. https://doi.org/10.1016/j.jocs.2022.101718

[62] Hameed, K., Garg, S., Amin, M. B., Kang, B., Khan, A. (2022). A context-aware information-based clone node attack detection scheme in Internet of Things. Journal of Network and Computer Applications, 197: 103271. https://doi.org/10.1016/j.jnca.2021.103271

[63] Sakthivel, M., Daniel, D.A.J., Karnavel, K. (2014). RIP: Clone detection in mobile ad hoc network. Transactions on Engineering and Sciences, 2(3): 21-26.

[64] Zhang, X., Lu, X., Zhang, X. (2020). Mobile wireless sensor network lifetime maximization by using evolutionary computing methods. Ad Hoc Networks, 101: 102094. https://doi.org/10.1016/j.adhoc.2020.102094

[65] Guo, W., Yan, C., Lu, T. (2019). Optimizing the lifetime of Wireless Sensor Networks via reinforcement-learning-based routing. International Journal of Distributed Sensor Networks, 15(2): 1550147719833541. https://doi.org/10.1177/1550147719833541